3Com® Telecommuting Module User Manual

Version 4.6.5

3Com® Telecommuting Module User Manual: Version 4.6.5

Part Number BETA

Published April 2009

3Com Corporation, 350 Campus Drive, Marlborough MA 01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, NBX, and SuperStack are registered trademarks of 3Com Corporation. NBX NetSet, pcXset, and VCX are trademarks of 3Com Corporation.

Adobe is a trademark and Adobe Acrobat is a registered trademark of Adobe Systems Incorporated. Microsoft, Windows, Windows 2000, Windows NT, and Microsoft Word are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

Table of Contents

Part I. Introduction to 3Com VCX IP Telecommuting Module

Chapter 1. Introduction to 3Com VCX IP Telecommuting Module

Some of the functions of 3Com VCX IP Telecommuting Module are:

- SIP proxy: Forwarding of SIP requests.
- SIP registrar: Registration of SIP users.
- Protection against such attacks as address spoofing.
- Logging/alarm locally on the Telecommuting Module, via email and/or via syslog.
- Managing several logical/directly-connected networks and several network connections/physical networks.
- Administration of the Telecommuting Module through a web browser using http or https.
- QoS - bandwidth limitation and traffic prioritizing (using the QoS module).
- Failover - connect two Telecommuting Modules in parallel; one handles traffic and the other acts as a hot standby.
- STUN server and Remote SIP Connectivity for SIP clients behind NAT boxes which are not SIP aware (using the Remote SIP Connectivity module).

Note that some of the functions mentioned here are only available if the corresponding extension module has been installed.

What is a Telecommuting Module?

A Telecommuting Module is a device which processes traffic under the SIP protocol (see RFC 3261). The Telecommuting Module receives SIP requests, processes them according to the rules you have set up, and forwards them to the receiver.

The Telecommuting Module connects to an existing enterprise firewall through a DMZ port, enabling the transmission of SIP-based communications without affecting firewall security. SIP messages are then routed through the firewall to the private IP addresses of authorized users on the internal network.

The Telecommuting Module can also be used as an extra gateway to the internal network without connecting to the firewall, transmitting only SIP-based communications.

Configuration alternatives

The 3Com VCX IP Telecommuting Module can be connected to your network in three different ways, depending on your needs.

Note that if the Standalone type is used, the interface which should receive traffic from the outside must have a public IP address (no NAT).

For a DMZ or DMZ/LAN type which uses a private IP address on the interface connected to the DMZ of the firewall, its corresponding public IP address must be entered on the Interoperability page.

DMZ Configuration

Using this configuration, the Telecommuting Module is located on the DMZ of your firewall, and connected to it with only one interface. The SIP traffic finds its way to the Telecommuting Module using DNS or by setting the Telecommuting Module as an outbound proxy on the clients.

This is the most secure configuration, since all traffic goes through both your firewall and your Telecommuting Module. It is also the most flexible, since all networks connected to any of your firewall's interfaces can be SIP-enabled.

The drawback is that the SIP traffic will pass the firewall twice, which can decrease performance.

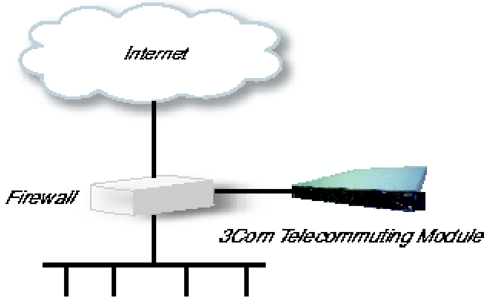


Fig 1. Telecommuting Module in DMZ configuration.

DMZ/LAN Configuration

Using this configuration, the Telecommuting Module is located on the DMZ of your firewall, and connected to it with one of the interfaces. The other interfaces are connected to your internal networks. The Telecommuting Module can handle several networks on the internal interface even if they are hidden behind routers.

This configuration is used to enhance the data throughput, since the traffic only needs to pass your firewall once.

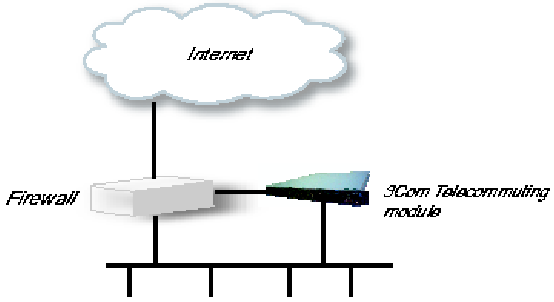


Fig 2. Telecommuting Module in DMZ/LAN configuration.

Standalone Configuration

Using this configuration, the Telecommuting Module is connected to the outside on one interface and your internal networks on the others.

Use this configuration only if your firewall lacks a DMZ interface, or for some other reason cannot be configured for the DMZ or DMZ/LAN alternatives.

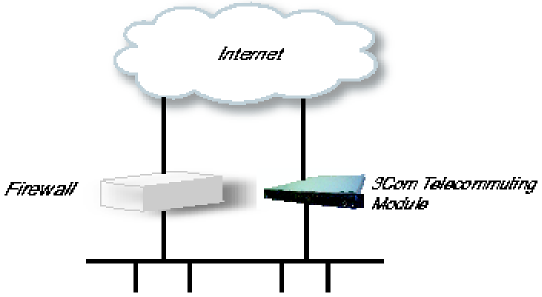


Fig 3. Telecommuting Module in Standalone configuration.

Quick guide to 3Com VCX IP Telecommuting Module installation

3Com VCX IP Telecommuting Module is easy to install:

- Select an IP address for the Telecommuting Module on your network.
- The network interfaces are marked with 1 and 2. These numbers correspond to the physical interfaces *eth0* and *eth1* respectively, the latter which should be use in the installation program.
- Plug in the power cord and turn on the Telecommuting Module.
- Wait while the Telecommuting Module boots up.
- Connect the network cables to the network interfaces.
- Connect a monitor and a keyboard to the Telecommuting Module.
- Log in as *admin*. No password is needed the first time you log in.
- Run the installation script, where you assign IP address, configuration computers and password.
- Direct your web browser to the IP address of the Telecommuting Module.

- Now you can see the main page of 3Com VCX IP Telecommuting Module. Click on the **Telecommuting Module Type** link and select the configuration for your Telecommuting Module. The types are described on the corresponding help page.
- Go to the **Basic Configuration** page and enter a **DNS server**. See also the Basic Configuration section.
- Go to the **Access Control** page and make settings for the configuration of the Telecommuting Module. See also the Access Control section.

- Go to the **Network Interface 1** page under **Network Configuration** and enter the necessary configuration. See also the Interface section. Note that the Telecommuting Module must have at least one IP address which can be reached from the Internet.
- If one of the Telecommuting Module Types DMZ/LAN or Standalone was chosen, move on to the **Network Interface 2** page and give the Telecommuting Module at least one IP address on this interface and state the networks connected to the interface. See also the Interface section.
- Go to the **Default Gateway** page and enter a **Default gateway**. See also the Default Gateway section.
- Go to the **Networks and Computers** page. Define the networks that will send and receive SIP traffic using the Telecommuting Module. Usually, you need at least one network per interface of the firewall connected to the Telecommuting Module (or, for the Standalone type, per interface of the Telecommuting Module). Some computers should be handled separately, and they therefore need their own networks. See also the Networks and Computers section.
- Go to the **Surroundings** page (for the DMZ Telecommuting Module Type) and state the networks connected to the *firewall*. See also the Surroundings section in the chapter titled Network Configuration.
- Go to **Basic Settings** under **SIP Services** and switch the **SIP module** on. Enter the port range to be used by the Telecommuting Module for the media streams. See also the Basic Settings section.
- Go to the **Filtering** page under **SIP Traffic** to create **Proxy rules** for the SIP traffic from different networks and allow the content types which should be allowed in the SIP media streams. See also the Filtering section.
- Go to the **Interoperability** page. Set **URI Encoding** to "Keep username in URIs".
- Go to the **Save/Load Configuration** page under **Administration**. Select **Apply configuration**. Now you can test your new configuration and save it permanently if you are satisfied with it. If the configuration is not satisfactory, select **Revert** or restart the Telecommuting Module. The old configuration will remain.
- When the configuration has been applied, you should save a backup to file. Press **Save to local file** to save the configuration.

When the Telecommuting Module is configured, the firewall connected to it must also be reconfigured (for the DMZ and DMZ/LAN Telecommuting Module Types).

- Allow UDP and TCP traffic in the port interval used for media streams by the Telecommuting Module, and port 5060. This traffic must be allowed to all networks which should be reached by SIP traffic.

See also the chapter titled Firewall and Client Configuration, for information on configuring the firewall and the SIP clients.

About settings in 3Com VCX IP Telecommuting Module

3Com VCX IP Telecommuting Module uses two sets of Telecommuting Module configurations: preliminary and permanent configuration. The permanent configuration is what is used in the active Telecommuting Module. The preliminary configuration is where you change and set the configuration. See chapter 3, Configuring 3Com VCX IP Telecommuting Module, for instructions.

The changes you make in the preliminary configuration are not stored in the permanent configuration until you click on **Apply configuration** on the **Save/Load Configuration** page under **Administration**.

The password configuration and time setting are the exceptions to this rule; they are saved immediately. Change the administrator passwords and create more administrator users on the **User Administration** page under **Administration**.

3Com VCX IP Telecommuting Module displays serious errors in red, e.g., if mandatory information is not entered. Blank fields are shown in red. Fields that you correct remain red until you select **Save**, **Add new rows** or update the page in some other way.

If you have a web connection with the Telecommuting Module that is inactive for 10 minutes, it will ask for a password again.

Always log out from the Telecommuting Module administration interface when you are not using it. Press the **Log out** button on the left to log out.

The terms used in the book are explained in appendix D, Definitions of Terms.

For a general description of how to configure and administer the Telecommuting Module, see chapter 3, Configuring 3Com VCX IP Telecommuting Module.

Chapter 2. Installing 3Com VCX IP Telecommuting Module

Installation

There are three ways to install an 3Com VCX IP Telecommuting Module: using a serial cable, using a diskette or perform a magic ping.

Installation with a serial cable or a diskette requires being at the same place as the Telecommuting Module, but will give more options for the start configuration.

Installation with magic ping does not require being on the same place as the Telecommuting Module (but the computer has to be connected to the same logical network as the Telecommuting Module), but restricts the start configuration.

Installation with magic ping

You can use the magic ping to set an IP address for the Telecommuting Module. This is how to perform a magic ping:

- Plug in the power cord and turn the Telecommuting Module on.
- Wait while the Telecommuting Module boots up.
- Connect the network cables to the network interfaces.
- Find out the MAC address of the Telecommuting Module (printed on the Telecommuting Module label). This is the MAC address of **Network Interface 1**.
- Add a static entry in your local ARP table consisting of the Telecommuting Module's MAC address and the IP address it should have on eth0.

  This is how to add a static ARP entry if you use a Windows computer:

  Run the command *command* (or cmd).

  In the Command window, enter the command arp -s *ipaddress macaddress* where *ipaddress* is the new IP address for the eth0 interface, and *macaddress* is the MAC address printed on the Telecommuting Module, but with all colons (:) replaced with dashes (-).

- Ping this IP address to give the Telecommuting Module its new IP address. You should receive a ping reply if the address distribution was successful.
- Configure the rest through a web browser.

The magic ping will not set any password. Set a password immediately via the web user interface. Before any configuration has been made, only the computer which performed the magic ping will be able to configure the 3Com VCX IP Telecommuting Module.

Installation with a serial cable

These steps are performed when installing with a serial cable:

- Connect the Telecommuting Module to your workstation with the enclosed serial cable.
- Plug in the power cord and turn the Telecommuting Module on.
- Wait while the Telecommuting Module boots up.
- Log on from your workstation.
- Run the installation program (see following instructions).
- Connect the network cables to the network interfaces.
- Configure the rest through a web browser.

Connect the Telecommuting Module to your workstation with the enclosed serial cable, plug in the power cord and turn the Telecommuting Module on. You will have to wait a few minutes while it boots up.

- If you use a Windows workstation, connect like this: Start *Hyperterm*. A Location dialogue will show, asking for your telephone number and area. Click Cancel followed by Yes. Then you will be asked to make a new connection. Type a name for this connection, select an icon and click OK. The Location dialogue will show again, so click Cancel followed by Yes.

  Now you can select Connect using COM1 and click OK. A Port settings dialogue will show, where you select 19200 as Bits per second. Use the default configuration for all other settings. Click OK and wait for a login prompt. (In some cases you have to press Return to get the login prompt.)

- If you use a Linux workstation, connect like this: Make sure that there is a symbolic link named /dev/modem which points to the serial port you connected the Telecommuting Module to. Connect using *minicom* with the bit rate 19200 bits/s, and wait for a login prompt.

Log on as the user *admin*. The first time you log on, no password is required. You set the password when you run the installation script, which starts automatically when you have logged on.

Each network interface is marked with a name (1 and 2), which corresponds to a tab under **Network Configuration**. All eth interfaces belong to ethernet cards and should only be connected using ethernet cables.

Decide which computer(s) are allowed to configure 3Com VCX IP Telecommuting Module and enter the name of the network interface to which they are connected, for example, eth0. You must use the physical device name (eth0 and eth1).

Enter the IP address of the Telecommuting Module on this interface and the network mask for the network.

A network mask can be written in two ways in 3Com VCX IP Telecommuting Module:

- The first looks just like an IP address, for example 255.255.192.0 or 255.255.254.0.

- The other way is as a number between 0 and 32. An IP address has 32 bits, where the number of the network mask indicates how many bits are used in the network's addresses. The rest of the bits identifies the computer on the network.

Now, you can select to deactivate any network interfaces. Select y to deactivate all interfaces but the one you just configured. The remaining network interfaces can be activated later when you complete the configuration via the web interface from your work station. This only applies to interfaces which was previously active; you can't activate interfaces with this setting.

Now enter the computer or computers from which the Telecommuting Module may be configured (the configuration computers).

Then enter a password for the Telecommuting Module. This is the password you use in your web browser to access and change the Telecommuting Module's configuration. Finally, you can reset all other configuration if you want to.

Following is a sample run of the installation program.

```
3Com VCX IP Telecommuting Module Administration
  1. Basic configuration
  2. Save/Load configuration


  5. Wipe email logs
  6. Set password
  7. Command line interface
  a. About
  q. Exit admin
  ==>
```

Select 1 to install your 3Com VCX IP Telecommuting Module.

```
Basic unit installation program version 4.6.5

Press return to keep the default value

Network configuration inside:
 Physical device name[eth0]:
 IP address [0.0.0.0]: 10.47.2.242
 Netmask/bits [255.255.255.0]: 255.255.0.0
 Deactivate other interfaces? (y/n) [n]

Computers from which configuration is allowed:

You can select either a single computer or a network.

Configure from a single computer? (y/n) [y]
```

If you choose to allow only one computer to configure the Telecommuting Module, you are asked for the IP address (the mask is set automatically).

```
IP address [0.0.0.0]: 10.47.2.240
```

If this IP address is not on the same network as the IP address of the Telecommuting Module, you are asked for the router. Enter the IP address of the router on the network where the Telecommuting Module is connected. Then enter the network address and mask of the network containing the *configuring computer*.

```
Static routing:
The computer allowed to configure from is not on a network local to
this unit. You must configure a static route to it. Give
the IP address of the router on the network the unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

You can choose to allow several computers to configure the Telecommuting Module, by answering no to the question:

```
Configure from a single computer? (y/n) [y] n
```

The installation program then asks for the network number. The configuration computers must be entered as a complete subnet, i. e. a range which can be written as a network number and a netmask (like 10.47.2.128 with netmask 255.255.255.128, which means the computers 10.47.2.128-10.47.2.255). All computers on this subnet will be allowed to configure the Telecommuting Module. For more information about network numbers and netmasks, see chapter 3, Configuring 3Com VCX IP Telecommuting Module.

```
Network number [0.0.0.0]: 10.47.2.0
Netmask/bits [255.255.255.0]: 255.255.255.0
```

If the network or partial network is not directly connected to the Telecommuting Module, you must enter the IP address of the router leading to that network. Then enter the network's address and mask.

```
Static routing:
The network allowed to configure from is not on a network local to this
unit. You must configure a static route to it. Give the
IP address of the router on the network this unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

Then enter a password.

```
Password []:
```

Finally, you are asked if you want to reset other configuration.

```
Other configuration
Do you want to reset the rest of the configuration? (y/n) [n]
```

If you answer **`n`**, nothing is removed. If you answer **`y`**, you have three alternatives to select from:

1. Clear as little as possible. This is the alternative that is used if you answer **`n`** to the question above. Both the preliminary and the permanent configurations will be updated with the configuration specified above.
2. Revert to the factory configuration and then apply the configuration specified above. This will affect the permanent but not the preliminary configuration.
3. Revert to the factory configuration and empty all logs and then apply the configuration specified above. Both the preliminary and the permanent configurations will be affected.

Select the update mode, which is what you want to remove.

```
Update mode (1-3) [1]:
```

All configuration is now complete. The installation program shows the configuration and asks if it is correct.

yes saves the configuration.

no runs the installation program over again.

abort ends the installation program without saving.

```
You have now entered the following configuration

Network configuration inside:
 Physical device name: eth0
 IP address: 192.168.150.2
 Netmask: 255.255.255.0
 Deactivate other interfaces: no

Computer allowed to configure from:
 IP address: 192.168.128.3

Password: eeyore

The rest of the configuration is kept.

Is this configuration correct (yes/no/abort)? yes
```

Now, finish configuration of the Telecommuting Module from the computer/computers specified in the installation program.

Installation with a diskette

These steps are performed when installing with a diskette:

- Select an IP address and store it on the installation diskette as described below.
- Insert the installation diskette into the Telecommuting Module's floppy drive.
- Plug in the power cord and turn the Telecommuting Module on.
- Connect the network cables to the network interfaces.
- Wait while the Telecommuting Module boots up.
- Configure the rest through a web browser.

You must first insert the diskette into your PC. If the PC is running Windows, open a Command window and run the **finst-en** script from the diskette. If the PC is running Linux, mount the diskette, change directory to the mounted one, and run the **finst-en** script.

Each network interface is marked with a name (1 and 2), which corresponds to a tab under **Network Configuration**. All eth interfaces belong to ethernet cards and should only be connected using ethernet cables.

Decide which computer(s) are allowed to configure 3Com VCX IP Telecommuting Module and enter the name of the network interface to which they are connected, for example, eth0. You must use the physical device name (eth0 and eth1).

Enter the IP address of the Telecommuting Module on this interface and the network mask for the network.

A network mask can be written in two ways in 3Com VCX IP Telecommuting Module:

- The first looks just like an IP address, for example 255.255.192.0 or 255.255.254.0.
- The other way is as a number between 0 and 32. An IP address has 32 bits, where the number of the network mask indicates how many bits are used in the network's addresses. The rest of the bits identifies the computer on the network.

Now, you can select to deactivate any network interfaces. Select y to deactivate all interfaces but the one you just configured. The remaining network interfaces can be activated later when you complete the configuration via the web interface from your work station. This only applies to interfaces which was previously active; you can't activate interfaces with this setting.

Now enter the computer or computers from which the Telecommuting Module may be configured (the configuration computers).

Then enter a password for the Telecommuting Module. This is the password you use in your web browser to access and change the Telecommuting Module's configuration. Finally, you can reset all other configuration if you want to.

Following is a sample run of the installation program on the diskette.

```
Basic unit installation program version 4.6.5

Press return to keep the default value

Network configuration inside:
 Physical device name[eth0]:
 IP address [0.0.0.0]: 10.47.2.242
 Netmask/bits [255.255.255.0]: 255.255.0.0
 Deactivate other interfaces? (y/n) [n]

Computers from which configuration is allowed:

You can select either a single computer or a network.

Configure from a single computer? (y/n) [y]
```

If you choose to allow only one computer to configure the Telecommuting Module, you are asked for the IP address (the netmask is set automatically).

```
IP address [0.0.0.0]: 10.47.2.240
```

If this IP address is not on the same network as the inside of the Telecommuting Module, you are asked for the router. Enter the IP address of the router on the network where the Telecommuting Module is connected. Now enter the network address and mask of the network containing the configuring computer.

```
Static routing:
The computer allowed to configure from is not on a network local to
this unit. You must configure a static route to it. Give
the IP address of the router on the network the unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

You can choose to allow several computers to configure the Telecommuting Module, by answering no to the question:

```
Configure from a single computer? (y/n) [y] n
```

The installation program then asks for the network number. The network number is the lowest IP address in the series of numbers that includes the configuration computers (see chapter 3, Configuring 3Com VCX IP Telecommuting Module). The network mask determines the number of computers that can act as configuration computers.

```
Network number [0.0.0.0]: 10.47.2.0
Netmask/bits [255.255.255.0]: 255.255.255.0
```

If the network or partial network is not directly connected to the Telecommuting Module, you must enter the IP address of the router leading to that network. Then enter the network's address and mask.

```
Static routing:
The network allowed to configure from is not on a network local to this
unit. You must configure a static route to it. Give the
IP address of the router on the network this unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

Then enter a password.

```
Password []:
```

Finally, you are asked if you want to reset other configuration.

```
Other configuration
Do you want to reset the rest of the configuration? (y/n) [n]
```

If you answer **n**, nothing is removed. If you answer **y**, you have three alternatives to select from:

1. Clear as little as possible. This is the alternative that is used if you answer **n** to the question above. Both the preliminary and the permanent configurations will be updated with the configuration specified above.
2. Revert to the factory configuration and then apply the configuration specified above. This will affect the permanent but not the preliminary configuration.
3. Revert to the factory configuration and empty all logs and then apply the configuration specified above. Both the preliminary and the permanent configurations will be affected.

Select the update mode, which is what you want to remove.

```
Update mode (1-3) [1]:
```

All configuration is now complete. The installation program shows the configuration and asks if it is correct.

yes saves the configuration.

no runs the installation program over again.

abort ends the installation program without saving.

Now, eject the diskette from your PC and insert it into the Telecommuting Module's floppy drive. Then power up the Telecommuting Module and wait for it to boot. Then, finish configuration of the Telecommuting Module from the computer/computers specified in the installation program.

> Note that the diskette contains a command to erase certain parts of the configuration during boot when the diskette is inserted. Make sure to eject it once the Telecommuting Module has booted up to avoid future loss of data.

If you happen to forget the administrator password for the Telecommuting Module, you can insert the diskette into the Telecommuting Module again and boot it. Note that if you selected anything but 1 as the update mode, you will lose configuration when doing this.

Turning off a Telecommuting Module

Backup the Telecommuting Module configuration (just in case something should happen). You do this on the **Save/Load Configuration** page under **Administration**. Once this is done, just turn the computer off. The computer that runs 3Com VCX IP Telecommuting Module is specially designed so that you can switch it off without causing any problems in the file structure.

Remember to lock up the Telecommuting Module

The Telecommuting Module is a computer with special software, and must be protected from unauthorized physical access just as other computers performing critical tasks. A locked up Telecommuting Module protects against:

- connecting to the console
- connecting a keyboard and monitor
- changing the administrator password using the installation diskette.
- changing BIOS configuration to allow the Telecommuting Module to be booted from a diskette

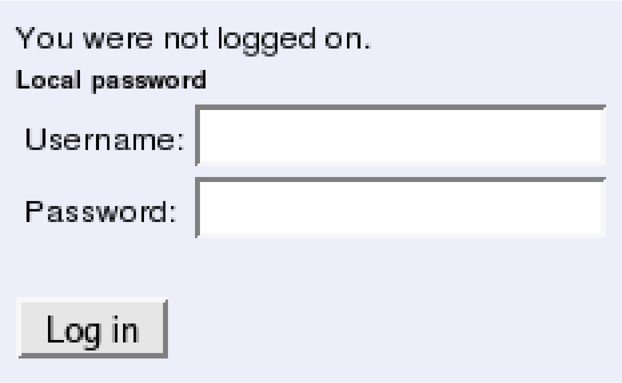
For more information about the necessary configuration, see chapter 3, Configuring 3Com VCX IP Telecommuting Module.

Chapter 3. Configuring 3Com VCX IP Telecommuting Module

You connect to your 3Com VCX IP Telecommuting Module by entering its name or IP address in the Location box of your web browser.

Logging on

Before you can configure the Telecommuting Module, you must enter your administrator username and password or RADIUS username and password. The *admin* user is predefined with complete administration privileges.



You were not logged on.

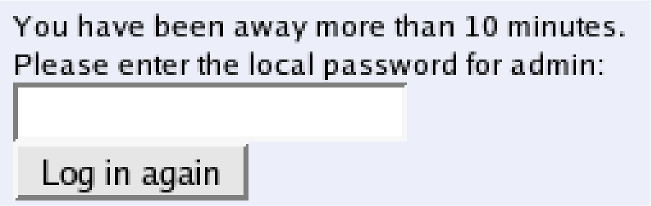
Local password

Username:

Password:

Log on again

If you have a web connection for Telecommuting Module configuration that is inactive for more than 10 minutes, you must enter the password again and click on one of the buttons **Keep changes below** and **Abandon changes below**.



You have been away more than 10 minutes.
Please enter the local password for admin:

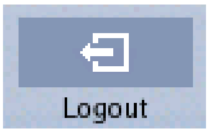
On all pages where changes have been made, the two buttons **Keep changes below** and **Abandon changes below** will be shown when you log on again. **Keep changes below** connects you to the Telecommuting Module and stores the preliminary configuration you have changed. **Abandon changes below** connects you to the Telecommuting Module and discards the changes you have made on this page.

On pages where nothing has been changed, the **Log in again** button is displayed. Enter the password and click on the button to re-connect to the Telecommuting Module.

The Telecommuting Module's encryption key is changed every 24 hours. If you have a web connection for Telecommuting Module configuration when this happens, you must enter the password again. This works in the same way as when your connection has been inactive for more than 10 minutes (see above).

Log out

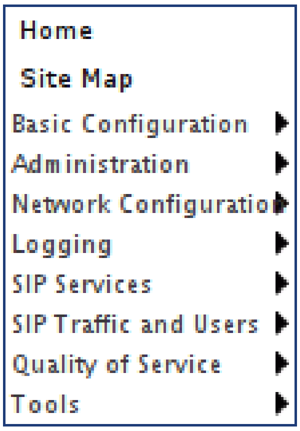
When you have finished looking at or adding settings, you should log out from the Telecommuting Module. Below the menu there is a Log out button which will end your session.



Note: You will not be logged out automatically just by directing your web browser to a different web address. You should log out using the button to make the browser forget your username and password.

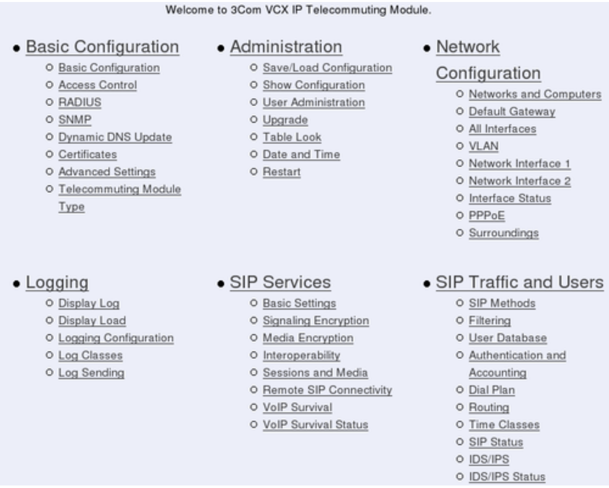
Navigation

There is a menu for quick navigation to all configuration pages. On top of the page, you also see the name of the Telecommuting Module.



Site Map

The Site Map is the first page displayed when you have logged on the Telecommuting Module. From this page, you can access **Basic Configuration**, **Administration**, **Network Configuration**, **Logging**, **SIP Services**, **SIP Traffic**, **Failover**, **Virtual Private Networks**, **Quality of Service**, and **Tools**. You can also access a special page by the text links below each category name.



Basic Configuration

Under **Basic Configuration**, select Telecommuting Module Type and the name of the Telecommuting Module. You also enter IP addresses for DNS servers. Here you also configure if the Telecommuting Module should interact with a RADIUS, a DynDNS or an SNMP server.

Administration

Under **Administration**, you store or load a configuration. You can also test your configuration to see if it works the way you planned, upgrade or reboot your Telecommuting Module, set date and time, and configure administration users and passwords.

Network Configuration

Under **Network Configuration**, you enter the Telecommuting Module's IP address, the routing for the different networks, and define groups of IP addresses which are used in various settings of the Telecommuting Module.

Logging

Under **Logging**, you specify the type of traffic you want to log/alarm and how it should be logged. You can also view the logs and the traffic load here.

SIP Services

Under **SIP Services**, you configure SIP encryption, interoperability settings, Remote SIP Connectivity and VoIP Survival.

SIP Traffic

Under **SIP Traffic**, you configure the SIP traffic and the SIP registrar in the Telecommuting Module. You can also view current user registrations and SIP sessions.

Failover

Under **Failover**, you configure the failover team and its dedicated network. You can also view the status of the other team member.

Virtual Private Networks

Under **Virtual Private Networks**, you configure the encrypted traffic between your Telecommuting Module and other VPN gateways and clients. VPN connections can be made using IPSec or PPTP.

Quality of Service

The Quality of Service module enables bandwidth limitation and prioritizing for different kinds of traffic through the Telecommuting Module. For each interface you can state a guaranteed and a maximum bandwidth for classes of traffic.

You can also set bandwidth limits for SIP calls and ensure that when there is not enough bandwidth for call media, the call will not be set up at all.

Tools

Under **Tools**, you find tools for troubleshooting the Telecommuting Module and the network.

Overview of configuration

Start by installing the Telecommuting Module as described in chapter 2, Installing 3Com VCX IP Telecommuting Module.

Select the **Telecommuting Module Type**.

The Telecommuting Module must have at least one IP address for each network card to work. A routing, or path, for each network must also be set on the interface pages under **Network Configuration**. Go to the **Networks and Computers** page and enter the networks which are using the Telecommuting Module. For a DMZ Telecommuting Module, also state the Telecommuting Module's **Surroundings**.

Go to **SIP Services** and switch the SIP module on.

Then move on to **SIP Traffic** and configure the Telecommuting Module to state how SIP requests should be processed.

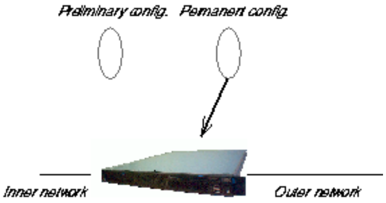
Use logging to analyze the traffic that passes through the Telecommuting Module. Choose to log locally on the Telecommuting Module, send logs to a syslog server or send them by email to an email address. Specify the type of logging wanted under **Logging**. This is also where the logs of traffic through the Telecommuting Module are viewed.

When the configuration is complete, apply it. Go to **Save/Load Configuration** under **Administration**. Select **Apply configuration**. Now the new configuration is tested. Save it permanently if it works satisfactorily. If the configuration is not satisfactory, select **Revert** or restart the Telecommuting Module. The old configuration will remain.

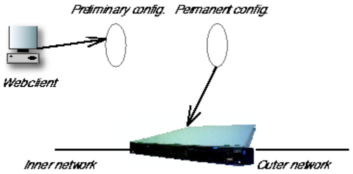
When the configuration has been applied, you should save a backup to file. Press **Save to local file** to save the configuration.

Preliminary and permanent configuration

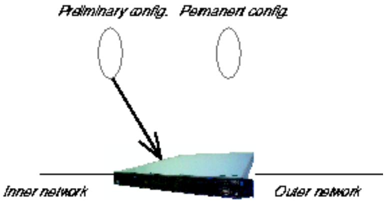
3Com VCX IP Telecommuting Module has two kinds of settings: preliminary and permanent configuration. When the Telecommuting Module is running, the permanent configuration controls the Telecommuting Module functions.



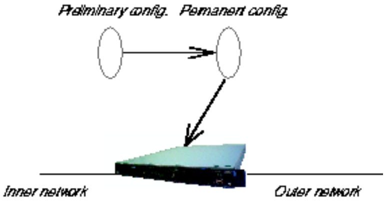
When you configure your Telecommuting Module, you are working with the preliminary configuration. As you change the preliminary configuration, the permanent configuration continues to control the Telecommuting Module functions.



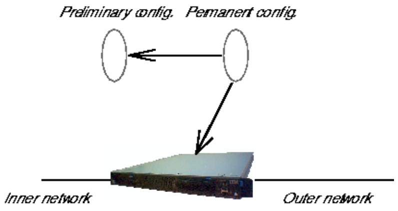
When you are done with the preliminary configuration, you can test it by selecting **Apply configuration** on the **Save/Load Configuration** page. Now the preliminary configuration controls the Telecommuting Module functions.



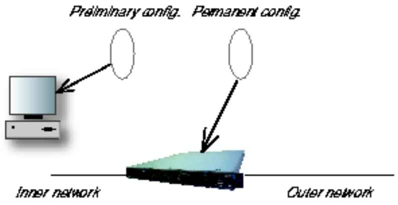
When you are satisfied with the preliminary configuration, you can apply it permanently, which copies the preliminary configuration to the permanent configuration. Now the new configuration controls the Telecommuting Module functions.



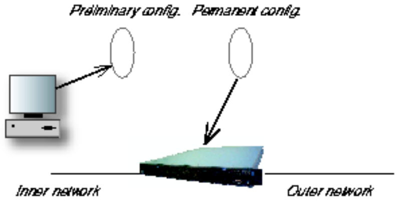
You can also copy the permanent configuration to the preliminary configuration. This does not affect the permanent configuration or the Telecommuting Module functions, which are still being run by the permanent configuration. You do this by selecting **Abort all edits** on the **Save/Load Configuration** page under **Administration**. This will discard all changes made in the preliminary configuration since last time you applied a configuration by pressing **Save configuration**.



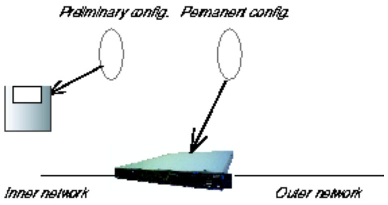
You can save the preliminary configuration to a file on your work station (the computer that is running your web browser). Select **Save to local file** or **Save config to CLI file** on the **Save/Load Configuration** page.



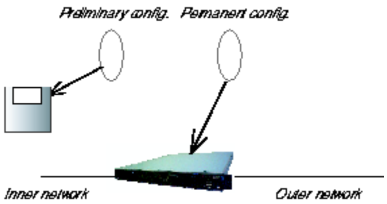
A saved configuration can be loaded to the preliminary configuration. Use Browse to search your local computer or enter path and file name in the box. When you have chosen the file you want to load, select **Load from local file** or **Load CLI file** on the **Save/Load Configuration** page.



You can save the preliminary configuration to a diskette. Insert a formatted diskette in the Telecommuting Module's floppy drive and press **Save to diskette** on the **Save/Load Configuration** page.



You can load a saved configuration to the preliminary configuration. Insert a diskette containing the saved configuration in the Telecommuting Module's floppy drive and press **Load from diskette** on the **Save/Load Configuration** page.



You can perform all of these functions on the **Save/Load Configuration** page under **Administration**.

Configuring IP addresses and masks in 3Com VCX IP Telecommuting Module

IP address

IP addresses are written as four groups of numbers with dots between them. The numbers must be between 0 and 255 (inclusive); for example, 192.168.129.17.

Mask/Bits

The binary system uses the numbers 0 and 1 to represent numbers. A binary digit is called a bit. Eight bits in the binary system can represent numbers from 0 to 255.

The mask indicates how much of the IP address is used for the network address and the computers' individual addresses, respectively. A mask consists of 8+8+8+8 = 32 bits. Below is a mask with 26 bits set to 1, which means that 26 bits of the IP address is locked to the network address and can't be changed within the network.

Bits	11111111	11111111	11111111	11000000
No.	255	255	255	192

In the 3Com VCX IP Telecommuting Module, a mask is written either as the number of bits that are 1 or as four numbers (0-255) with dots between the numbers.

Sometimes it can be convenient to give a group of computers a network name, such as Administration, or specify that only a handful of computers can change the Telecommuting Module configuration.

You can form a group of computers with a network name, if the computers have consecutive IP addresses. In order to do this, you must set the mask to indicate that the network group consists of those computers only. The lowest IP address for these computers tells the network number of the group.

This is easiest to explain with a simple example. You have 7 computers that will make up a group called Administration.

Take the nearest power of two above the number of computers you want to include: 2, 4, 8, 16, 32, 64, 128 or 256. Since you have 7 computers, 8 is the nearest. In this example, one IP address is free for future use.

Give the computers consecutive IP addresses. Make the first IP address a multiple of the power of two number you selected, but under 255. In the above example, this means 0, 8, 16, 24, 32, 40, 48 and so on, up to 248. You might choose to start with 136 (17 x 8). This would give the computers the IP addresses 196.176.1.136, 196.176.1.137, 196.176.1.138, 196.176.1.139, 196.176.1.140, 196.176.1.141, 196.176.1.142 and 196.176.1.143.

One of the IP addresses is free and can be used for an eighth computer in the future. You must enter the first IP address in the series, 196.176.1.136, in the **Network/IP address** field.

Now you must set the mask so that only the computers with these eight IP addresses are included in this network. Take 256 and subtract the number of IP addresses in the named network. In the example, we would have 256-8 = 248. The complete mask is 255.255.255.248.

Now you have created a group of computers (IP addresses) that you can give a single name, such as Administration.

Table of netmasks.

No. of computers	Mask	Bits
1	255.255.255.255	32
2	255.255.255.254	31
4	255.255.255.252	30
8	255.255.255.248	29
16	255.255.255.240	28
32	255.255.255.224	27
64	255.255.255.192	26
128	255.255.255.128	25
256	255.255.255.0	24

See appendix C, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols, for more information on netmasks.

Name queries in 3Com VCX IP Telecommuting Module

A Telecommuting Module should be as independent of other computers as possible. At the same time, the person who changes the configuration of the Telecommuting Module may want to use names for the computers instead of IP addresses. Also, the SIP module needs to look up names of SIP domains. This makes it necessary to use a DNS (name server) for SIP requests.

There are three instances when 3Com VCX IP Telecommuting Module uses a DNS server:

- When it receives a SIP request for a SIP domain.

  The results of these DNS queries are stored for a short while in the Telecommuting Module.

- When you change names/IP addresses and save the page.

The results of these DNS queries are stored in the Telecommuting Module.

- When you click on **Look up all IP addresses again**.

  The results of these DNS queries are stored in the Telecommuting Module.

- When negotiations start for an IPsec tunnel where the IPsec peer has a dynamic DNS name.

  The results of these DNS queries are stored in the Telecommuting Module.

3Com VCX IP Telecommuting Module is dependent of a working name server for the SIP functions. However, it doesn't automatically look up IP addresses in the configuration, which makes it necessary to click on **Look up all IP addresses again** every time a computer changes its IP address.

When you enter IP addresses in the Telecommuting Module, they are not updated automatically. If you change a name/IP address in a row, the row is updated when you click on **Save**, switch to another page of the Telecommuting Module user interface, or click on **Look up all IP addresses again**.

Part II. How To

In the How To part, you find step-by-step descriptions for many common configurations for the Telecommuting Module. You also find references to relevant chapters in Part III, Description of 3Com VCX IP Telecommuting Module settings.

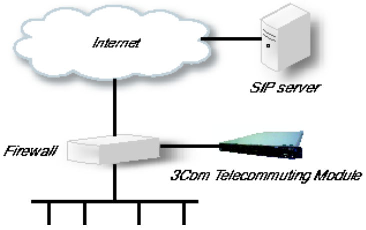
Chapter 4. How To Configure SIP

3Com VCX IP Telecommuting Module provides a lot of SIP possibilities. In this chapter, the most common SIP setups are setup with step-by-step instructions for the configuration.

DMZ Telecommuting Module, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the Telecommuting Module SIP function is only used to traverse NAT.

Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.

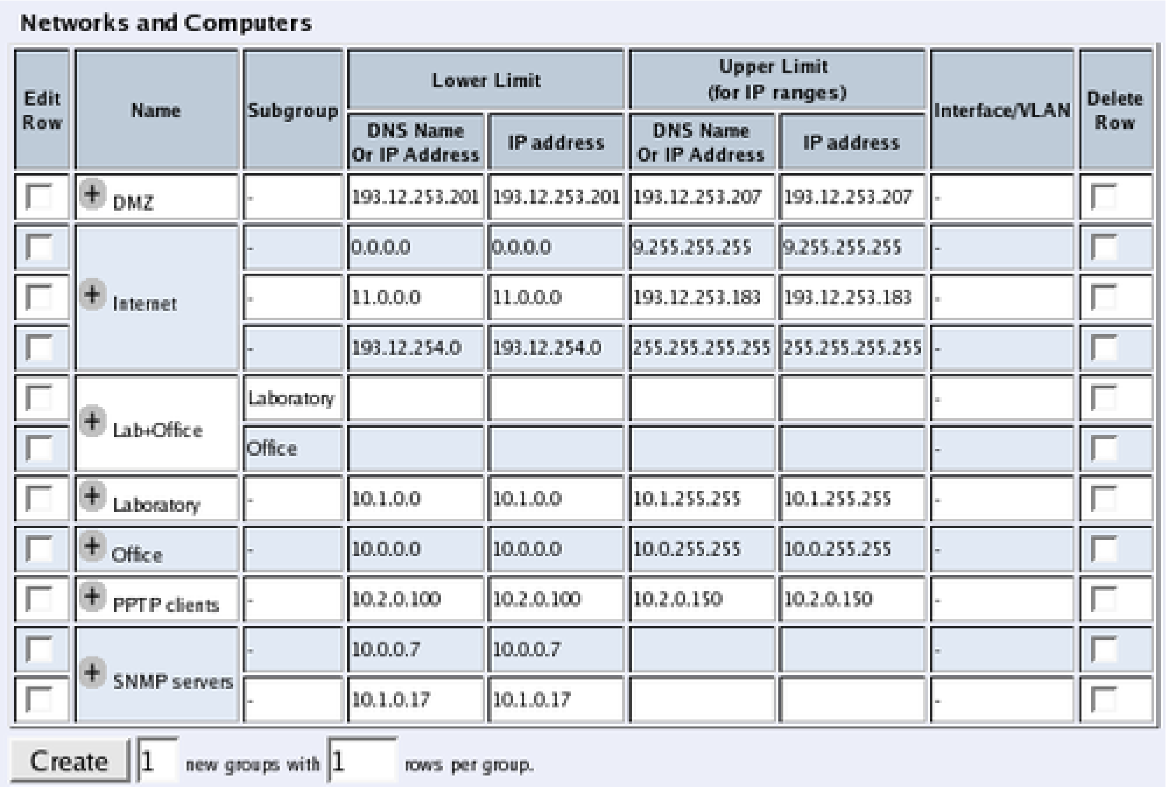


Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

Networks and Computers

The Telecommuting Module must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name Or IP Address	IP address	DNS Name Or IP Address	IP address		
□	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	□
□	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	□
□		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	□
□		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	□
□	+ Lab+Office	Laboratory					-	□
□		Office					-	□
□	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	□
□	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	□
□	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	□
□	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	□
□		-	10.1.0.17	10.1.0.17			-	□

Create [1] new groups with [1] rows per group.

Surroundings

To make the Telecommuting Module aware of the network structure, the networks defined above should be listed on the **Surroundings** page.

Settings in the **Surroundings** table are only required when the Telecommuting Module has been made the **DMZ** (or **LAN**) type.

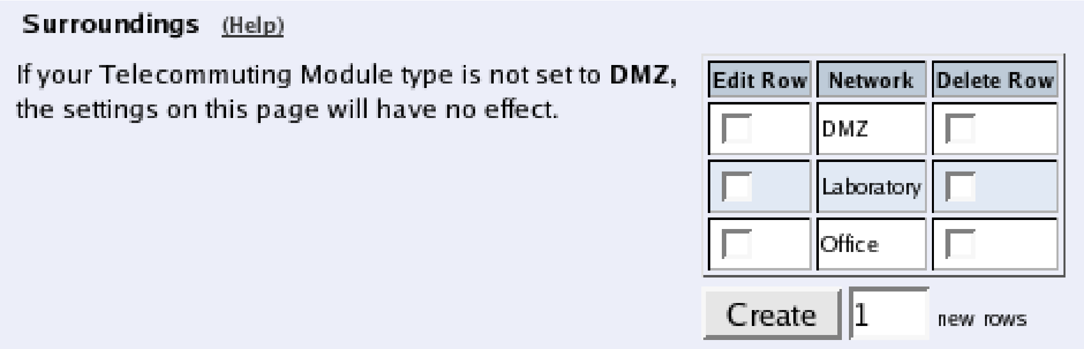
The Telecommuting Module must know what the networks around it looks like. On this page, you list all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network. When you are finished, there should be one line for each of your firewall's network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Surroundings, no ports for RTP sessions will be opened, since the Telecommuting Module assumes that they are both on the same side of the firewall.

For DMZ and LAN SIParators, at least one network should be listed here. If no networks are listed, the Telecommuting Module will not perform NAT for any traffic.



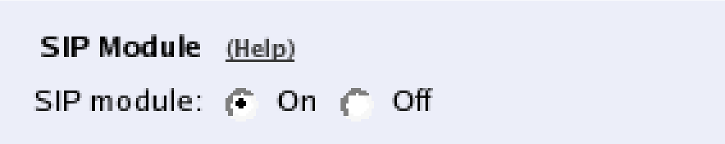
Surroundings (Help)

If your Telecommuting Module type is not set to **DMZ,** the settings on this page will have no effect.

Edit Row	Network	Delete Row
☐	DMZ	☐
☐	Laboratory	☐
☐	Office	☐

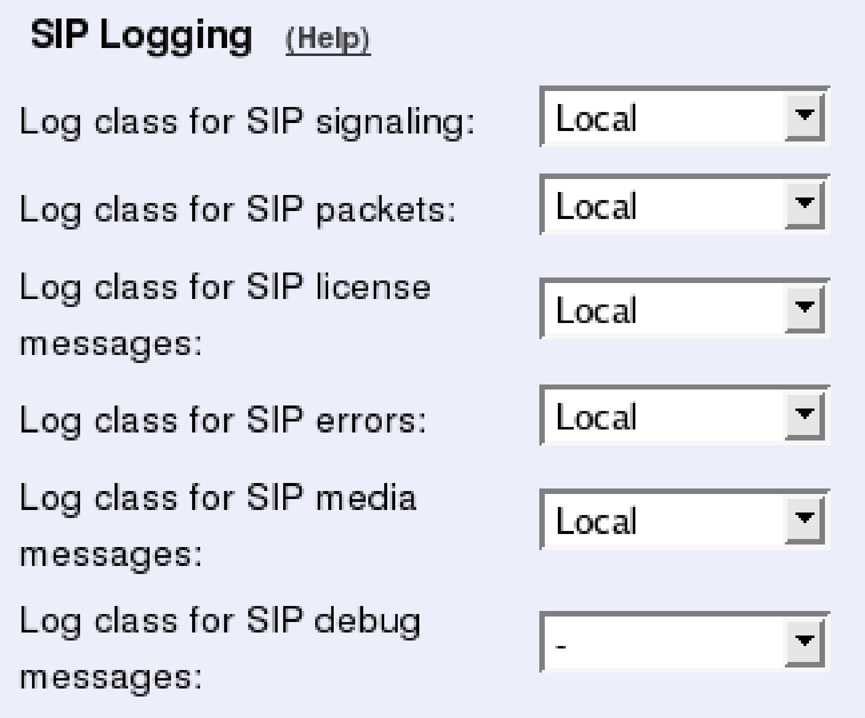
Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off

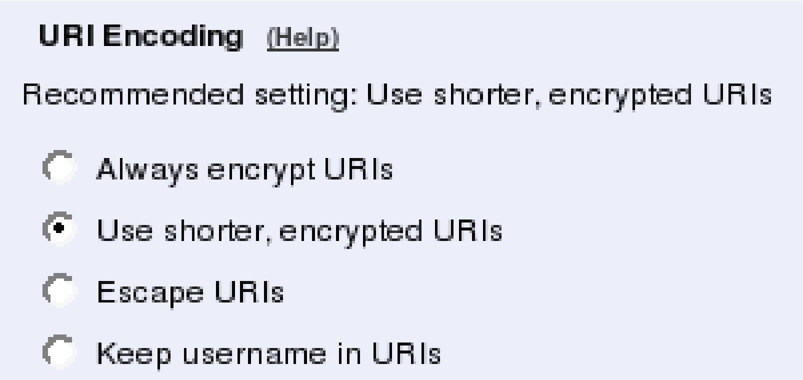


SIP Logging (Help)

Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

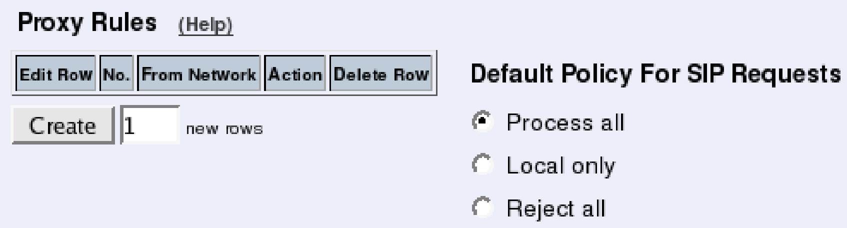
○ Escape URIs

○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

Create [1] new rows

Default Policy For SIP Requests

● Process all

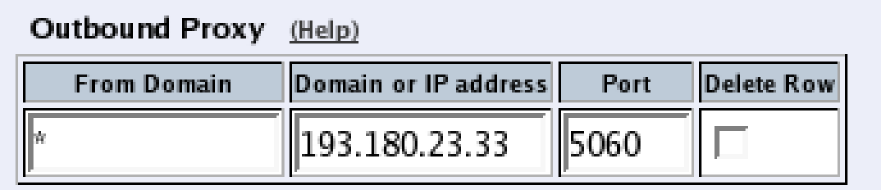
○ Local only

○ Reject all

Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

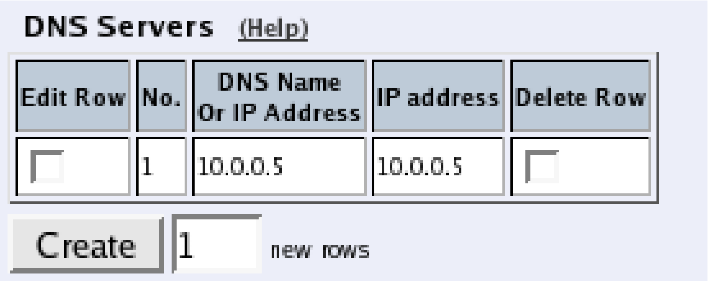


Outbound Proxy (Help)

From Domain	Domain or IP address	Port	Delete Row
*	193.180.23.33	5060	□

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

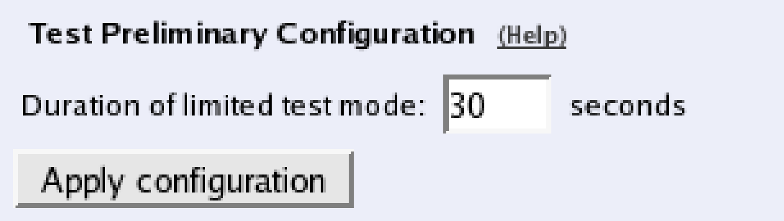


DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Save/Load Configuration

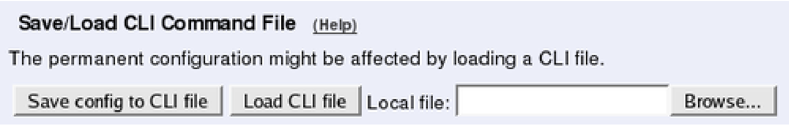
Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

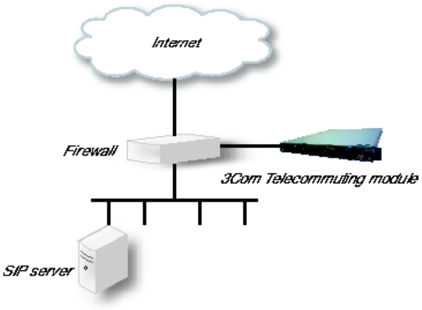
Local file:

DMZ Telecommuting Module, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the Telecommuting Module. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the Telecommuting Module, which in turn will forward the SIP traffic to the server.

Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.

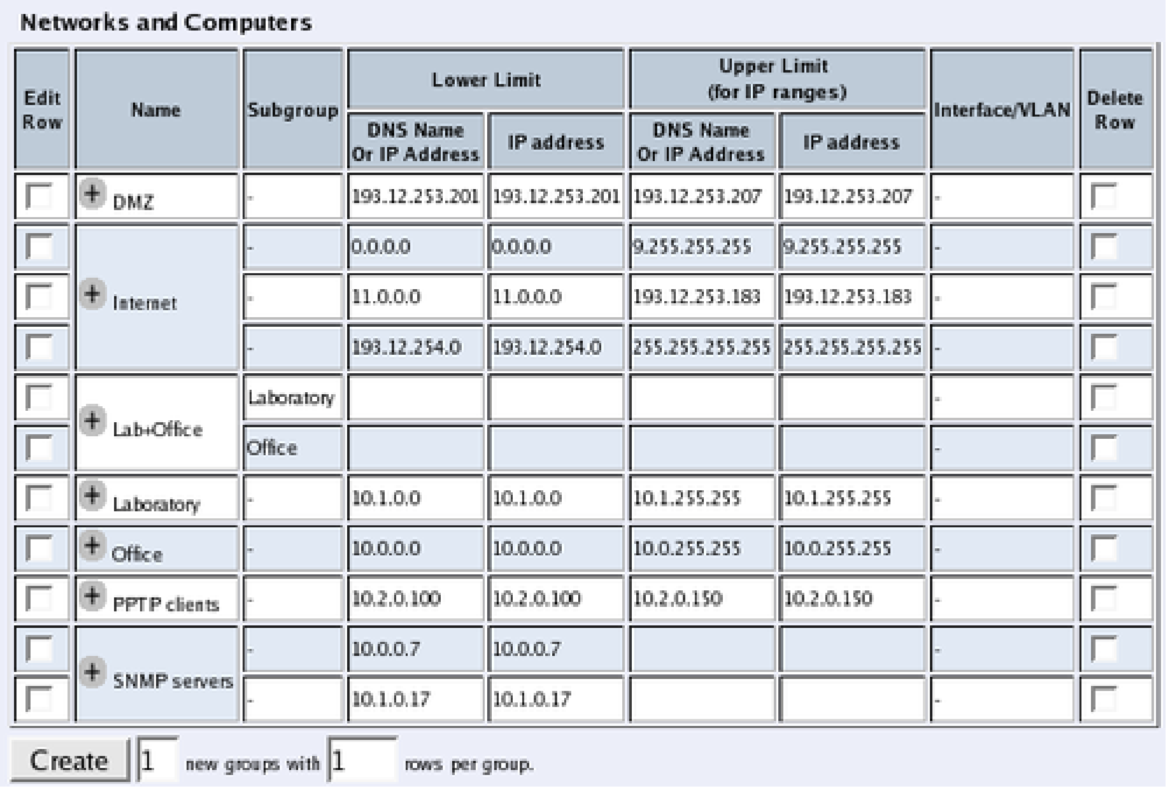


Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

Networks and Computers

The Telecommuting Module must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name Or IP Address	IP address	DNS Name Or IP Address	IP address		
□	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	□
□	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	□
□		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	□
□		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	□
□	+ Lab+Office	Laboratory					-	□
□		Office					-	□
□	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	□
□	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	□
□	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	□
□	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	□
□		-	10.1.0.17	10.1.0.17			-	□

Create 1 new groups with 1 rows per group.

Surroundings

To make the Telecommuting Module aware of the network structure, the networks defined above should be listed on the **Surroundings** page.

Settings in the **Surroundings** table are only required when the Telecommuting Module has been made the **DMZ** (or **LAN**) type.

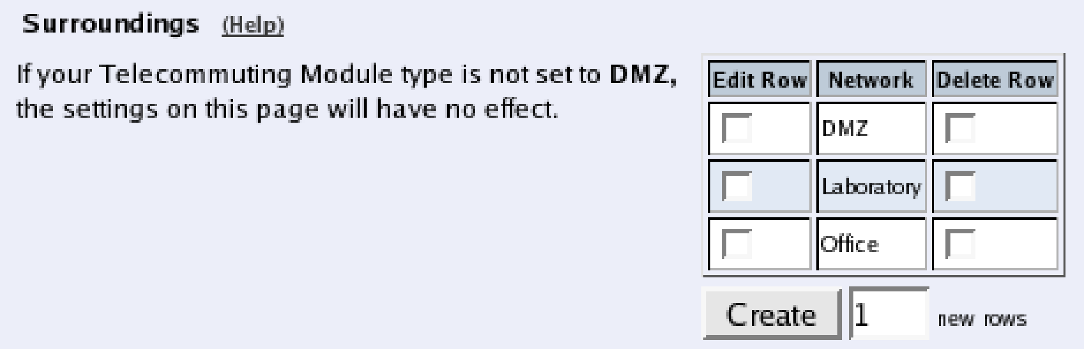
The Telecommuting Module must know what the networks around it looks like. On this page, you list all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network. When you are finished, there should be one line for each of your firewall’s network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Surroundings, no ports for RTP sessions will be opened, since the Telecommuting Module assumes that they are both on the same side of the firewall.

For DMZ and LAN SIParators, at least one network should be listed here. If no networks are listed, the Telecommuting Module will not perform NAT for any traffic.



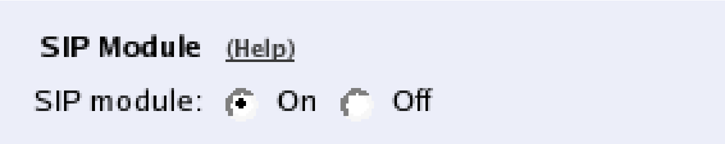
Surroundings (Help)

If your Telecommuting Module type is not set to **DMZ**, the settings on this page will have no effect.

Edit Row	Network	Delete Row
□	DMZ	□
□	Laboratory	□
□	Office	□

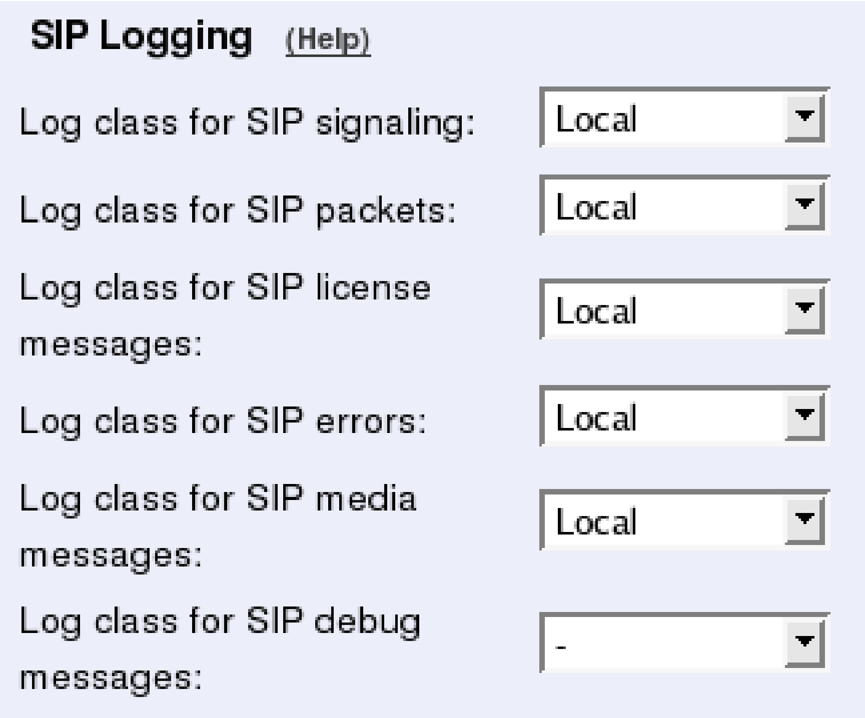
Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off



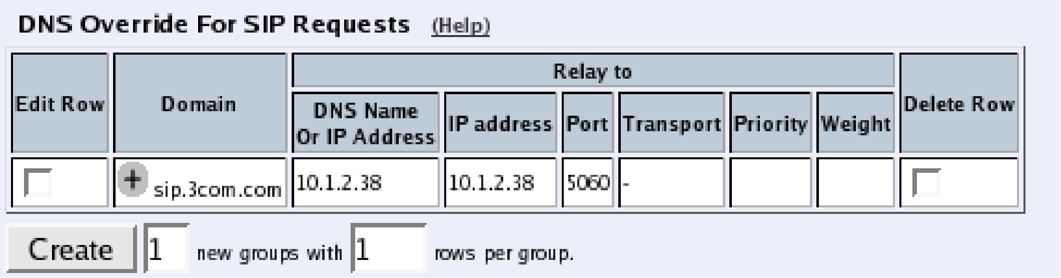
SIP Logging (Help)

Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the Telecommuting Module, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The Telecommuting Module will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.



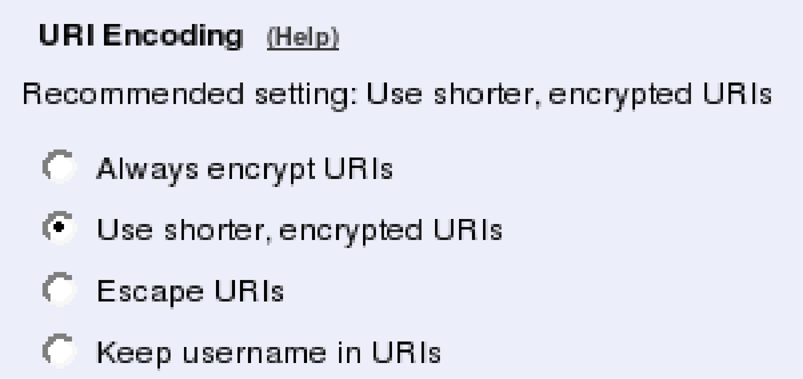
DNS Override For SIP Requests (Help)

Edit Row	Domain	Relay to						Delete Row
		DNS Name Or IP Address	IP address	Port	Transport	Priority	Weight	
☐	+ sip.3com.com	10.1.2.38	10.1.2.38	5060	-			☐

Create [1] new groups with [1] rows per group.

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

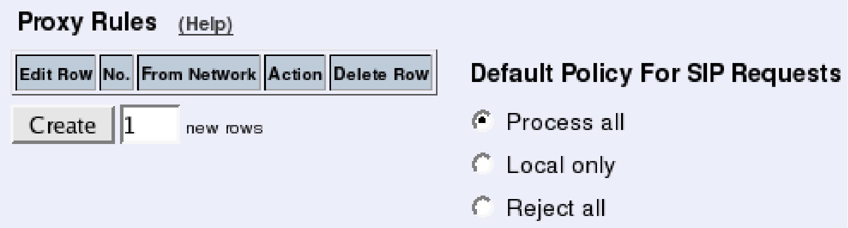
○ Escape URIs

○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

Create [1] new rows

Default Policy For SIP Requests

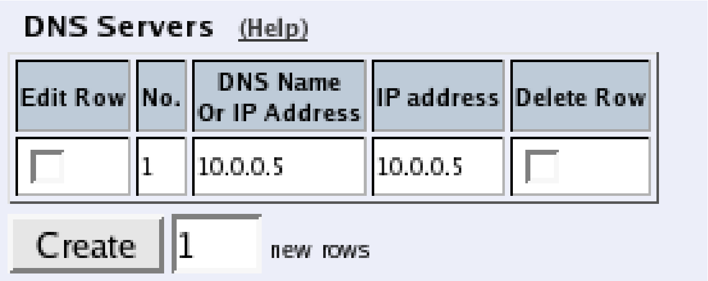
● Process all

○ Local only

○ Reject all

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

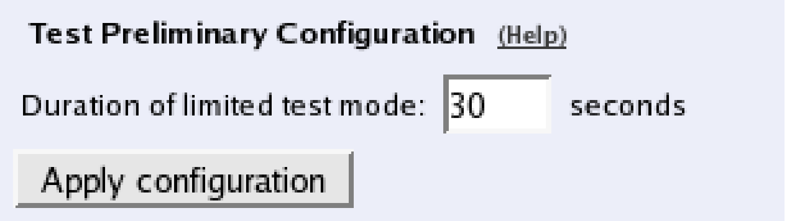


DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Save/Load Configuration

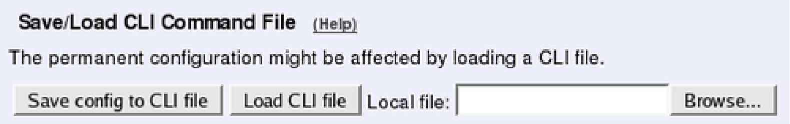
Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



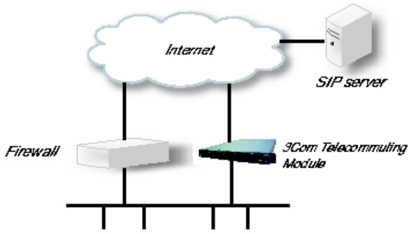
Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Standalone Telecommuting Module, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the Telecommuting Module SIP function is only used to traverse NAT.

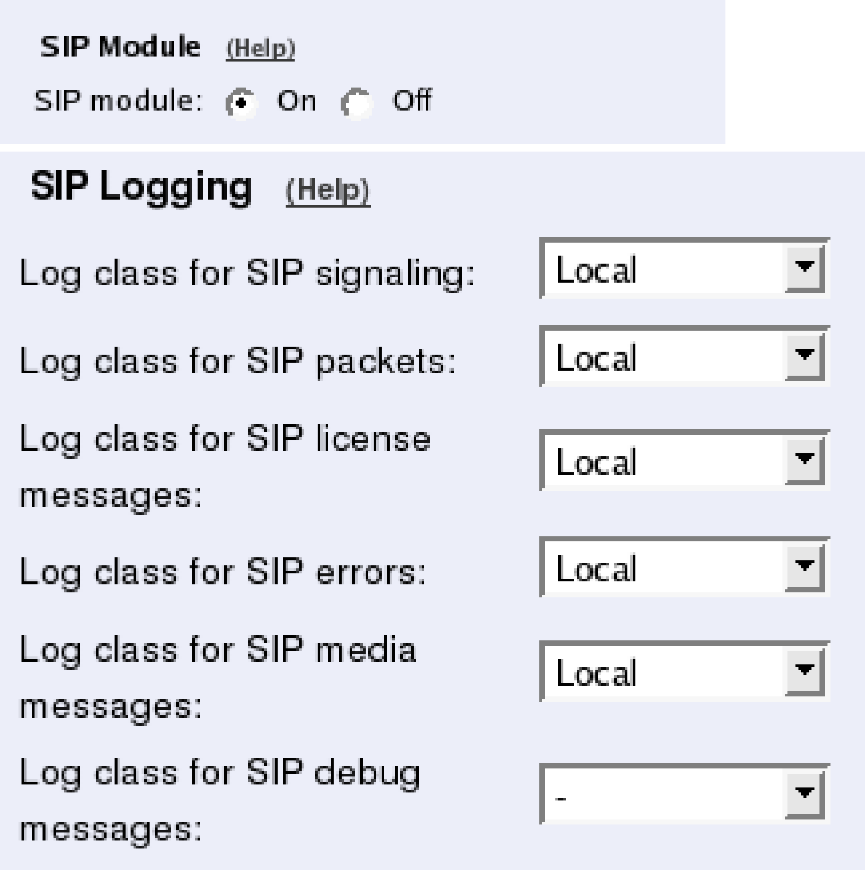
Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off

SIP Logging (Help)

Log class for SIP signaling: Local

Log class for SIP packets: Local

Log class for SIP license messages: Local

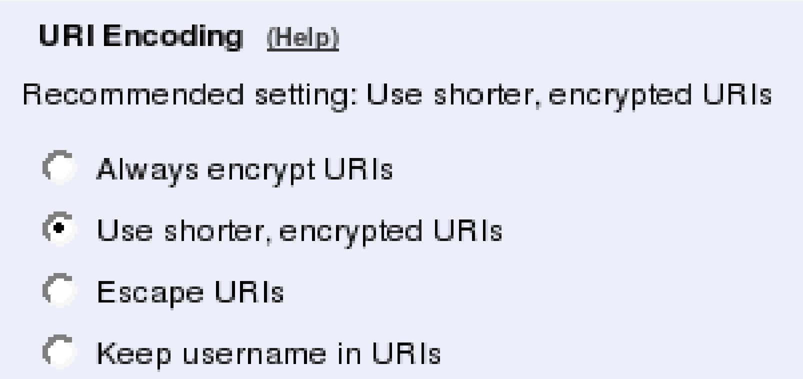
Log class for SIP errors: Local

Log class for SIP media messages: Local

Log class for SIP debug messages: -

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

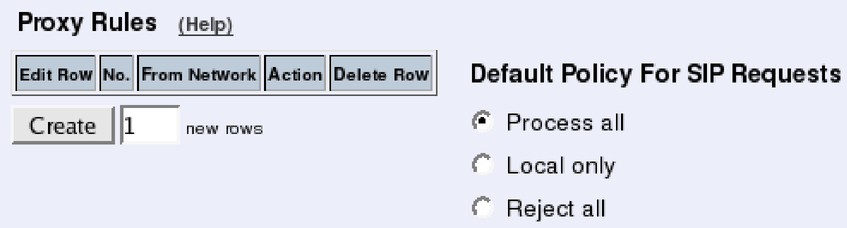
○ Escape URIs

○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

Default Policy For SIP Requests

● Process all

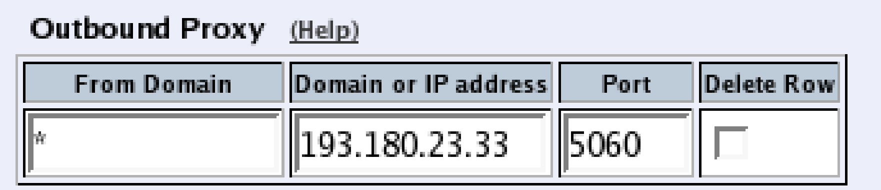
○ Local only

○ Reject all

Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

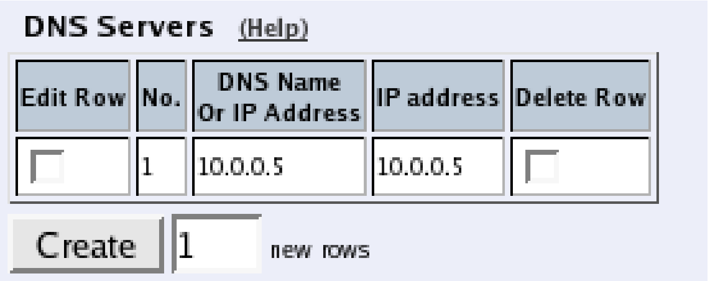


Outbound Proxy (Help)

From Domain	Domain or IP address	Port	Delete Row
*	193.180.23.33	5060	□

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.



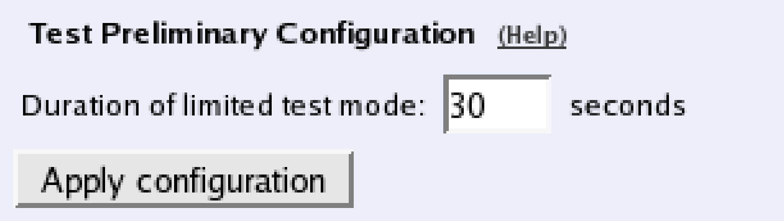
DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Create 1 new rows

Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

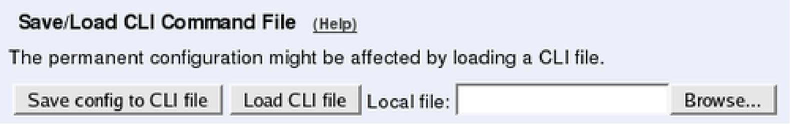


Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

Apply configuration

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file | Load CLI file | Local file: | Browse...

Client Settings

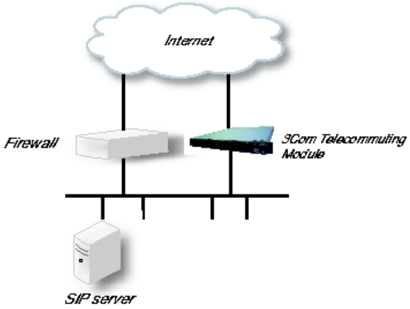
SIP clients will use the Telecommuting Module as their outgoing SIP proxy and the SIP domain as the registrar.

Standalone Telecommuting Module, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the Telecommuting Module. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the Telecommuting Module, which in turn will forward the SIP traffic to the server.

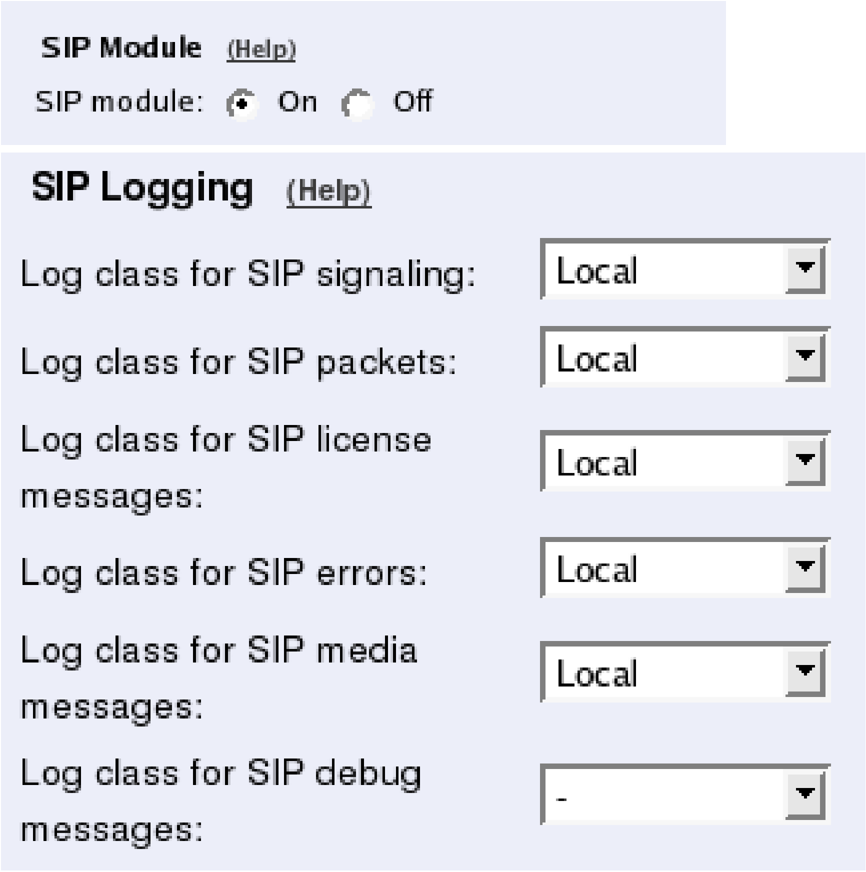
Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off

SIP Logging (Help)

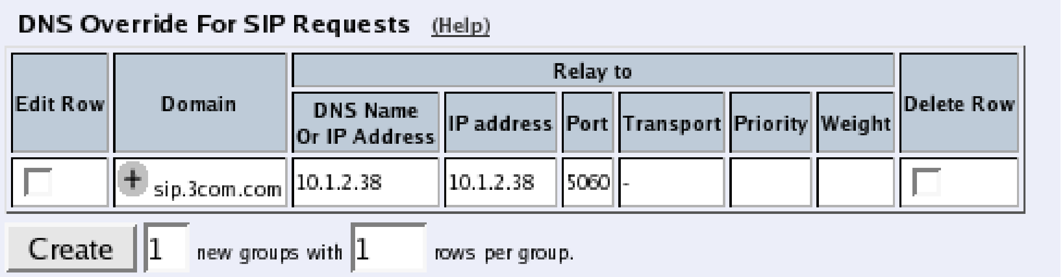
Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the Telecommuting Module, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The Telecommuting

Module will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.



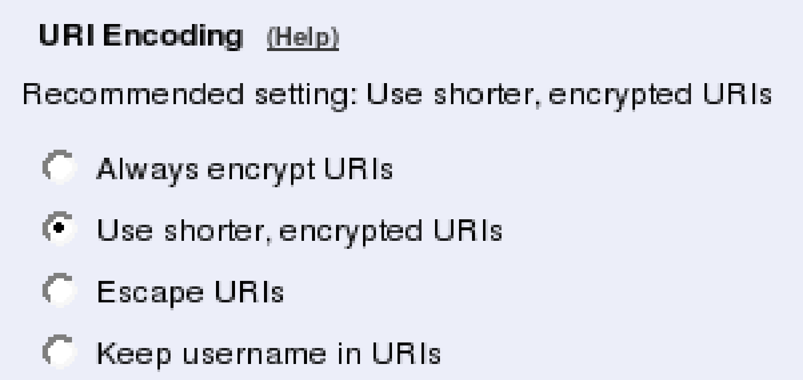
DNS Override For SIP Requests (Help)

Edit Row	Domain	Relay to						Delete Row
		DNS Name Or IP Address	IP address	Port	Transport	Priority	Weight	
□	+ sip.3com.com	10.1.2.38	10.1.2.38	5060	-			□

Create 1 new groups with 1 rows per group.

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

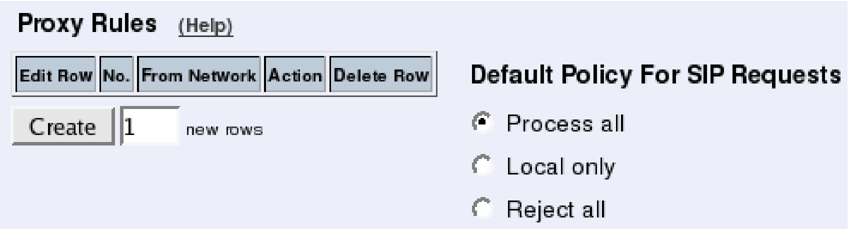
Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs
● Use shorter, encrypted URIs
○ Escape URIs
○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

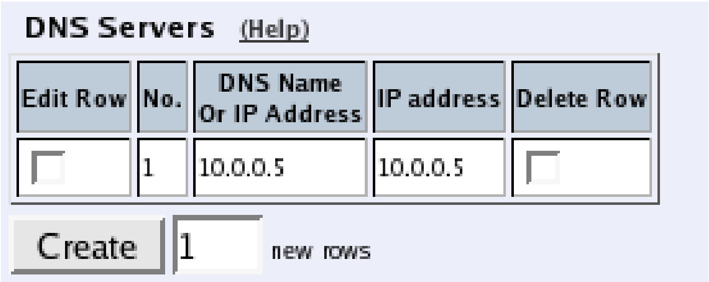
Create 1 new rows

Default Policy For SIP Requests

● Process all
○ Local only
○ Reject all

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.



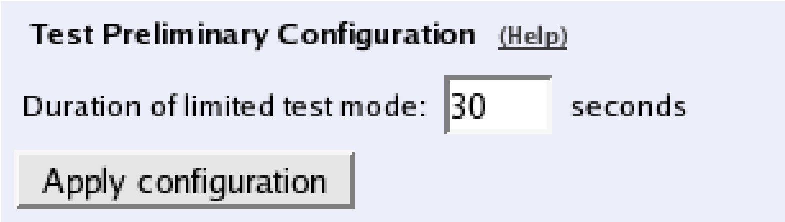
DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
☐	1	10.0.0.5	10.0.0.5	☐

Create 1 new rows

Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

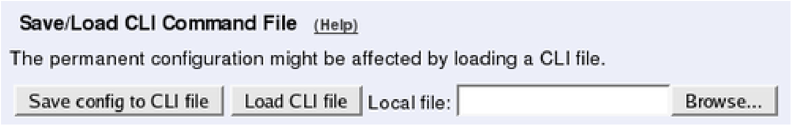


Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

Apply configuration

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file | Load CLI file | Local file: | Browse...

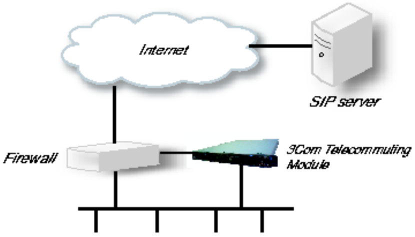
Client Settings

SIP clients will use the Telecommuting Module as their outgoing SIP proxy and the SIP domain as the registrar.

DMZ/LAN Telecommuting Module, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the Telecommuting Module SIP function is only used to traverse NAT.

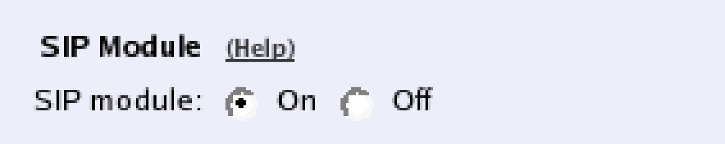
Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

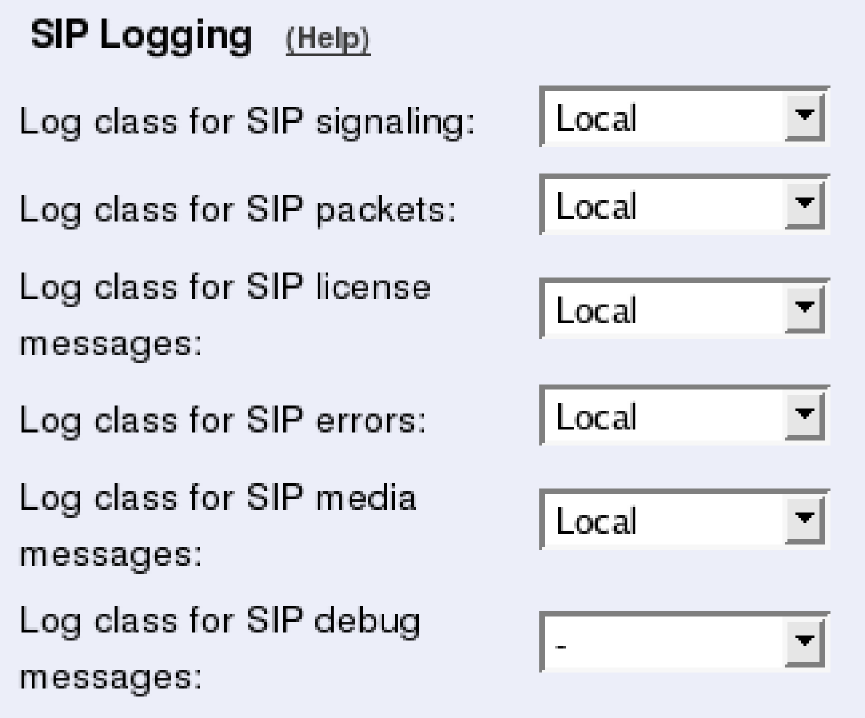
Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off

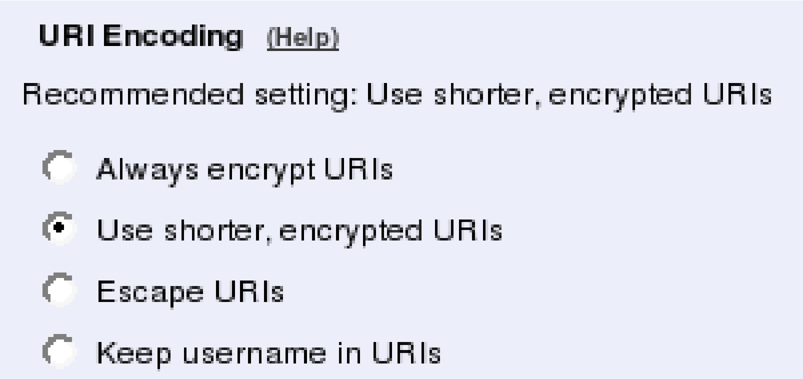


SIP Logging (Help)

Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

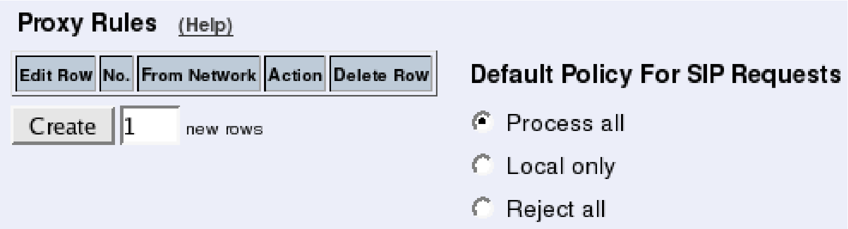
○ Escape URIs

○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

Create 1 new rows

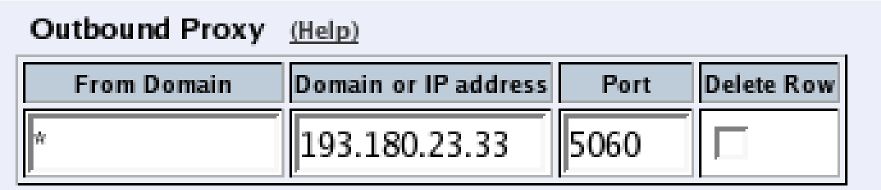
Default Policy For SIP Requests

● Process all
○ Local only
○ Reject all

Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

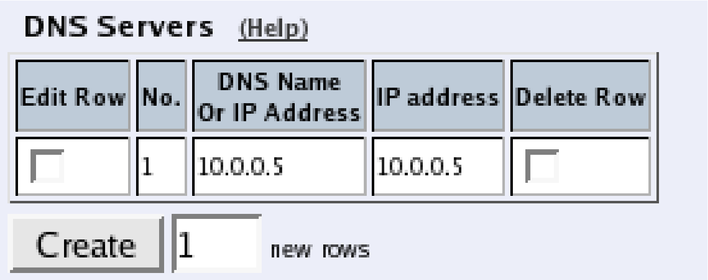


Outbound Proxy (Help)

From Domain	Domain or IP address	Port	Delete Row
*	193.180.23.33	5060	□

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.



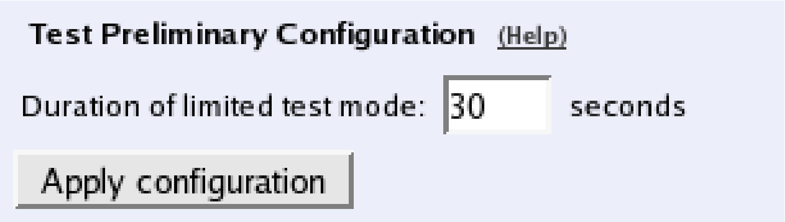
DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Create 1 new rows

Save/Load Configuration

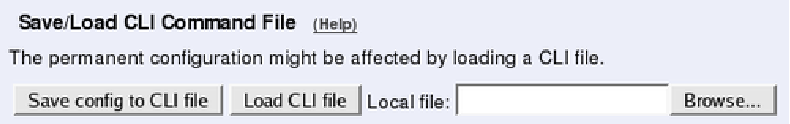
Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

Client Settings

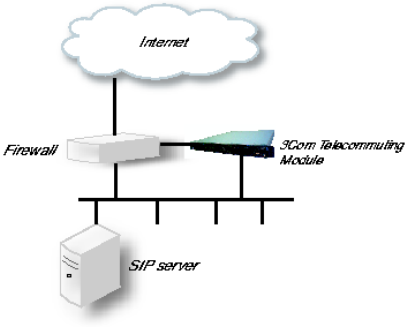
SIP clients will use the Telecommuting Module as their outgoing SIP proxy and the SIP domain as the registrar.

DMZ/LAN Telecommuting Module, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the Telecommuting Module. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the Telecommuting Module, which in turn will forward the SIP traffic to the server.

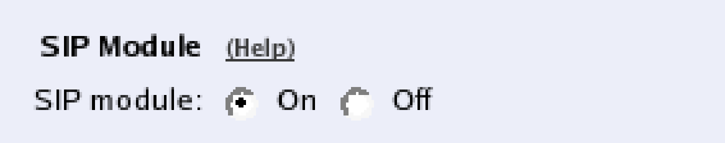
Note that the Telecommuting Module must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

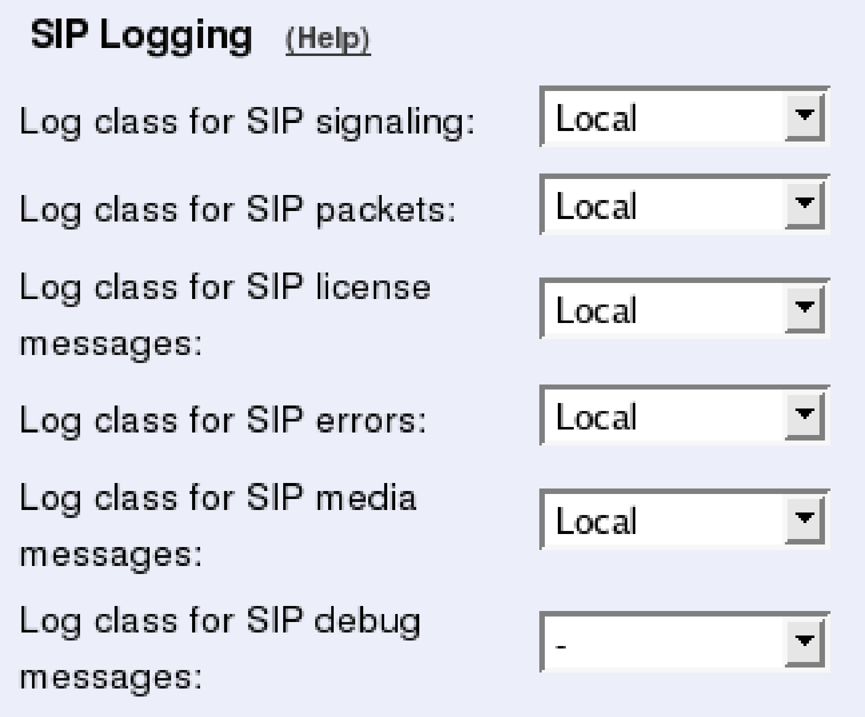
Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off



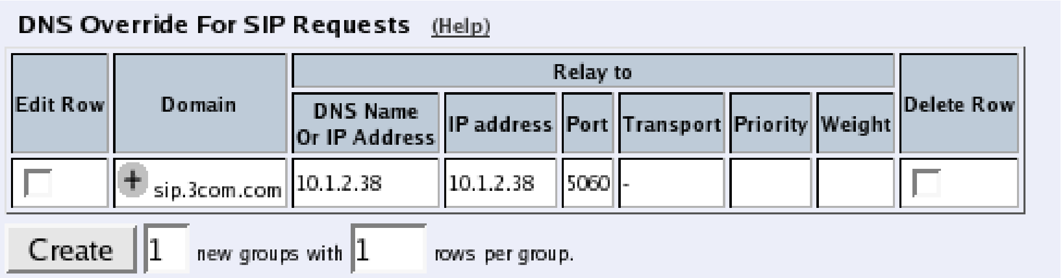
SIP Logging (Help)

Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the Telecommuting Module, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The Telecommuting Module will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.



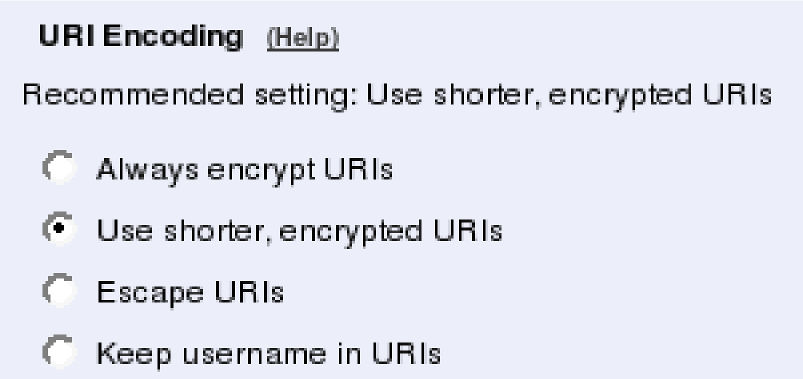
DNS Override For SIP Requests (Help)

Edit Row	Domain	Relay to						Delete Row
		DNS Name Or IP Address	IP address	Port	Transport	Priority	Weight	
□	+ sip.3com.com	10.1.2.38	10.1.2.38	5060	-			□

Create 1 new groups with 1 rows per group.

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".



URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

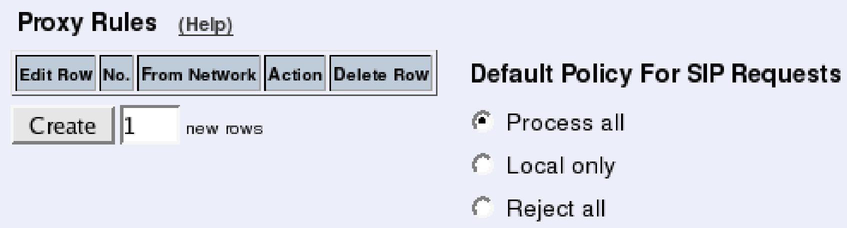
○ Escape URIs

○ Keep username in URIs

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row

Default Policy For SIP Requests

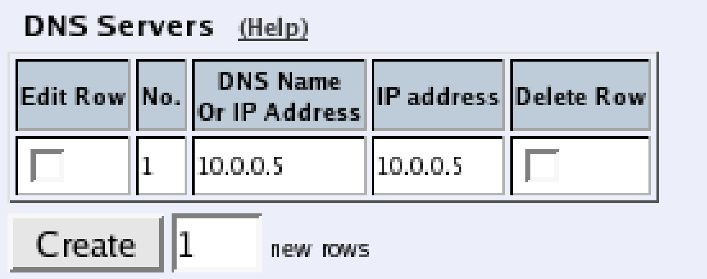
● Process all

○ Local only

○ Reject all

Basic Configuration

If no Outbound proxy is entered, the Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

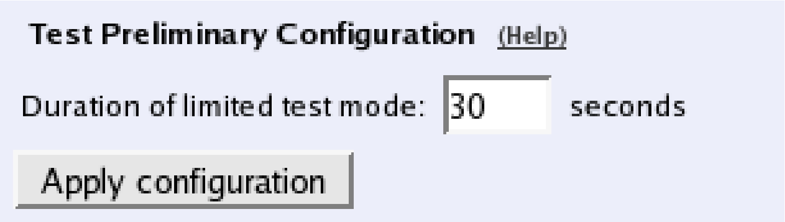


DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Save/Load Configuration

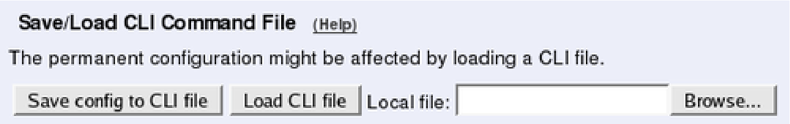
Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

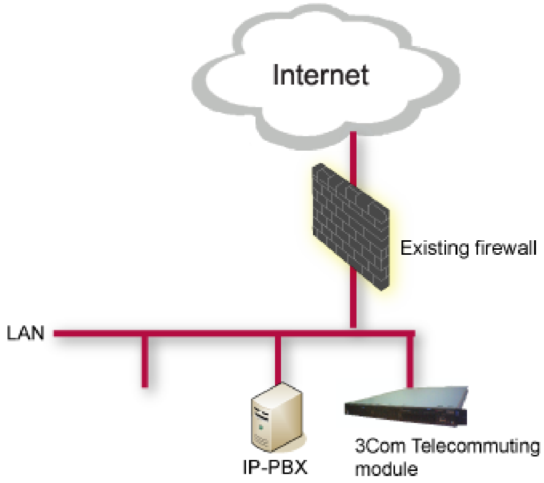
Client Settings

SIP clients will use the Telecommuting Module as their outgoing SIP proxy and the SIP domain as the registrar.

LAN Telecommuting Module

For various reasons, you might want to use a separate SIP server instead of the built-in server in the Telecommuting Module. That SIP server would be located on the inside or maybe on a DMZ.

With the LAN Telecommuting Module, you connect the Telecommuting Module to a NATed network.



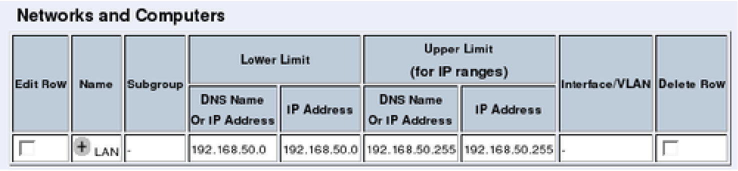
Here are the settings needed for this. It is assumed that the Telecommuting Module already has a network configuration. Only the additional SIP settings are listed.

Networks and Computers

The Telecommuting Module must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name Or IP Address	IP Address	DNS Name Or IP Address	IP Address		
□	⊕ LAN	-	192.168.50.0	192.168.50.0	192.168.50.255	192.168.50.255	-	□

Surroundings

To make the Telecommuting Module aware of the network structure, the networks defined above should be listed on the **Surroundings** page.

Settings in the **Surroundings** table are only required when the Telecommuting Module has been made the **DMZ** (or **LAN**) type.

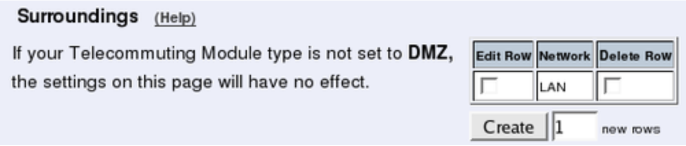
The Telecommuting Module must know what the networks around it looks like. On this page, you list all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network. When you are finished, there should be one line for each of your firewall's network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Surroundings, no ports for RTP sessions will be opened, since the Telecommuting Module assumes that they are both on the same side of the firewall.

For DMZ and LAN SIParators, at least one network should be listed here. If no networks are listed, the Telecommuting Module will not perform NAT for any traffic.



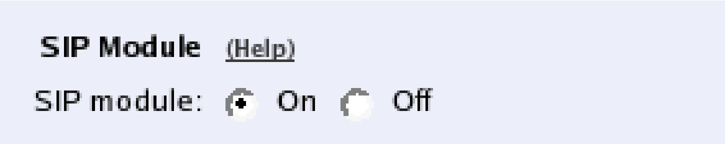
Surroundings (Help)

If your Telecommuting Module type is not set to **DMZ,** the settings on this page will have no effect.

Edit Row	Network	Delete Row
□	LAN	□

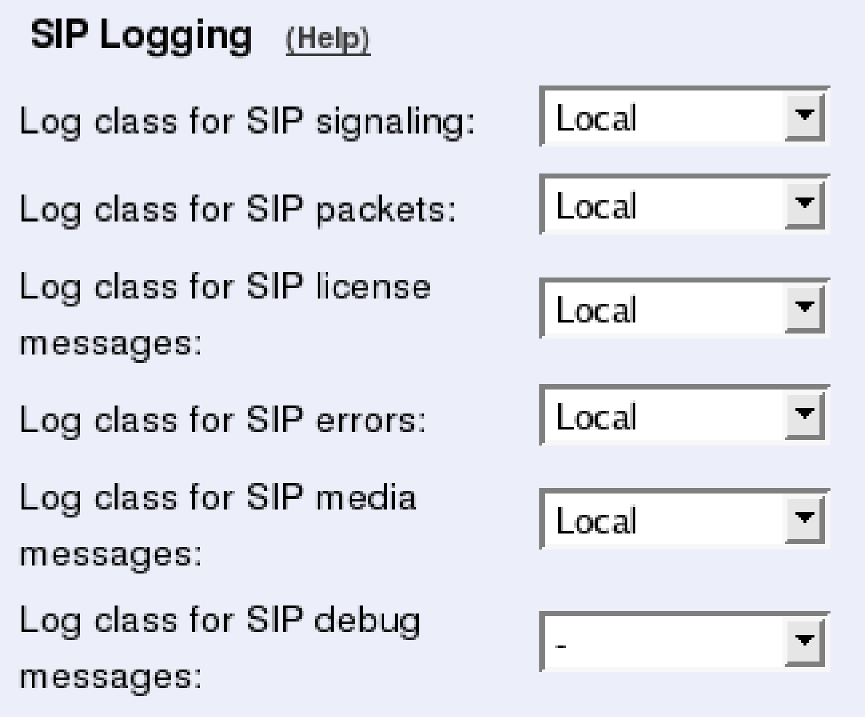
Basic Settings

Go to the **Basic Settings** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.



SIP Module (Help)

SIP module: ● On ○ Off



SIP Logging (Help)

Log class for SIP signaling: Local

Log class for SIP packets: Local

Log class for SIP license messages: Local

Log class for SIP errors: Local

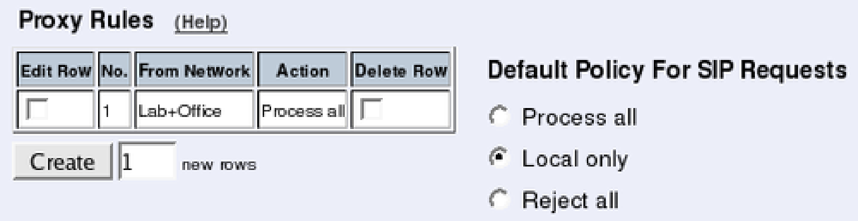
Log class for SIP media messages: Local

Log class for SIP debug messages: -

Filtering

To allow SIP traffic through the Telecommuting Module, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the Telecommuting Module does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row
□	1	Lab+Office	Process all	□

Create 1 new rows

Default Policy For SIP Requests

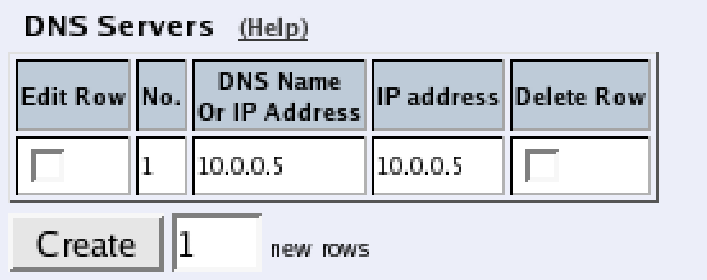
○ Process all

● Local only

○ Reject all

Basic Configuration

The Telecommuting Module must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.



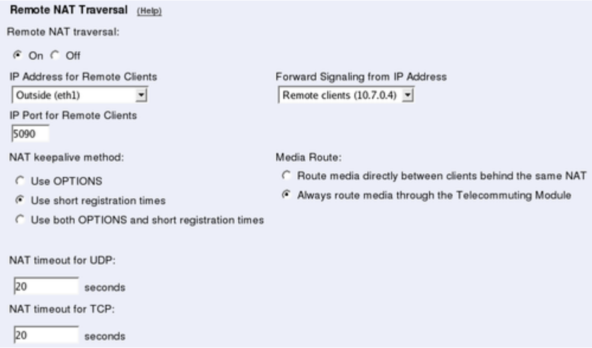
DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

Create 1 new rows

Remote SIP Connectivity

If you have remote SIP clients behind other NAT boxes, you need to activate **Remote NAT Traversal**.



Remote NAT Traversal (Help)

Remote NAT traversal:

● On ○ Off

IP Address for Remote Clients: Outside (eth1)

Forward Signaling from IP Address: Remote clients (10.7.0.4)

IP Port for Remote Clients: 5090

NAT keepalive method:

○ Use OPTIONS
● Use short registration times
○ Use both OPTIONS and short registration times

Media Route:

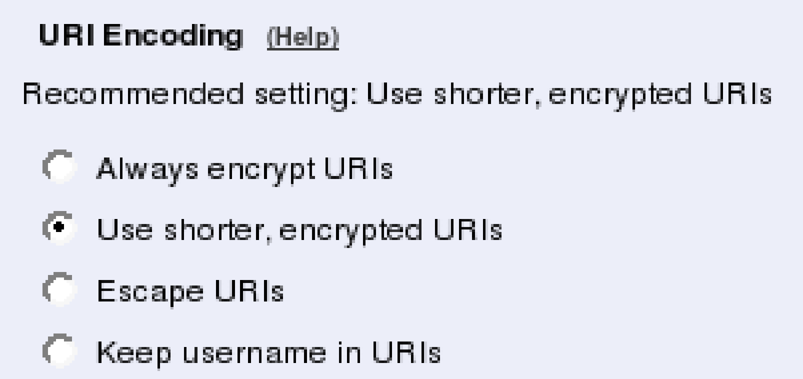
○ Route media directly between clients behind the same NAT
● Always route media through the Telecommuting Module

NAT timeout for UDP: 20 seconds

NAT timeout for TCP: 20 seconds

Interoperability

You need to set the **URI Encoding** settings on the **Interoperability** page to "Use shorter, encrypted URIs".

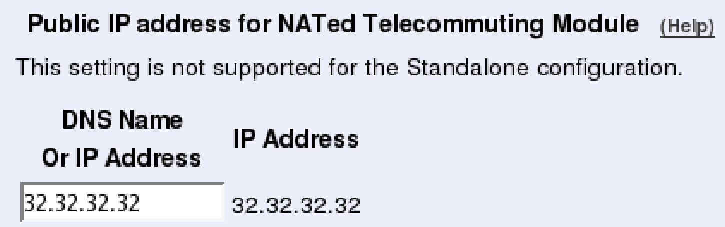


URI Encoding (Help)

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs
● Use shorter, encrypted URIs
○ Escape URIs
○ Keep username in URIs

You need to enter the public IP that corresponds to the Telecommuting Module under **Public IP address for NATed Telecommuting Module**. This will make the Telecommuting Module able to rewrite outgoing SIP packets properly.



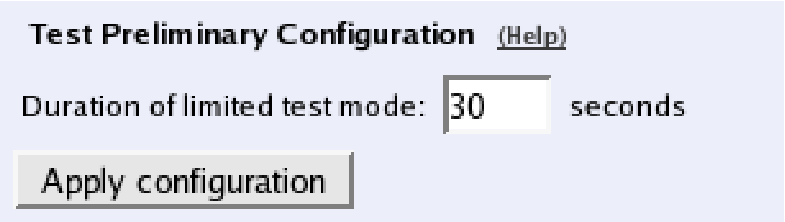
Public IP address for NATed Telecommuting Module (Help)

This setting is not supported for the Standalone configuration.

DNS Name Or IP Address	IP Address
32.32.32.32	32.32.32.32

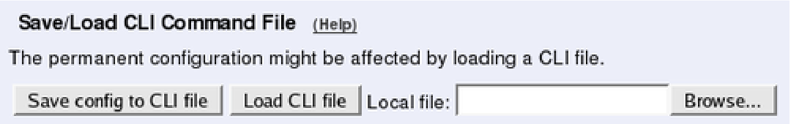
Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Duration of limited test mode: 30 seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



The permanent configuration might be affected by loading a CLI file.

The Firewall

The firewall in front of the LAN Telecommuting Module must be configured in this way:

- There must be a static IP address that can be mapped to the Telecommuting Module's private IP address. All traffic to this IP address must be forwarded to the SIParator.
- When the firewall forwards traffic to the Telecommuting Module, it must not NAT this traffic, i.e. the Telecommuting Module needs to see the original sender IP address.
- All outgoing traffic from the Telecommuting Module should be allowed through the firewall.
- For outgoing traffic from the Telecommuting Module, the firewall needs to use the same IP address as above when performing NAT. If another IP address is used, some SIP signalling will go awry, and Remote SIP Connectivity will not always work properly.
- For outgoing traffic from the Telecommuting Module the firewall must not change sender port when performing NAT. If it does change port, Remote SIP Connectivity will not always work properly.

Chapter 5. How To Configure Advanced SIP

3Com VCX IP Telecommuting Module provides a lot of SIP possibilities. In this chapter, some advanced SIP setups will be presented with step-by-step instructions for the configuration.

How To Use Your SIP Operator Account Via 3Com VCX IP Telecommuting Module

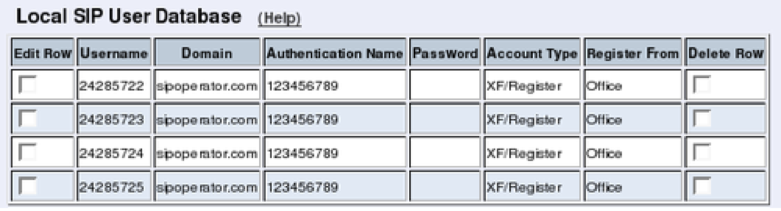
This is how to configure your Telecommuting Module to register at your SIP operator, and to use that SIP account for your local users.

This feature is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Enter your SIP operator account on the **Local Registrar** page. You enter the username and password from the operator, and select the *XF/Register* account type. This account type will make the Telecommuting Module register at the SIP operator with the credentials you enter.

Some operators don't require registration. In this case, select the *XF* account type instead.

You can select any network in the Register from field, as it is not used for these account types.



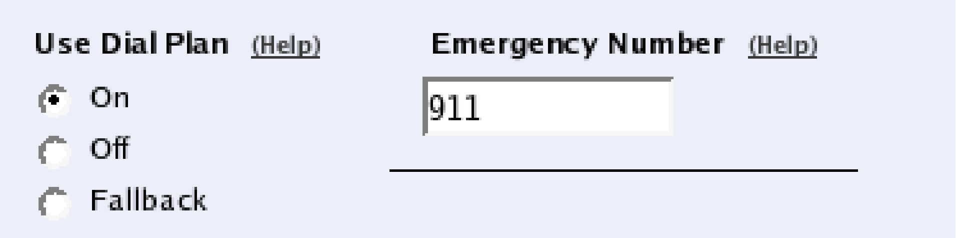
Local SIP User Database (Help)

Edit Row	Username	Domain	Authentication Name	Password	Account Type	Register From	Delete Row
□	24285722	sipoperator.com	123456789		XF/Register	Office	□
□	24285723	sipoperator.com	123456789		XF/Register	Office	□
□	24285724	sipoperator.com	123456789		XF/Register	Office	□
□	24285725	sipoperator.com	123456789		XF/Register	Office	□

Outgoing Calls

For outgoing calls, you have to define when your SIP operator account should be used. Usually, you use this type of account to call to the PSTN network ("ordinary telephones").

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.



Use Dial Plan (Help)

● On

○ Off

○ Fallback

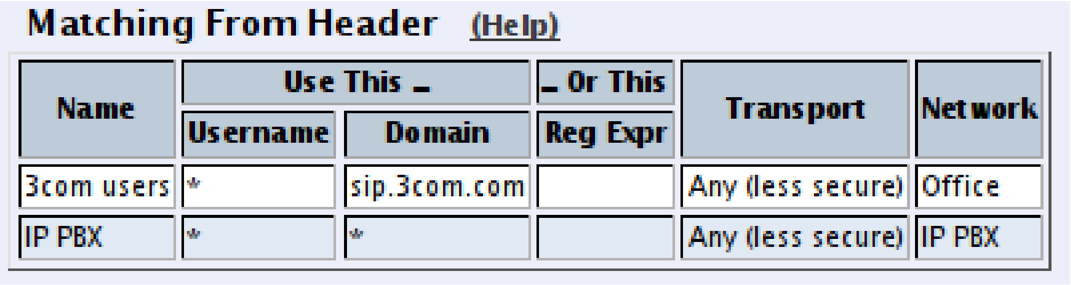
Emergency Number (Help)

911

Show One Number When Calling

You can select to show one single calling number regardless of which user makes the call. This is useful when you want others to use your Answering service/Auto Attendant when calling back to you.

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.



Matching From Header (Help)

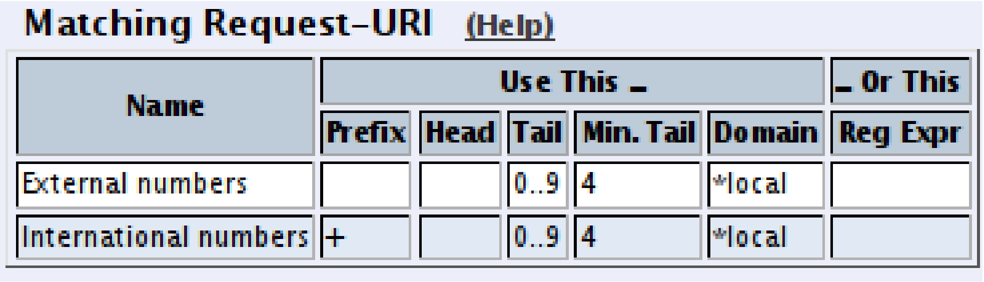
Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
3com users	*	sip.3com.com		Any (less secure)	Office
IP PBX	*	*		Any (less secure)	IP PBX

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like *helen@sip.ingate.com* should not be routed via the SIP operator, but be handled by the Telecommuting Module itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.



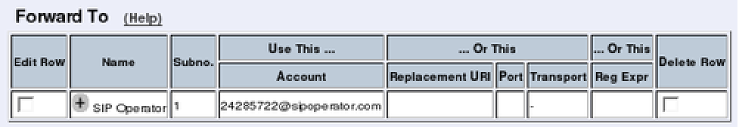
Matching Request-URI (Help)

Name	Use This –					– Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
External numbers			0..9	4	*local	
International numbers	+		0..9	4	*local	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

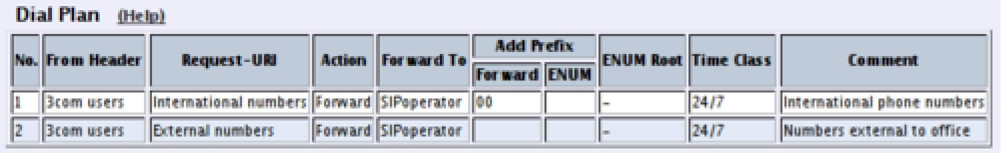
The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ SIP Operator	1	24285722@sipoperator.com			-		□

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	3com users	International numbers	Forward	SIPoperator	00		-	24/7	International phone numbers
2	3com users	External numbers	Forward	SIPoperator			-	24/7	Numbers external to office

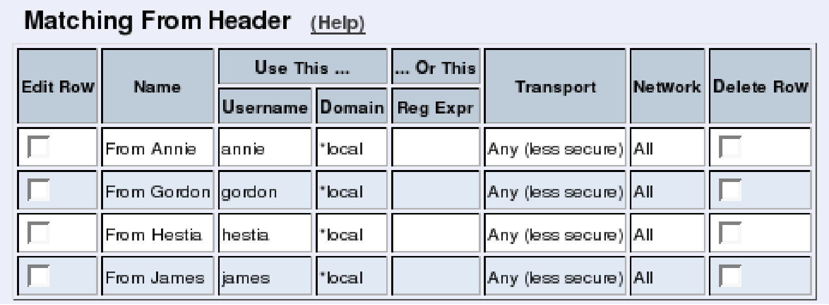
Now, when a local user calls an external phone number, the Telecommuting Module will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

Show Different Numbers When Calling

You can select to show different calling numbers based on which user makes the call. This is useful when you want to let the called person use number presentation to see who is calling.

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

Create one row per user. These will be used to present the correct calling number for the called user.



Matching From Header (Help)

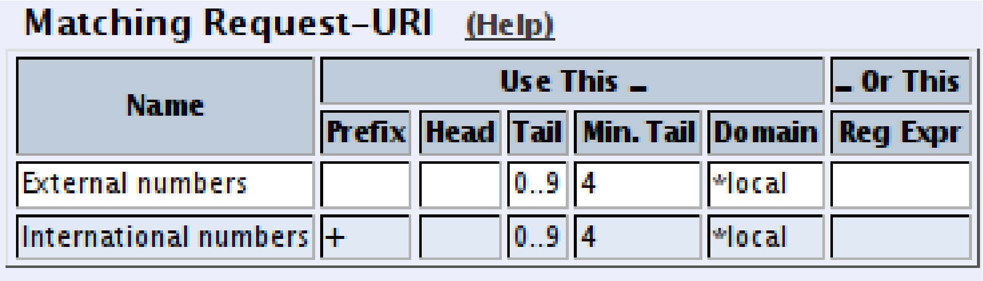
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
□	From Annie	annie	*local		Any (less secure)	All	□
□	From Gordon	gordon	*local		Any (less secure)	All	□
□	From Hestia	hestia	*local		Any (less secure)	All	□
□	From James	james	*local		Any (less secure)	All	□

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like *helen@sip.ingate.com* should not be routed via the SIP operator, but be handled by the Telecommuting Module itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.

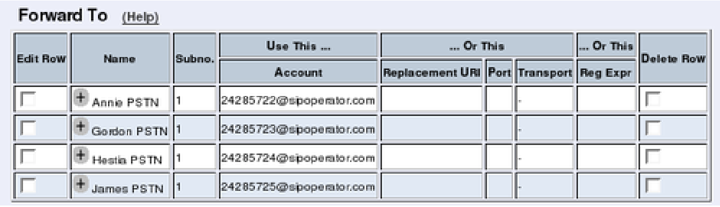


Matching Request-URI (Help)

Name	Use This ...					... Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
External numbers			0..9	4	*local	
International numbers	+		0..9	4	*local	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

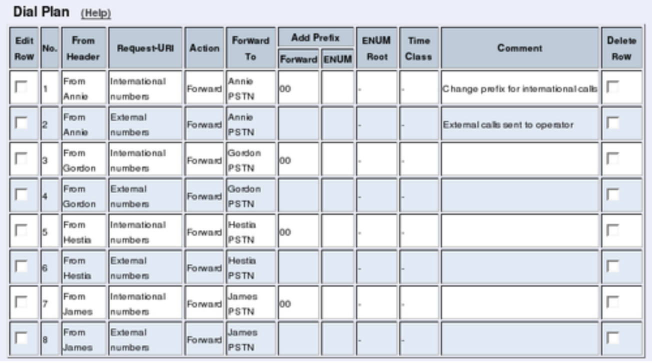
In this case, calls from one user should be forwarded to the corresponding SIP operator account. Create one row per user and select the account under **Account**.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ Annie PSTN	1	24285722@sipoperator.com			-		□
□	+ Gordon PSTN	1	24285723@sipoperator.com			-		□
□	+ Hestia PSTN	1	24285724@sipoperator.com			-		□
□	+ James PSTN	1	24285725@sipoperator.com			-		□

At last, you combine these definitions in the **Dial Plan** table. For each user, make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.



Dial Plan (Help)

Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
□	1	From Annie	International numbers	Forward	Annie PSTN	00		-	-	Change prefix for international calls	□
□	2	From Annie	External numbers	Forward	Annie PSTN			-	-	External calls sent to operator	□
□	3	From Gordon	International numbers	Forward	Gordon PSTN	00		-	-		□
□	4	From Gordon	External numbers	Forward	Gordon PSTN			-	-		□
□	5	From Hestia	International numbers	Forward	Hestia PSTN	00		-	-		□
□	6	From Hestia	External numbers	Forward	Hestia PSTN			-	-		□
□	7	From James	International numbers	Forward	James PSTN	00		-	-		□
□	8	From James	External numbers	Forward	James PSTN			-	-		□

Now, when a local user calls an external phone number, the Telecommuting Module will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

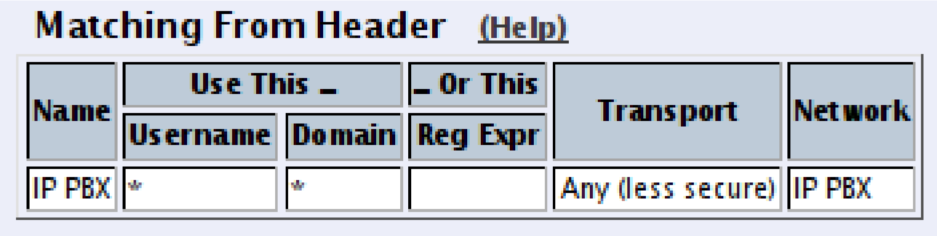
Incoming Calls

For incoming calls, there are two different ways of forwarding the calls to your SIP server; either via the **Dial Plan** or via the **User Routing** table. Which one should be used depends on how the operator sends out your calls.

If they just send them out as *number@yourdomain.com*, you should use the Dial Plan. If they use the Contact information in the registration, you should use the User Routing.

If you use the Dial Plan, you need to add some more settings on the **Dial Plan** page.

First, add a row in the **Matching From Header** table to match incoming calls.

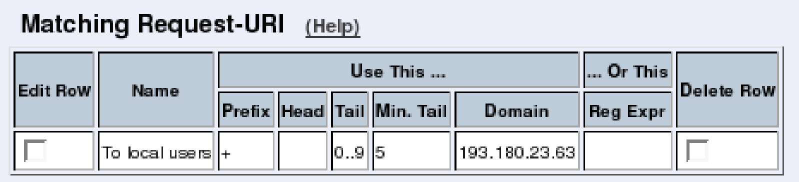


Matching From Header (Help)

Name	Use This ...		... Or This	Transport	Network
	Username	Domain	Reg Expr		
IP PBX	*	*		Any (less secure)	IP PBX

Then, match on the incoming phone number and domain in the **Matching Request-URI** table. The Domain will usually be the public IP address of the Telecommuting Module.

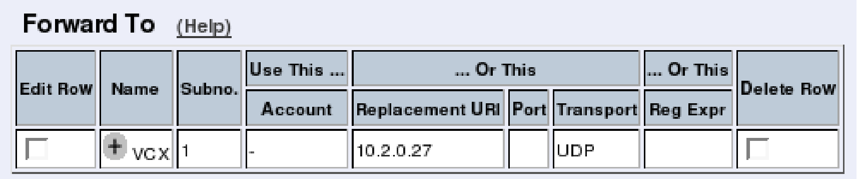
If the operator uses a '+' in front of the phone number and your SIP server doesn't want that, enter '+' in the **Prefix** field. This will make the Telecommuting Module strip the '+' before forwarding the call.



Matching Request-URI (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
□	To local users	+		0..9	5	193.180.23.63		□

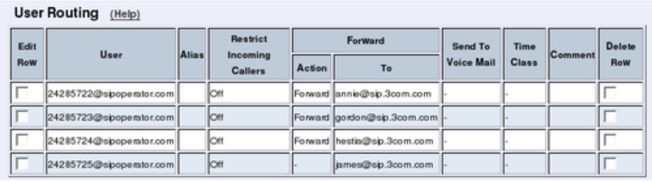
Enter the SIP server in the **Forward To** table.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ VCX	1	-	10.2.0.27		UDP		□

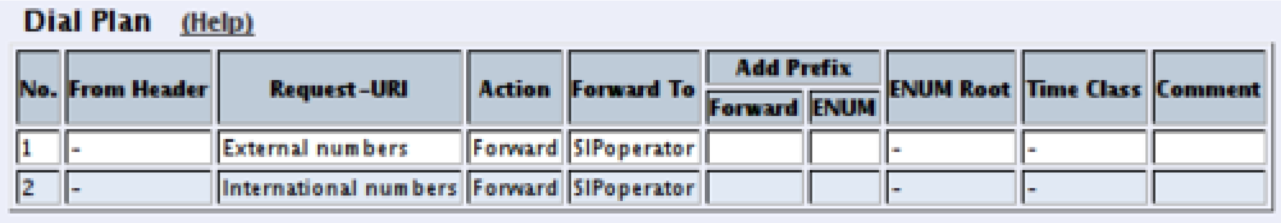
Combine these in the **Forward To** table.



User Routing (Help)

Edit Row	User	Alias	Restrict Incoming Callers	Forward		Send To Voice Mail	Time Class	Comment	Delete Row
				Action	To				
□	24285722@sipoperator.com		Off	Forward	annie@sip.3com.com	-	-		□
□	24285723@sipoperator.com		Off	Forward	gordon@sip.3com.com	-	-		□
□	24285724@sipoperator.com		Off	Forward	hestia@sip.3com.com	-	-		□
□	24285725@sipoperator.com		Off	-	james@sip.3com.com	-	-		□

If you use **User Routing**, you need to add a forwarding address for each of the SIP operator accounts you have.

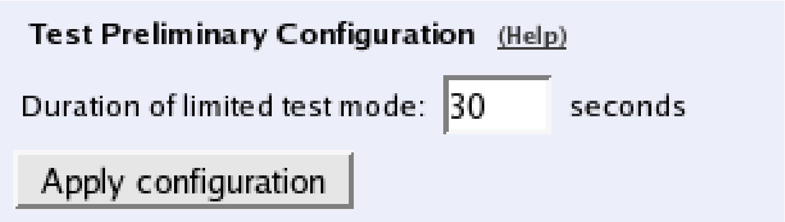


Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	-	External numbers	Forward	SIPoperator			-	-	
2	-	International numbers	Forward	SIPoperator			-	-	

Note that you can only use the **User Routing** table for incoming call forwarding. The **Static Registrations** should not be used when XF or XF/Register accounts are involved.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

How To Use Your SIP Operator Account and Your IP-PBX Via 3Com VCX IP Telecommuting Module

This is how to configure your Telecommuting Module to forward requests between your SIP operator and your local IP-PBX.

The configuration varies slightly depending on if the operator uses accounts or IP addresses for the authentication.

This feature is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Instead of configuring this manually, you can use the 3Com Startup Tool, which can be found at http://www.ingate.com/Startup_Tool.php.

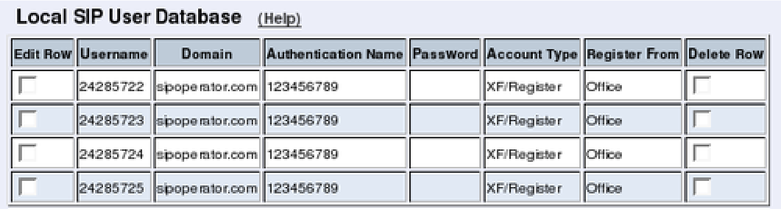
Outgoing Calls

Authentication by Accounts a.k.a SIP Trunk via SIP accounts

Enter your SIP operator account on the **Local Registrar** page. You enter the username and password from the operator, and select the *XF/Register* account type. This account type will make the Telecommuting Module register at the SIP operator with the credentials you enter.

Some operators don’t require registration. In this case, select the *XF* account type instead.

You can select any network in the Register from field, as it is not used for these account types.

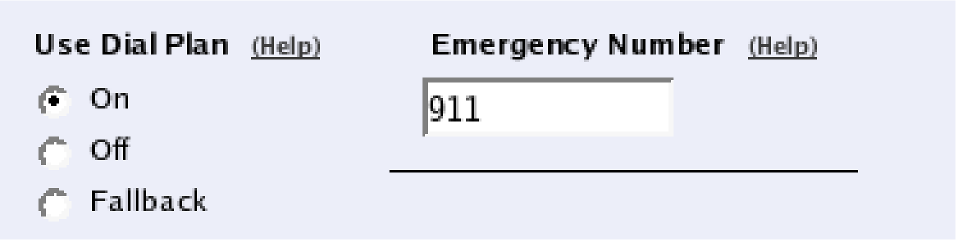


Local SIP User Database (Help)

Edit Row	Username	Domain	Authentication Name	Password	Account Type	Register From	Delete Row
□	24285722	sipoperator.com	123456789		XF/Register	Office	□
□	24285723	sipoperator.com	123456789		XF/Register	Office	□
□	24285724	sipoperator.com	123456789		XF/Register	Office	□
□	24285725	sipoperator.com	123456789		XF/Register	Office	□

For outgoing calls, you have to define when your SIP operator account should be used. Usually, you use this type of account to call to the PSTN network ("ordinary telephones").

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.



Use Dial Plan (Help)

● On

○ Off

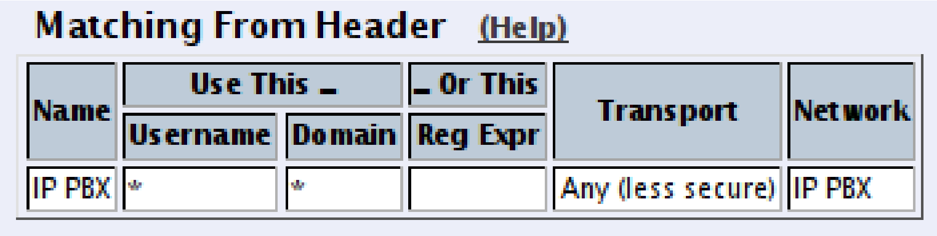
○ Fallback

Emergency Number (Help)

911

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we want to match on calls coming from the IP-PBX. This will ensure that only users who have been autorized by the PBX to use the SIP trunk will be able to make outgoing calls.



Matching From Header (Help)

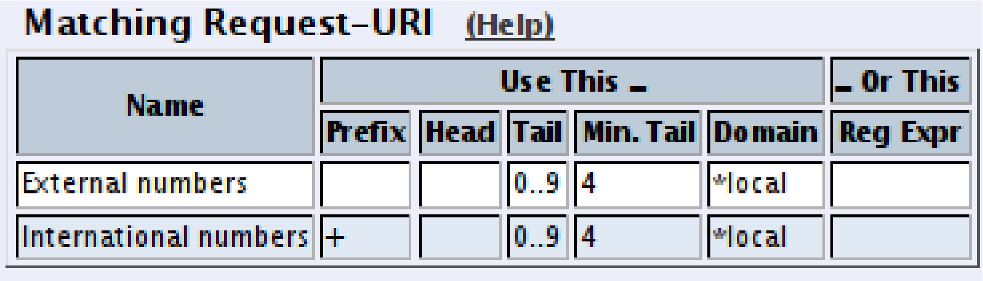
Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
IP PBX	*	*		Any (less secure)	IP PBX

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like *helen@sip.ingate.com* should not be routed via the SIP operator, but be handled by the Telecommuting Module itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.



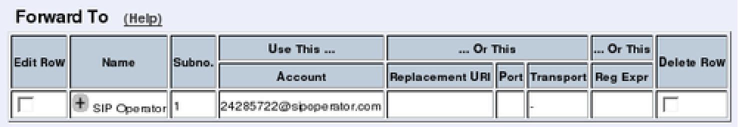
Matching Request-URI (Help)

Name	Use This –					– Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
External numbers			0..9	4	*local	
International numbers	+		0..9	4	*local	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

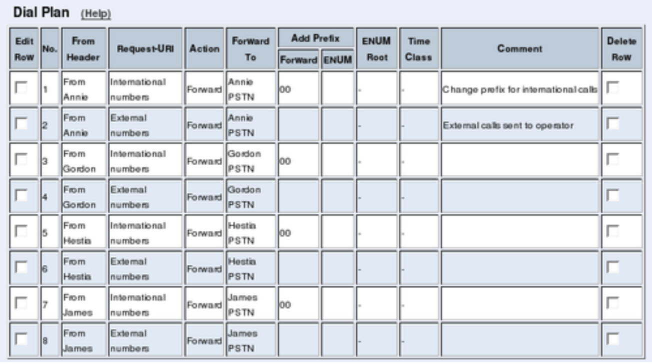
The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ SIP Operator	1	24285722@sipoperator.com			-		□

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.



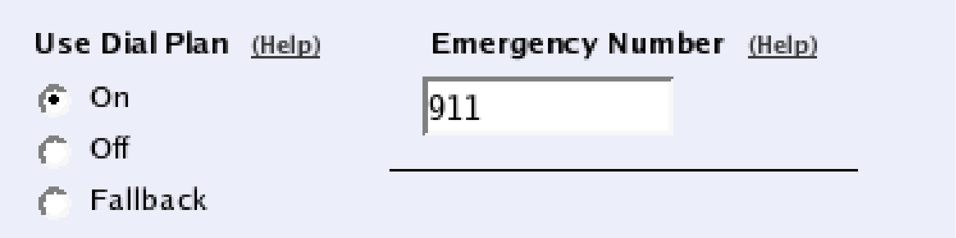
Dial Plan (Help)

Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
□	1	From Annie	International numbers	Forward	Annie PSTN	00		-	-	Change prefix for international calls	□
□	2	From Annie	External numbers	Forward	Annie PSTN			-	-	External calls sent to operator	□
□	3	From Gordon	International numbers	Forward	Gordon PSTN	00		-	-		□
□	4	From Gordon	External numbers	Forward	Gordon PSTN			-	-		□
□	5	From Hestia	International numbers	Forward	Hestia PSTN	00		-	-		□
□	6	From Hestia	External numbers	Forward	Hestia PSTN			-	-		□
□	7	From James	International numbers	Forward	James PSTN	00		-	-		□
□	8	From James	External numbers	Forward	James PSTN			-	-		□

Now, when a local user calls an external phone number, the Telecommuting Module will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

Authentication by IP Addresses a.k.a SIP Trunk via IP address

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.



Use Dial Plan (Help)

● On

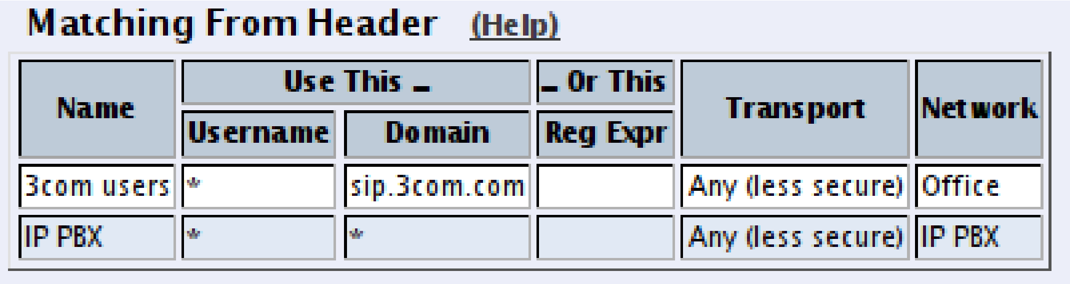
○ Off

○ Fallback

Emergency Number (Help)

911

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.



Matching From Header (Help)

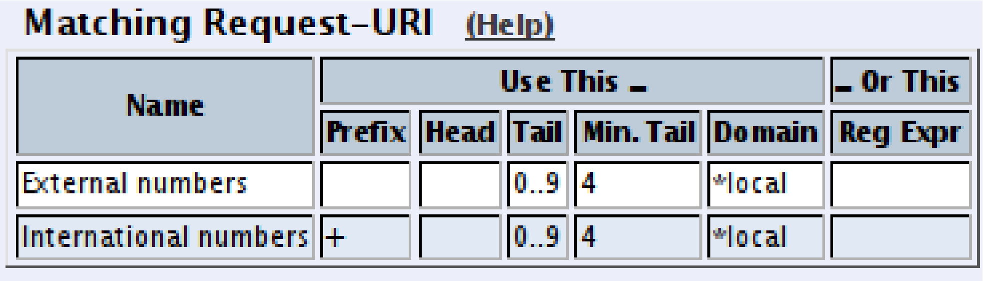
Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
3com users	*	sip.3com.com		Any (less secure)	Office
IP PBX	*	*		Any (less secure)	IP PBX

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like *helen@sip.ingate.com* should not be routed via the SIP operator, but be handled by the Telecommuting Module itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.



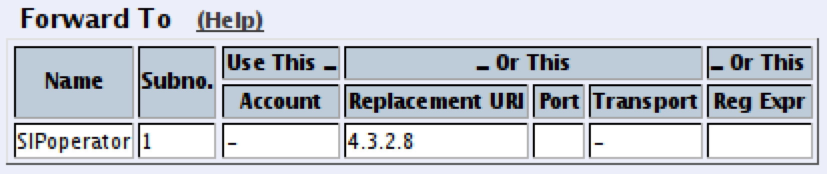
Matching Request-URI (Help)

Name	Use This –					– Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
External numbers			0..9	4	*local	
International numbers	+		0..9	4	*local	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

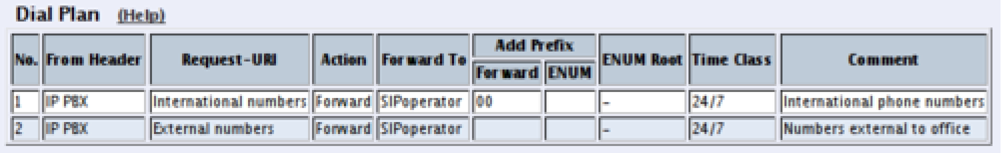
The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.



Forward To (Help)

Name	Subno.	Use This –	– Or This			– Or This
		Account	Replacement URI	Port	Transport	Reg Expr
SIPoperator	1	-	4.3.2.8		-	

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.



Dial Plan (Help)

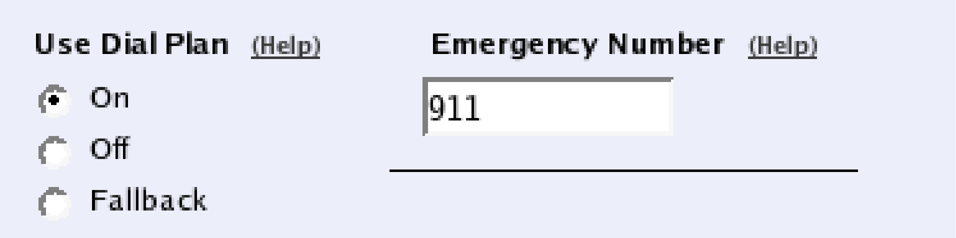
No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	IP PBX	International numbers	Forward	SIPoperator	00		-	24/7	International phone numbers
2	IP PBX	External numbers	Forward	SIPoperator			-	24/7	Numbers external to office

Now, when a local user calls an external phone number, the Telecommuting Module will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

Incoming Calls

All incoming calls from the operator should be forwarded to the PBX. This is done on the **Dial Plan** page.

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.



Use Dial Plan (Help)

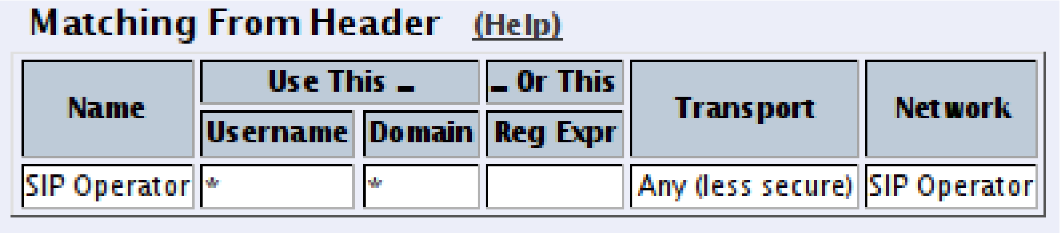
● On
○ Off
○ Fallback

Emergency Number (Help)

911

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we only need to define the operator by its sending network.

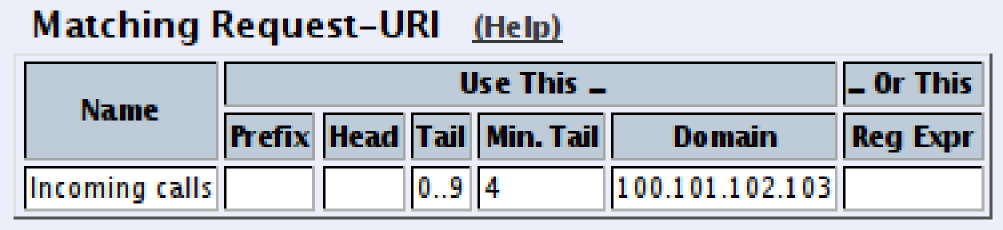


Matching From Header (Help)

Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
SIP Operator	*	*		Any (less secure)	SIP Operator

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your PBX, which is call destinations where the usernames consist of numbers only. For extra matching, enter the outside IP address of the Telecommuting Module, which the operator will be using.



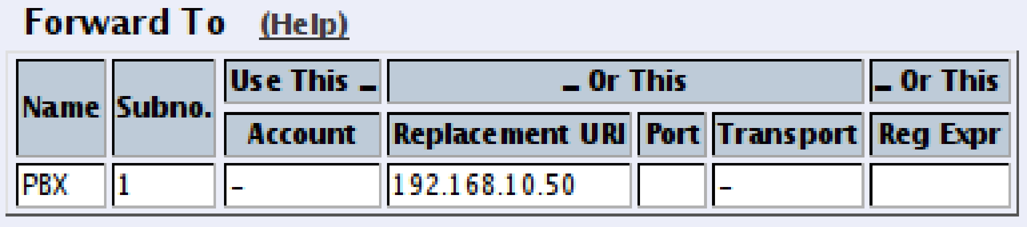
Matching Request-URI (Help)

Name	Use This –					– Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
Incoming calls			0..9	4	100.101.102.103	

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

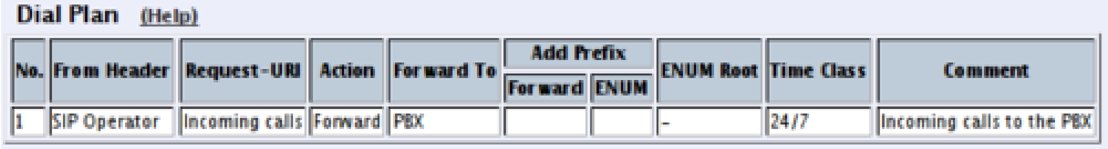
Enter the IP address of the IP-PBX in the **Replacement URI** field. This will make the Telecommuting Module replace the domain part in the incoming call with this IP address. The username part of the URI will be kept.



Forward To (Help)

Name	Subno.	Use This –	– Or This			– Or This
		Account	Replacement URI	Port	Transport	Reg Expr
PBX	1	-	192.168.10.50		-	

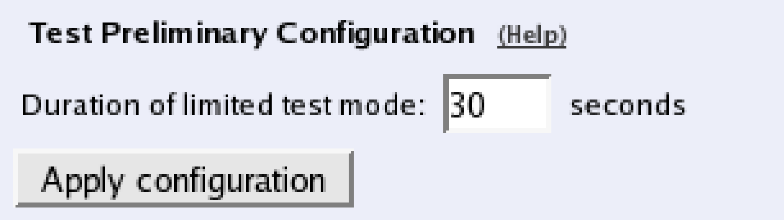
At last, you combine these definitions in the **Dial Plan** table. Select the operator and the Request-URI, and forward to the PBX.



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	SIP Operator	Incoming calls	Forward	PBX			-	24/7	Incoming calls to the PBX

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

How To Use Multiple SIP Operators or IP-PBXs Via 3Com VCX IP Telecommuting Module

This is how to configure your Telecommuting Module to forward requests between your SIP operator and your local IP-PBX.

The configuration varies slightly depending on if the operator uses accounts or IP addresses for the authentication.

This description is targeted for multiple operators or PBXs where the Telecommuting Module selects destination based on the called number and the caller.

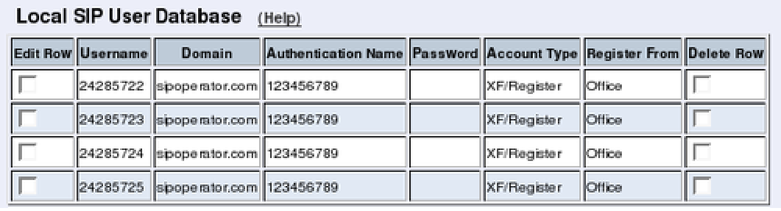
This feature is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Multiple Operators (Least Cost Routing)

If any of the SIP operators use accounts, enter that on the **Local Registrar** page. You enter the username and password from the operator, and select the *XF/Register* account type. This account type will make the Telecommuting Module register at the SIP operator with the credentials you enter.

Some operators don't require registration. In this case, select the *XF* account type instead.

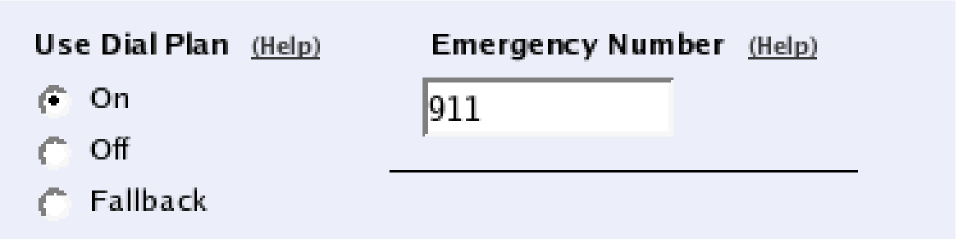
You can select any network in the Register from field, as it is not used for these account types.



Local SIP User Database (Help)

Edit Row	Username	Domain	Authentication Name	Password	Account Type	Register From	Delete Row
□	24285722	sipoperator.com	123456789		XF/Register	Office	□
□	24285723	sipoperator.com	123456789		XF/Register	Office	□
□	24285724	sipoperator.com	123456789		XF/Register	Office	□
□	24285725	sipoperator.com	123456789		XF/Register	Office	□

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.



Use Dial Plan (Help)

● On

○ Off

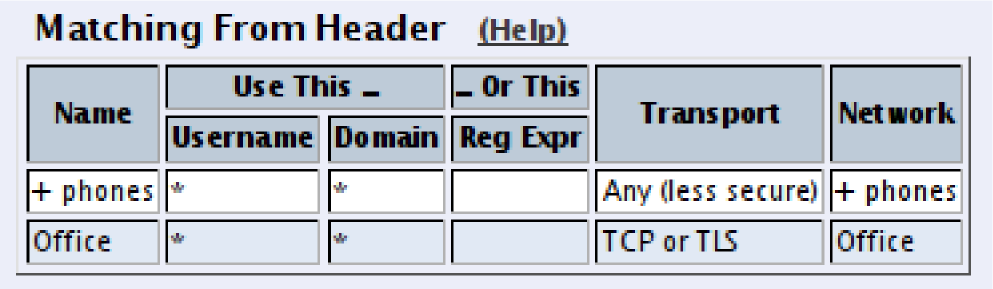
○ Fallback

Emergency Number (Help)

911

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this office, there is a group of phones that always put a "+" first in the phone number when dialing a non-US number. We need to match on these to handle them specially.



Matching From Header (Help)

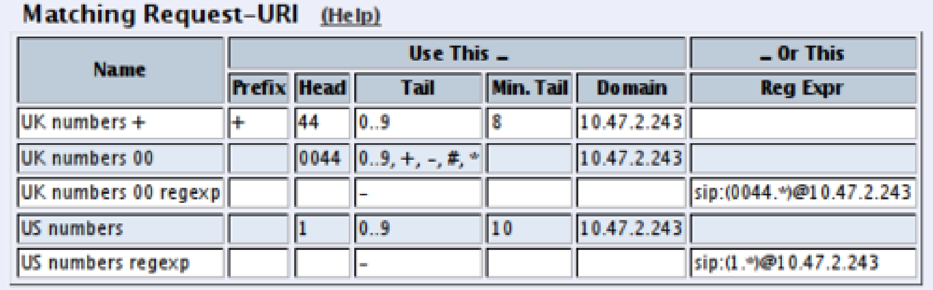
Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
+ phones	*	*		Any (less secure)	+ phones
Office	*	*		TCP or TLS	Office

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to sort out calls that should be routed to the different operators. You might have a UK operator and a US operator, and thus you want to be able to recognize these calls.

The basic way of recognizing calls is to check the country code, which is the first part of the phone number. In the table, there are three rows for matching UK calls. The two "UK numbers 00" rows give the same result, as does the two "US numbers" rows. The 10.47.2.243 IP address is that of the Telecommuting Module itself.

The ".*" expression in the **Reg Expr** fields match 0 or more characters of any kind. The parantheses show how much of the incoming Request-URI we want to keep when forwarding the request.



Matching Request–URI (Help)

Name	Use This –					– Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
UK numbers +	+	44	0..9	8	10.47.2.243	
UK numbers 00		0044	0..9, +, -, #, *		10.47.2.243	
UK numbers 00 regexp			-			sip:(0044.*)@10.47.2.243
US numbers		1	0..9	10	10.47.2.243	
US numbers regexp			-			sip:(1.*)@10.47.2.243

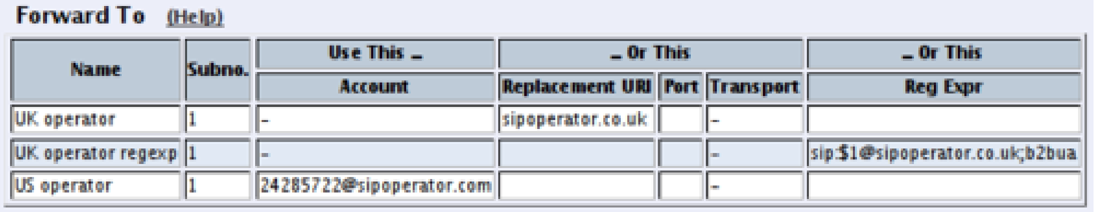
In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, define your two SIP operators. One may use accounts and the other IP addresses for authentication.

The two "UK Operator" rows are nearly the same.

With the "UK Operator" row, the Request-URI in the incoming call will have the domain part replaced with what is entered in the **Replacement URI** field. The username part of the URI will be kept.

With the "UK Operator regexp" row, the Telecommuting Module will get whatever was in the first set of parantheses in the **Matching Request-URI** table, and use that as the username part. The domain part is "sipoperator.co.uk;b2bua". The ";b2bua" parameter makes the Telecommuting Module handle all REFER requests itself; instead of forwarding them. This can be useful as many operators do not support the REFER method, which is used for call transfers.



Forward To (Help)

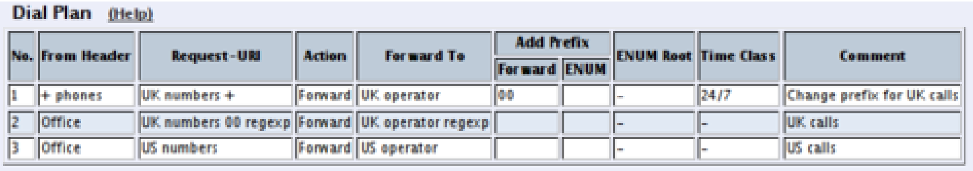
Name	Subno.	Use This –	– Or This			– Or This
		Account	Replacement URI	Port	Transport	Reg Expr
UK operator	1	-	sipoperator.co.uk		-	
UK operator regexp	1	-			-	sip:$1@sipoperator.co.uk;b2bua
US operator	1	24285722@sipoperator.com			-	

At last, you combine these definitions in the **Dial Plan** table.

For UK calls, the operator requires that the phone number begins with "00", which means that some calls can be forwarded directly (row 2), but for calls where the number starts with "+", this has to be replaced with "00" (row 3). This means the calls that originate from the "+ phones".

For US calls, use any of the defined US Request-URIs, and forward to the US operator.

Note that if you want to use a Reg Expr definition for **Forward To**, you also need to use a Reg Expr definition for the **Request-URI**.



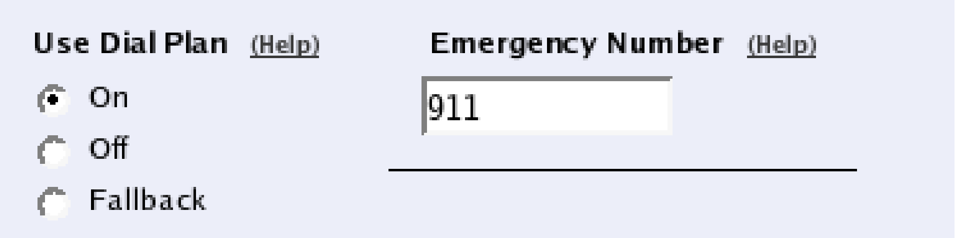
Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	+ phones	UK numbers +	Forward	UK operator	00		-	24/7	Change prefix for UK calls
2	Office	UK numbers 00 regexp	Forward	UK operator regexp			-	-	UK calls
3	Office	US numbers	Forward	US operator			-	-	US calls

Multiple PBXs

If you have multiple PBXs on the inside, you might want to send calls to different servers based on the sender or the called number.

On the **Dial Plan** page, you define which calls should be redirected to which PBX. First, turn the Dial Plan on.



Use Dial Plan (Help)

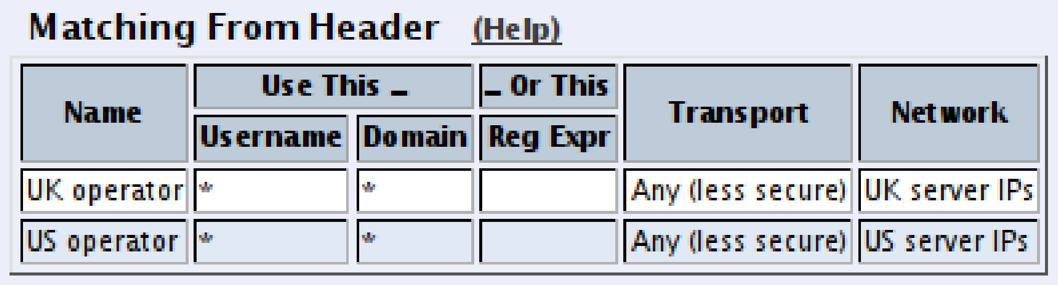
● On
○ Off
○ Fallback

Emergency Number (Help)

911

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we define one entry for each operator.



Matching From Header (Help)

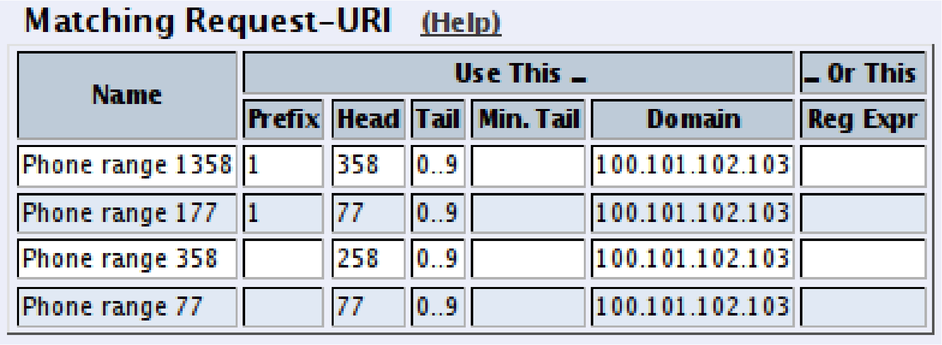
Name	Use This _		_ Or This	Transport	Network
	Username	Domain	Reg Expr		
UK operator	*	*		Any (less secure)	UK server IPs
US operator	*	*		Any (less secure)	US server IPs

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to sort out which calls go to which PBX.

Assuming that each PBX manage a phone number range where the leading digits are different, it is easy to make matching definitions.

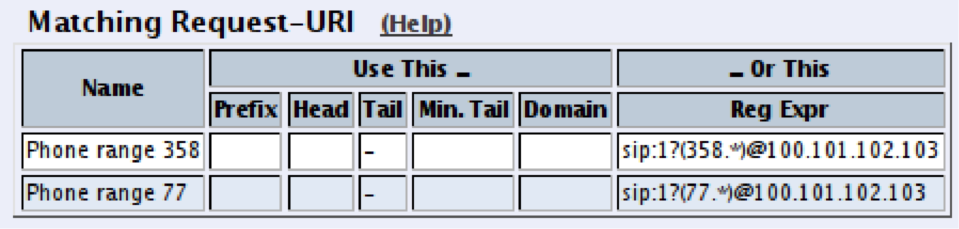
As the UK operator will send phone numbers that start with a "1", we allow for that, but by putting the "1" in the **Prefix** column, it will be stripped from the phone number when the Telecommuting Module forwards the call.



Matching Request-URI (Help)

Name	Use This _					_ Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
Phone range 1358	1	358	0..9		100.101.102.103	
Phone range 177	1	77	0..9		100.101.102.103	
Phone range 358		258	0..9		100.101.102.103	
Phone range 77		77	0..9		100.101.102.103	

The same matching definitions can be made with regular expressions. Here, each number range only needs one definition, as the "?" sign marks that the previous character can appear 0 or 1 times. The part of the number that we want to forward should be within parantheses.

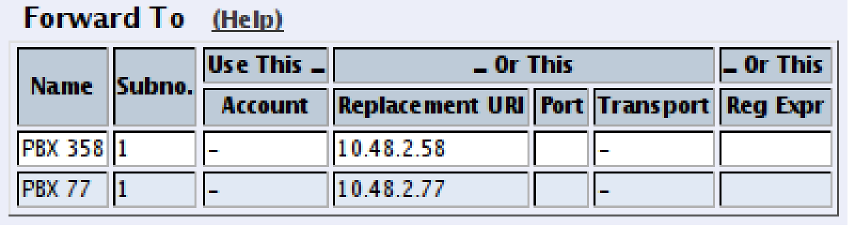


Matching Request-URI (Help)

Name	Use This _					_ Or This
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr
Phone range 358			-			sip:1?(358.*)@100.101.102.103
Phone range 77			-			sip:1?(77.*)@100.101.102.103

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

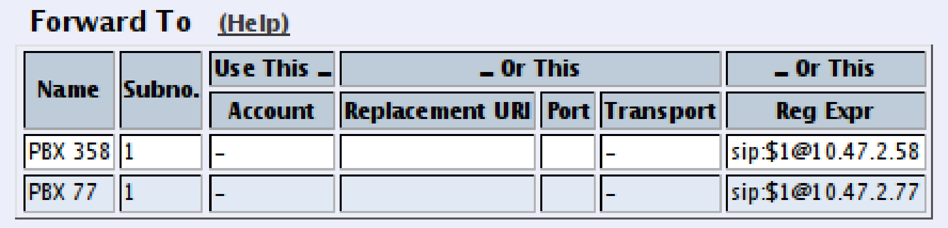
In this case, define your two PBXs, simply by entering their respective IP addresses in the **Replacement URI** field.



Forward To (Help)

Name	Subno.	Use This _	_ Or This			_ Or This
		Account	Replacement URI	Port	Transport	Reg Expr
PBX 358	1	-	10.48.2.58		-	
PBX 77	1	-	10.48.2.77		-	

The same forwarding definitions can be made with regular expressions. The "$1" expression collects the number that matched the expression inside the parantheses in the **Matching Request-URI** table.

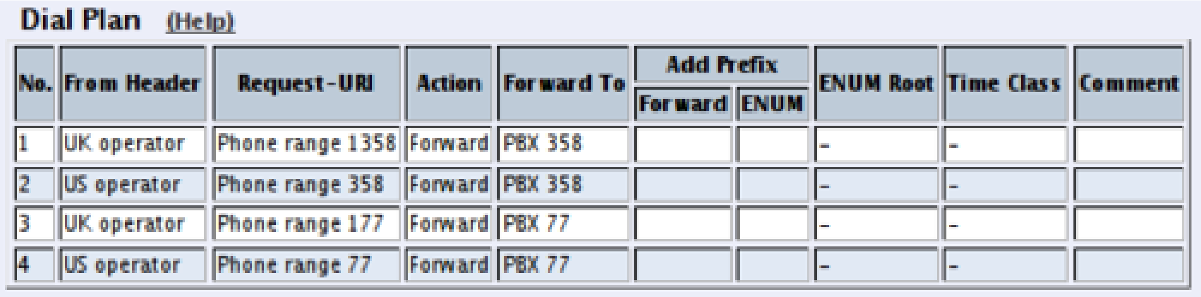


Forward To (Help)

Name	Subno.	Use This _	_ Or This			_ Or This
		Account	Replacement URI	Port	Transport	Reg Expr
PBX 358	1	-			-	sip:$1@10.47.2.58
PBX 77	1	-			-	sip:$1@10.47.2.77

At last, you combine these definitions in the **Dial Plan** table.

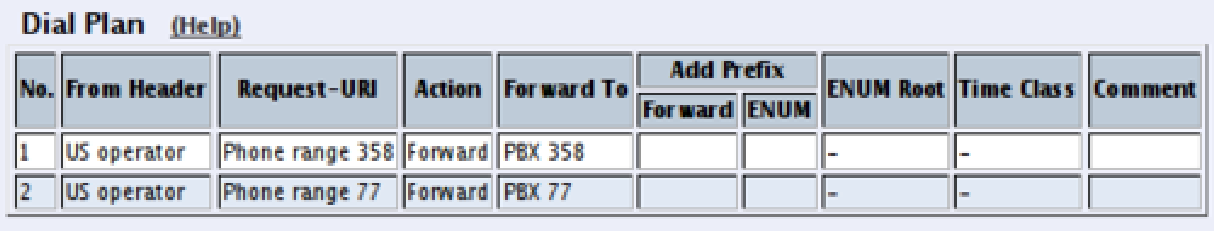
Select the operator, range, and then select to which PBX to send this call.



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	UK operator	Phone range 1358	Forward	PBX 358			-	-	
2	US operator	Phone range 358	Forward	PBX 358			-	-	
3	UK operator	Phone range 177	Forward	PBX 77			-	-	
4	US operator	Phone range 77	Forward	PBX 77			-	-	

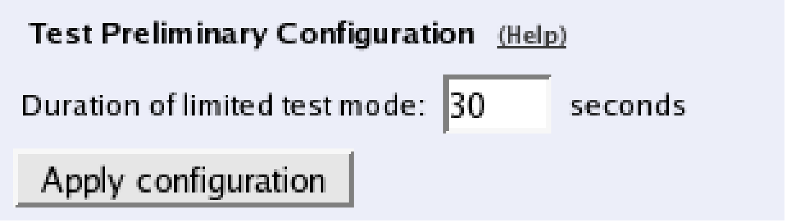
If regular expressions were used, you only need one line per PBX. As the expressions were designed to match calls from both operators, you don't need to select an operator here.



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	US operator	Phone range 358	Forward	PBX 358			-	-	
2	US operator	Phone range 77	Forward	PBX 77			-	-	

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

How To Use RADIUS Accounting with 3Com VCX IP Telecommuting Module

This is how to configure your Telecommuting Module to use RADIUS Accounting for calls to or from local users.

If you are only interested in accounting for calls to other domains, you only have to turn the RADIUS Accounting on.

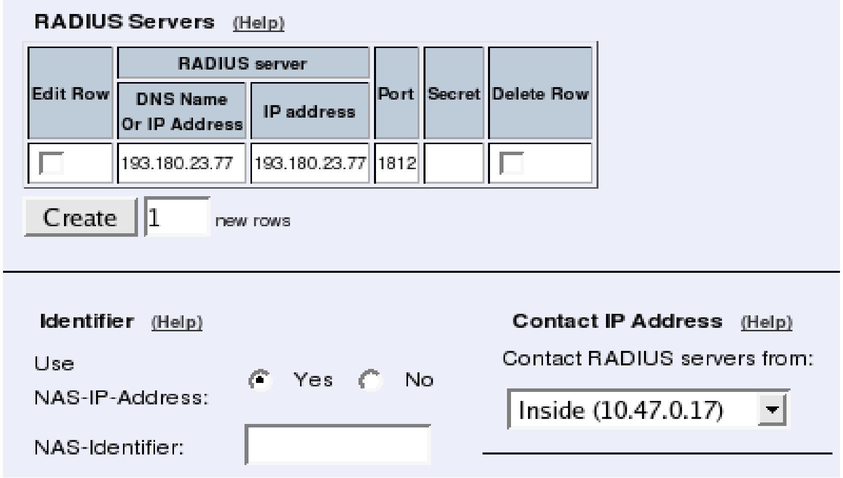
If you want to bill for local calls too, you will have to force the users to go via the Telecommuting Module even when they are both on the same side. For this, the Telecommuting Module will have to act as a back-to-back user agent (B2BUA) for all calls.

This feature is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

First, define the RADIUS server to receive accounting ticks. This is done on the **RADIUS** page. If the RADIUS server should only be used for accounting, you can enter any port number in the table. The Telecommuting Module will use port 1813 for accounting.

If you use the Telecommuting Module as the SIP registrar, and the RADIUS server should be used for SIP authentication as well, you need to enter the port number on which the

RADIUS server listens for authentication requests (usually ports 1812 or 1645).



RADIUS Servers (Help)

Edit Row	RADIUS server		Port	Secret	Delete Row
	DNS Name Or IP Address	IP address			
□	193.180.23.77	193.180.23.77	1812		□

Create 1 new rows

Identifier (Help)

Use NAS-IP-Address: ● Yes ○ No

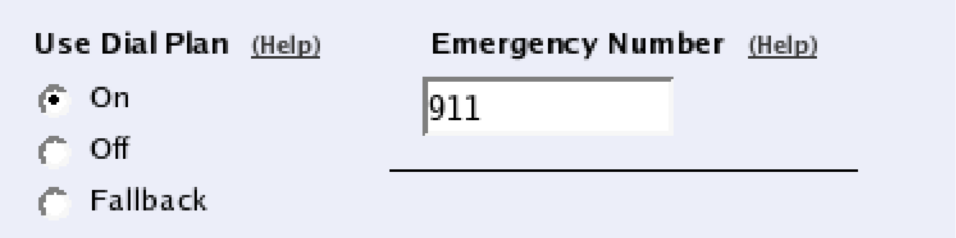
NAS-Identifier:

Contact IP Address (Help)

Contact RADIUS servers from:

Inside (10.47.0.17)

On the **Dial Plan** page, you define how calls should be routed through the Telecommuting Module. First, turn the Dial Plan on.



Use Dial Plan (Help)

● On

○ Off

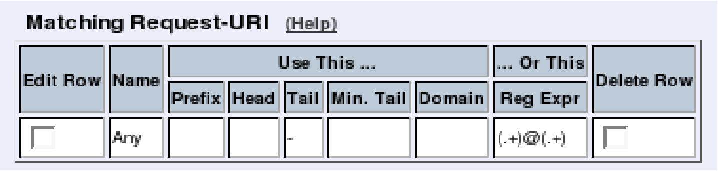
○ Fallback

Emergency Number (Help)

911

In the **Matching Request-URI** table, you define call destinations. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define a **Reg Exp** (regular expression) which matches all Request-URIs. Enter "(.+)@(.+)" in the Reg Exp field.

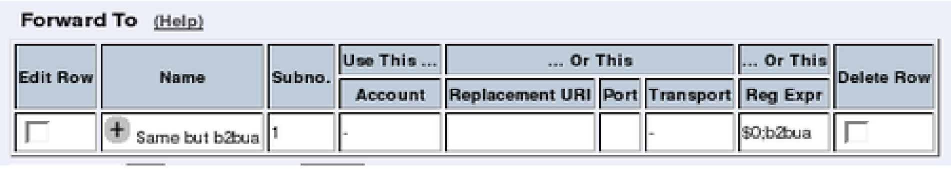


Matching Request-URI (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
□	Any			-			(.+)@(.+)	□

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

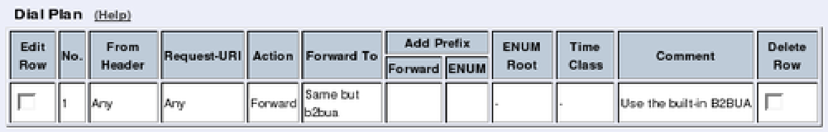
In this case, the calls should be forwarded to their original destination, but the Telecommuting Module should forward them as a B2BUA. Enter "$0;b2bua" in the Reg Exp field. This will reuse the incoming Request-URI, but make the Telecommuting Module act as a B2BUA instead of a proxy.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ Same but b2bua	1	-			-	$0;b2bua	□

At last, you combine these definitions in the **Dial Plan** table. Make a new row in the table and select the definitions from the tables above.

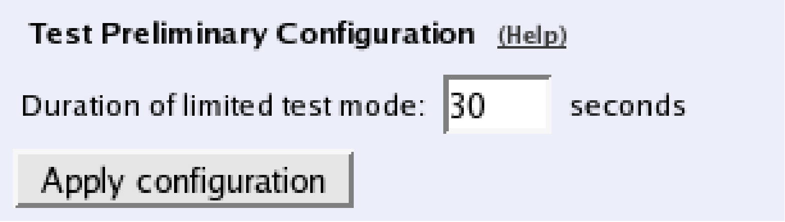


Dial Plan (Help)

Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
□	1	Any	Any	Forward	Same but b2bua			-	-	Use the built-in B2BUA	□

Now, when a SIP user calls another SIP user, the Telecommuting Module will step in and always stay in the path for the call. Both SIP clients will signal to the Telecommuting Module only, and the Telecommuting Module will forward signaling between them. Media will still go directly between the clients.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

Part III. Description of 3Com VCX IP Telecommuting Module Settings

This part contains complete descriptions of settings in the 3Com VCX IP Telecommuting Module GUI. The descriptions are grouped in the same way as they are in the GUI.

Chapter 6. Basic Configuration

Under **Basic Configuration**, you configure:

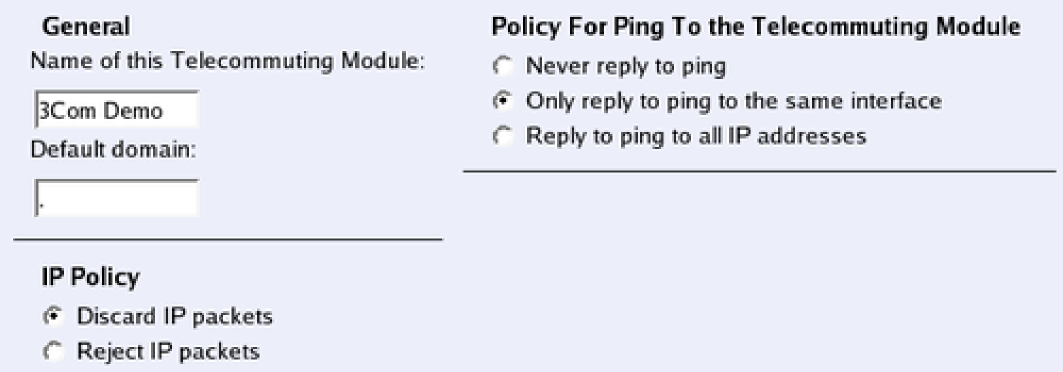
- Telecommuting Module Type
- The name of the Telecommuting Module
- The computers and networks from which the Telecommuting Module can be administered
- Policies for ping packets and unwanted packets
- Default domain
- DNS servers
- RADIUS configuration
- SNMP configuration
- If the Telecommuting Module should use external services to update a DNS server dynamically when the Telecommuting Module changes its own IP address.
- Creation of Telecommuting Module certificates and upload of CA certificates

This configuration is usually not changed very often.

Basic Configuration

On the **Basic Configuration** page, general settings for the Telecommuting Module are made. The most important one for getting started is the DNS server.

General



General

Name of this Telecommuting Module: 3Com Demo

Default domain: .

IP Policy

● Discard IP packets
○ Reject IP packets

Policy For Ping To the Telecommuting Module

○ Never reply to ping
● Only reply to ping to the same interface
○ Reply to ping to all IP addresses

Name of this Telecommuting Module

Here, you can give your 3Com VCX IP Telecommuting Module a name. The name of the Telecommuting Module is displayed in the title bar of your web browser. This can be a good idea if you administer several Telecommuting Modules. The name is also used if you use SNMP and when you export log files into the WELF format.

Default domain

Here, you can enter a default domain for all settings. If a default domain is entered, the Telecommuting Module will automatically assume that an incomplete computer name should be completed with the default. If, for example, **Default domain** contains **`company.com`**, you could as the name of the computer axel.company.com use only **`axel`**. If no default domain should be used, the **Default domain** field should contain a single dot (.).

IP Policy

Here, you specify what will happen to IP packets which are neither SIP packets, SIP session media streams, or Telecommuting Module administration traffic. **Discard IP packets** means that the Telecommuting Module ignores the IP packets without replying that the packet did not arrive. **Reject IP packets** makes the Telecommuting Module reply with an ICMP packet telling that the packet did not arrive.

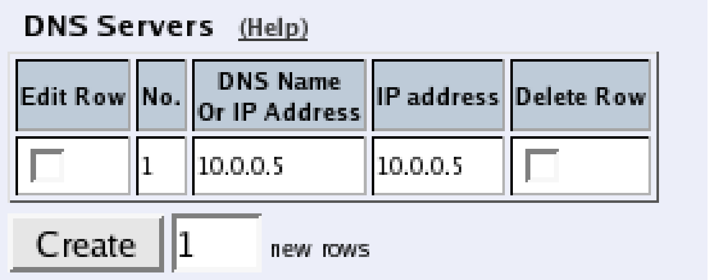
Policy For Ping To Your 3Com VCX IP Telecommuting Module

Here, you specify how the Telecommuting Module should reply to ping packets to its IP addresses. You can choose between **Never reply to ping**, **Only reply to ping from the same interface** and **Reply to ping to all IP addresses**. **Only reply to ping from the same interface** means that the ping request should originate from a network which is directly-connected to the pinged interface of the Telecommuting Module or from a network to which there exists a static route from the pinged interface, or the request will be ignored.

Ping is a way of finding out whether a computer is working. See appendix D, Definitions of Terms, for further information on ping.

DNS Servers

Here, you configure DNS servers for the Telecommuting Module. The servers are used in the order they appear in this table, which means that the Telecommuting Module uses the top server to resolve DNS records until it doesn't reply. Only then is server number two contacted.



DNS Servers (Help)

Edit Row	No.	DNS Name Or IP Address	IP address	Delete Row
□	1	10.0.0.5	10.0.0.5	□

1 new rows

No.

The DNS servers are used in the order they are presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other servers are renumbered automatically. When you click on **Save**, the DNS servers are re-sorted.

Dynamic

If an interface will receive its IP address from a DHCP server, the Telecommuting Module can also get information about its DNS server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

DNS Name Or IP Address

The DNS name/IP address of the DNS server which the Telecommuting Module should use. Note that to use DNS names here, there must exist a DNS server in the Telecommuting Module's permanent configuration.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the Basic Configuration configuration to the preliminary configuration.

Cancel

Reverts all the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered above.

Access Control

On the **Access Control** page, settings are made which controls the access to the Telecommuting Module administration interfaces. The Telecommuting Module can be configured via the web (http and https) and via ssh or the serial cable (using the CLI, see chapter 18, Command Line Reference).

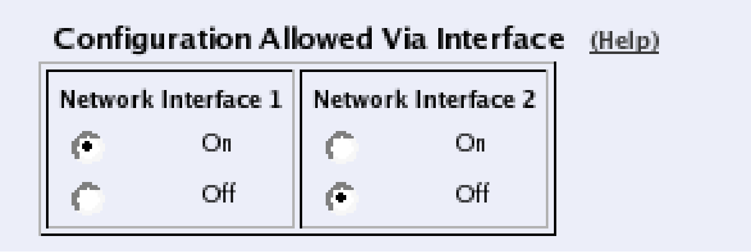
Select one or more configuration IP addresses for the Telecommuting Module. The configuration address is the IP address to which you direct your web browser to access the web interface of the Telecommuting Module, or connect your ssh client to.

For each network interface, you also specify whether or not the Telecommuting Module can be configured via this network interface.

You also select what kind of authentication will be performed for the users trying to access the administration interfaces.

To further increase security, the Telecommuting Module can only be configured from one or a few computers that are accessed from one of these interfaces. Enter the IP address or addresses that can configure the Telecommuting Module. The IP addresses can belong to one or more computers. For each IP address or interval of addresses, select which configuration protocols are allowed.

Configuration Allowed Via Interface



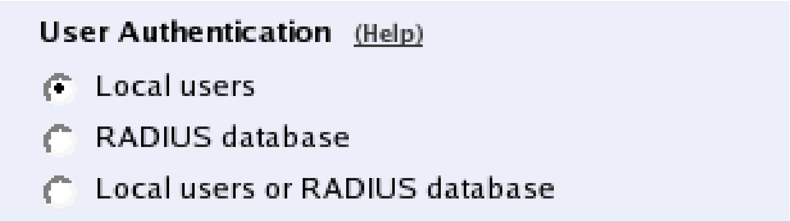
Configuration Allowed Via Interface (Help)

Network Interface 1	Network Interface 2
● On	○ On
○ Off	● Off

This setting specifies whether configuration traffic is allowed via this interface. If you only allow configuration via eth1, configuration traffic will only be allowed from computers connected to the eth1 interface, regardless of which IP address the configuration traffic is directed to or which IP addresses the computers have.

The choices for each interface are **On** and **Off**. This configuration is a complement to the **Configuration Computers** setting below.

User Authentication For Web Interface Access



User Authentication (Help)

● Local users

○ RADIUS database

○ Local users or RADIUS database

Select the mode of administrator authentication for logins via the web interface: **Local users**, via a **RADIUS database**, or a choice between the two alternatives at login (**Local users or RADIUS database**).

Local administrator users and their passwords are defined on the **User Administration** page under **Administration**. If the authentication should be made by help of a RADIUS server, you must enter one on the **RADIUS** page.

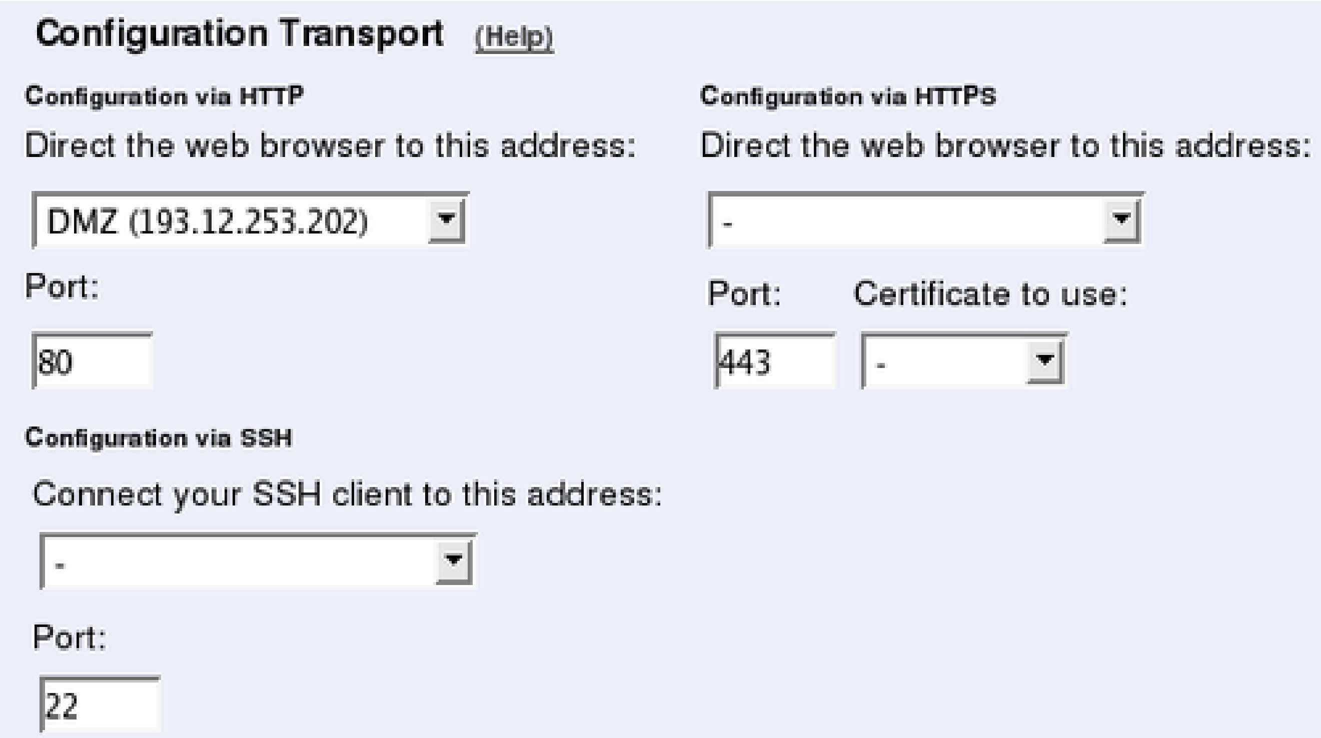
When connecting to the administration interface via SSH, you can only log in as *admin*.

Configuration Transport

Select Telecommuting Module IP addresses for the allowed configuration protocols. The Telecommuting Module web server will listen for web traffic on the IP addresses and ports selected under HTTP and HTTPS.

This is the IP address and port which should be entered in your web browser to connect to the Telecommuting Module.

For configuration via ssh, you need an ssh client to log on to the Telecommuting Module.



Configuration Transport (Help)

Configuration via HTTP

Direct the web browser to this address: DMZ (193.12.253.202)

Port: 80

Configuration via HTTPS

Direct the web browser to this address: -

Port: 443

Certificate to use: -

Configuration via SSH

Connect your SSH client to this address: -

Port: 22

Configuration via HTTP

Select which IP address and port the Telecommuting Module administrator should direct her web browser to when HTTP is used for Telecommuting Module configuration. You can select from the Telecommuting Module IP addresses configured on the **Interface** pages under **Network Configuration**.

You can use different IP addresses for HTTP, HTTPS, and SSH configuration.

Configuration via HTTPS

Select which IP address and port the Telecommuting Module administrator should direct her web browser to when HTTPS is used for Telecommuting Module configuration. You can select from the Telecommuting Module IP addresses configured on the **Interface** pages under **Network Configuration**.

You can use different IP addresses for HTTP, HTTPS, and SSH configuration.

You also need to select an X.509 certificate, which works as an ID card, identifying the Telecommuting Module to your web browser. This will ensure that you are really communicating with your Telecommuting Module and not somebody else's computer. HTTPS uses an encryption method using two keys, one secret and one public. The secret key is kept in the Telecommuting Module and the public key is used in the certificate. If any of the keys is changed, the HTTPS connection won't work.

All local certificates for the Telecommuting Module are created on the **Certificates** page under **Basic Configuration**.

Configuration via SSH

Select which IP address and port the Telecommuting Module administrator should direct her ssh client to when SSH is used for Telecommuting Module configuration. You can select from the Telecommuting Module IP addresses configured on the **Interface** pages under **Network Configuration**.

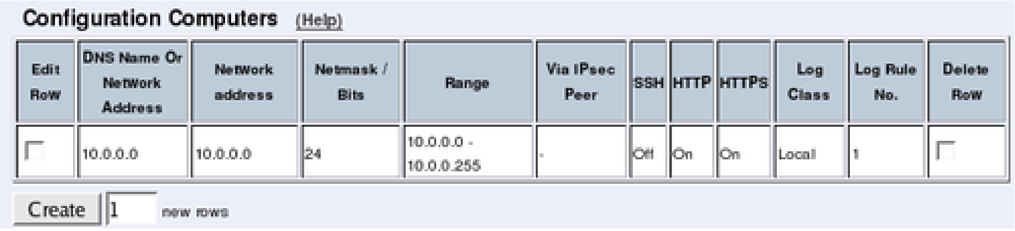
For SSH configuration, the Command Language Interface is used. See also chapter 18, Command Line Reference.

You can use different IP addresses for HTTP, HTTPS, and SSH configuration.

Configuration Computers

Enter the IP address or addresses that can configure the Telecommuting Module. The IP addresses can belong to one or more computers.

Note that you must also allow configuration via the Telecommuting Module interface that the computers are connected to. See **Configuration Allowed Via Interface** above.



Configuration Computers (Help)

Edit Row	DNS Name Or Network Address	Network address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Log Rule No.	Delete Row
□	10.0.0.0	10.0.0.0	24	10.0.0.0 - 10.0.0.255	-	Off	On	On	Local	1	□

No.

The **No.** field determines the order of the lines. The order is important in deciding what is logged and warned for. The Telecommuting Module uses the first line that matches the configuration traffic.

Perhaps you want to configure the Telecommuting Module so that configuration traffic from one specific computer is simply logged while traffic from the rest of that computer's network is both logged and generates alarms.

The rules are used in the order in which they are listed, so if the network is listed first, *all* configuration traffic from that network is both logged and generates alarms, including the traffic from that individual computer. But if the individual computer is listed on a separate line before the network, that line will be considered first and all configuration traffic from that computer is only logged while the traffic from the rest of the computer's network is both logged and generates alarms.

DNS Name Or Network Address

Enter the DNS name or IP address of the computer or network from which the Telecommuting Module can be configured. Avoid allowing configuration from a network or computer on the Internet or other insecure networks, or use HTTPS or IPsec to connect to the Telecommuting Module from these insecure networks.

Network address

Shows the network address of the **DNS Name Or Network Address** you entered in the previous field.

Netmask/Bits

Netmask/Bits is the mask that will be used to specify the configuration computers. See chapter 3, Configuring 3Com VCX IP Telecommuting Module, for instructions on writing the netmask. To limit access so that only one computer can configure, use the netmask 255.255.255.255. You can also specify the netmask as a number of bits, which in this case would be 32. To allow configuration from an entire network, you must enter the network address under **Network address**, and a netmask with a lower number here. To allow configuration from several computers or networks, create several lines for the information.

Range

The **Range** shows all IP addresses from which the Telecommuting Module can be configured. The range is calculated from the configuration under **DNS Name Or Network Address** and **Netmask/Bits**. Check that the correct information was entered in the **DNS Name Or Network Address** and **Netmask/Bits** fields.

Via IPsec Peer

Here, you can select an **IPsec Peer** from which this connection must be made. If an IPsec peer is selected, you will only be able to configure the Telecommuting Module from this IP address through an IPsec tunnel.

SSH

Check the check box if this computer/network should be allowed to configure the Telecommuting Module via SSH.

HTTP

Check the check box if this computer/network should be allowed to configure the Telecommuting Module via HTTP.

HTTPS

Check the check box if this computer/network should be allowed to configure the Telecommuting Module via HTTPS.

Log Class

Here, you enter what log class the Telecommuting Module should use to log the configuration traffic to the Telecommuting Module's web server. Log classes are defined on the **Log Classes** page under **Logging**. See also the chapter titled Logging.

No.

The **No.** field determines the order of the lines. The order is important in deciding what is logged and warned for. The Telecommuting Module uses the first line that matches the configuration traffic.

Perhaps you want to configure the Telecommuting Module so that configuration traffic from one specific computer is simply logged while traffic from the rest of that computer's network is both logged and generates alarms.

The rules are used in the order in which they are listed, so if the network is listed first, *all* configuration traffic from that network is both logged and generates alarms, including the traffic from that individual computer. But if the individual computer is listed on a separate line before the network, that line will be considered first and all configuration traffic from that computer is only logged while the traffic from the rest of the computer's network is both logged and generates alarms.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the Access Control configuration to the preliminary configuration.

Cancel

Reverts all the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

RADIUS

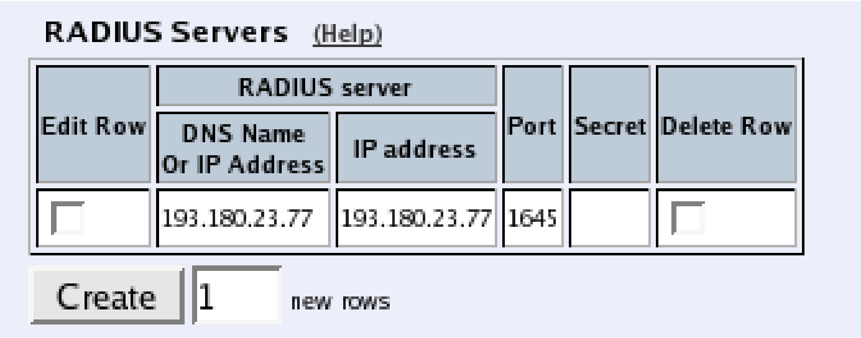
RADIUS (Remote Authentication Dial-In User Service) is an authentication system consisting of one or more servers, and clients using the servers to authenticate users. You could, for example, equip the company modems with RADIUS clients, demanding that a user connecting to a modem first identifies himself to the RADIUS server. Servers and clients communicate via UDP.

3Com VCX IP Telecommuting Module uses RADIUS for authentication for Telecommuting Module administration, for SIP users, and VPN connections from road warriors. If RADIUS is used for user authentication from VPN connections, you must do additional configuration on the **Authentication Server** page.

The Telecommuting Module can also send accounting information about SIP calls to a RADIUS server.

RADIUS Servers

Enter the server(s) that the Telecommuting Module should use. When more than one RADIUS server is entered, make sure that their databases contain the same data, since the Telecommuting Module regards them all alike and uses the server which first replies to a request.



RADIUS Servers (Help)

Edit Row	RADIUS server		Port	Secret	Delete Row
	DNS Name Or IP Address	IP address			
□	193.180.23.77	193.180.23.77	1645		□

Create 1 new rows

RADIUS server

Enter the **DNS Name Or IP Address** for the RADIUS server used for authentication.

In **IP address**, the IP address of the server is shown. It is updated whenever **Look up all IP addresses again** is pressed, or the **DNS Name Or IP Address** field is changed.

Port

The official port for RADIUS is UDP port 1812. However, several RADIUS servers use port 1645, so you may have to change the port number either on the RADIUS server or in the table.

Secret

A RADIUS authentication requires a ’shared secret’, which must be the same on both sides. Since the secret is used as an encryption key, it is important that it is kept a secret. Since the secret is saved unencrypted in the Telecommuting Module configuration, you should be careful with where you store the configuration.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

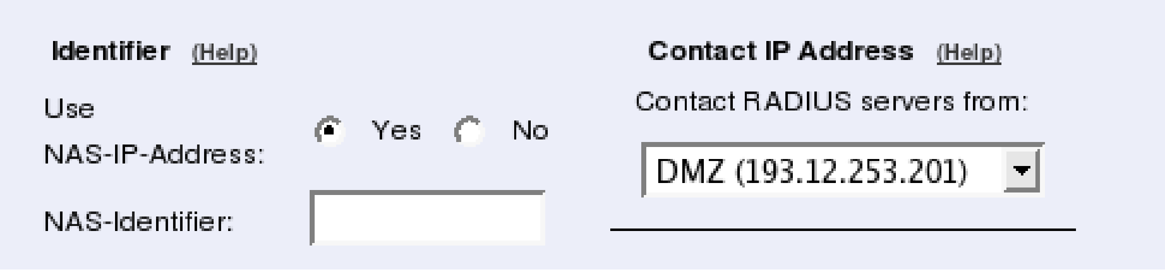
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Identifier

A RADIUS client may use either of two ways to identify itself for the RADIUS server: an IP address or a name (identifier). You must use at least one of these ways, or the authentication will fail.

Select here which method to use. The address or name in use must be registered at the RADIUS servers specified in the top table, and must be unique in that RADIUS database.



Use NAS-IP-Address: ● Yes ○ No

NAS-Identifier:

Contact RADIUS servers from: DMZ (193.12.253.201)

Use NAS-IP-Address

If you select **Yes**, the Telecommuting Module's IP address (the address selected under **Contact IP Address**) will be enclosed as identity. If you select **No**, you must enter a **NAS-Identifier** for the Telecommuting Module.

NAS-Identifier

You can enter a special identifier into this field. All characters except space are allowed according to the Telecommuting Module, but your RADIUS server may have some restrictions on the identifier.

Contact IP Address

Select the IP address from which the Telecommuting Module should make connections to RADIUS servers.

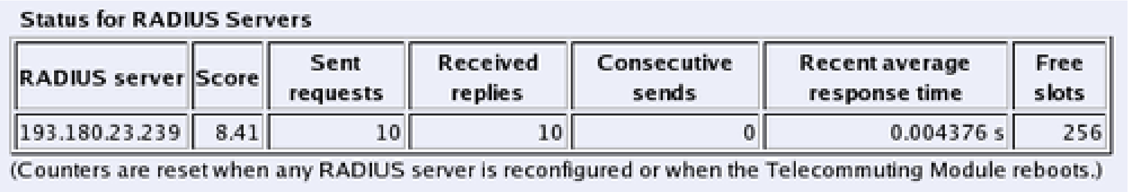
Contact RADIUS servers from

Select an IP address from which the Telecommuting Module should make connections to the RADIUS server. A convenient choice of address is one on the interface closest to the server. Select from the IP addresses configured for the Telecommuting Module interfaces under **Directly Connected Networks** and **Alias**.

Status for RADIUS Servers

At the bottom of the page the status for the RADIUS servers is shown. *Radiusmux* is the part of 3Com VCX IP Telecommuting Module that connects to the RADIUS servers.

If no authentication by RADIUS is configured, the radiusmux is not run. When you apply a configuration which involves contacting a RADIUS server, the radiusmux is started.



Status for RADIUS Servers

RADIUS server	Score	Sent requests	Received replies	Consecutive sends	Recent average response time	Free slots
193.180.23.239	8.41	10	10	0	0.004376 s	256

(Counters are reset when any RADIUS server is reconfigured or when the Telecommuting Module reboots.)

RADIUS server

The IP address for this RADIUS server.

Score

Radiusmux gives points (the scale is 1 to 40, inclusive) to the different servers according to their performance. The better server performance, the higher score. Radiusmux uses the score to select which server to query primarily.

Sent requests

The number of UDP packets sent to this server.

Received replies

The number of UDP packets received from this server.

Consecutive sends

The number of consecutive UDP packets sent without response from the server.

Recent average response time

A calculated average of response time for packets for which response has been received.

Free slots

The RADIUS server allocates a certain number of slots for each RADIUS client, and every pending request from the Telecommuting Module occupies a slot. Here you see the current number of free slots.

Save

Saves the RADIUS configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

Configuration of a RADIUS server

In this section it is assumed that you know how to configure your RADIUS server. Consult your RADIUS manual for details.

Add the Telecommuting Module as a client in the RADIUS server. Make sure that the shared secret here is the same as in the Telecommuting Module.

The Telecommuting Module checks the permissions for a user by looking at its RADIUS attribute *Service-Type*.

If the Service-Type has the value *Administrative (6)*, the user is allowed to configure the Telecommuting Module.

If the value is *Framed (2)*, the user is allowed to connect via VPN.

For the various privileges for users, there is an 3Com-specific RADIUS attribute defined thus:

```
VENDOR 3Com 43

ATTRIBUTE 3Com-Admin-Account 1 integer  3Com

#
#  Type of administrator account.
#
VALUE  3Com-Admin-Account Full-Access-Admin 1
VALUE  3Com-Admin-Account Backup-Admin  2
VALUE  3Com-Admin-Account Read-Only-Admin  3
VALUE  3Com-Admin-Account VPN-Admin  4
VALUE  3Com-Admin-Account SIP-Admin  5
VALUE         3Com-Admin-Account      VPN-Reneg-Admin 6
```

To be able to authenticate SIP users, the RADIUS server must support Digest authentication. You find a description of this in draft-sterman-aaa-sip-02 (Internet draft). This is all that is required for it to work with 3Com VCX IP Telecommuting Module.

More information about RADIUS can be found in RFC 2865.

SNMP

SNMP is a network monitoring protocol, which enables a single server to monitor one or more networks, including all network equipment like routers and firewalls. 3Com VCX IP Telecommuting Module supports SNMP and can accordingly be monitored automatically.

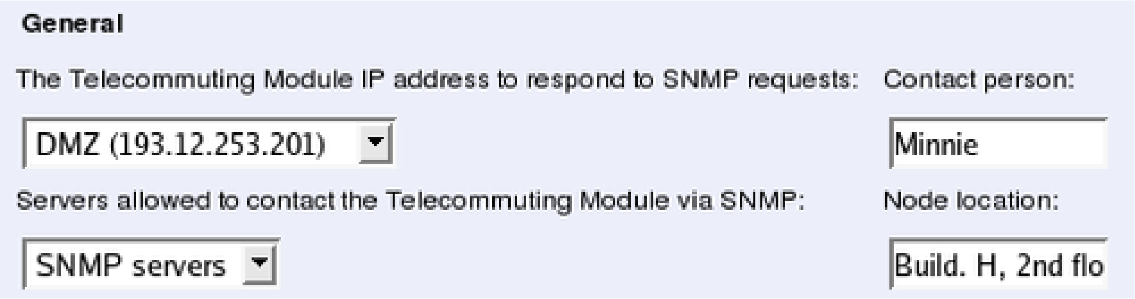
The monitoring signaling consists of two main parts. The SNMP server sends requests to the Telecommuting Module, which replies with a list of network parameters and their values for the Telecommuting Module. The Telecommuting Module can also send messages (traps) without the server prompting, when someone sends a request without valid authentication and when the Telecommuting Module boots. You can also configure the Telecommuting Module to send traps when certain threshold values are reached.

The 3Com VCX IP Telecommuting Module can only send parameters to the server; no changes of configuration can be made through SNMP requests.

For more information about SNMP, read RFC 1157.

General

Here, select the IP addresses (local and remote) involved in the SNMP signaling. You can also enter contact information for the Telecommuting Module.



General

The Telecommuting Module IP address to respond to SNMP requests: DMZ (193.12.253.201)

Contact person: Minnie

Servers allowed to contact the Telecommuting Module via SNMP: SNMP servers

Node location: Build. H, 2nd flo

The Telecommuting Module IP address to respond to SNMP requests

Select the IP address of the Telecommuting Module to which the SNMP servers should direct their requests. Select from the addresses defined on the **Interface** pages under **Network Configuration**.

Servers allowed to contact the Telecommuting Module via SNMP

Select the SNMP server(s) which are allowed to contact the Telecommuting Module. You select from the network groups defined on the **Networks and Computers** page under **Network Configuration**.

Contact person

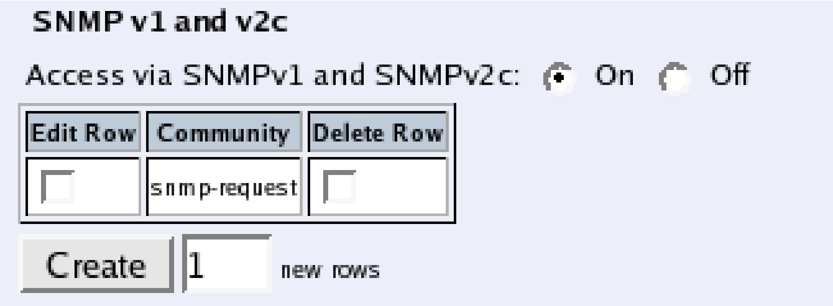
Enter the name of the contact person for this 3Com VCX IP Telecommuting Module. This information is sent with the parameter list as reply to an SNMP request from the server.

Node location

Enter the location of the Telecommuting Module. This information is sent with the parameter list as reply to an SNMP request from the server.

SNMP v1 and v2c

In SNMP version 1 and 2c, the authentication is managed through an unencrypted password, a *community*. Here, you select if the Telecommuting Module should accept access via v1 or v2c, and enter the valid communities.



SNMP v1 and v2c

Access via SNMPv1 and SNMPv2c: ● On ○ Off

Edit Row	Community	Delete Row
□	snmp-request	□

Access via SNMPv1 and SNMPv2c

Select if access via SNMP version 1 or 2c (using communities as the autentication method) should be **On** or **Off**.

Community

Enter a password. Note that this password is stored unencrypted.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

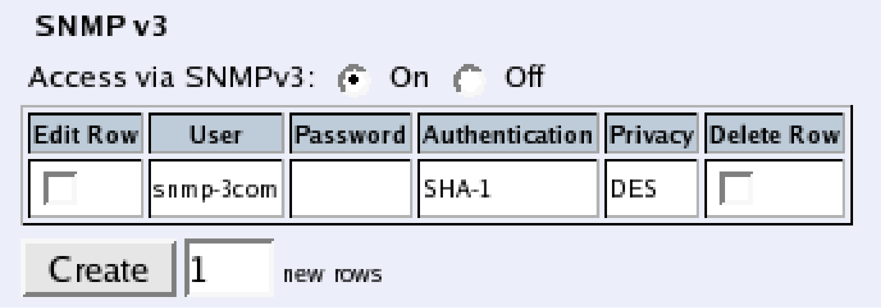
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

SNMP v3

In SNMP version 3, the authentication is managed through the server sending a username and an (in most cases) encrypted password to the Telecommuting Module, which verifies the validity of them.

Here, you select if the Telecommuting Module should accept access via v3, and select the authentication and encryption used for the SNMP reuqests.



SNMP v3

Access via SNMPv3: ● On ○ Off

Edit Row	User	Password	Authentication	Privacy	Delete Row
□	snmp-3com		SHA-1	DES	□

Access via SNMPv3

Select if access via SNMP version 3 (using usernames and encrypted passwords as the autentication method) should be **On** or **Off**.

User

Enter a username which the server should use when contacting the Telecommuting Module.

Password

Press the **Change password** button to enter a password for this user.

Authentication

Select the authentication algorithm to use for SNMP requests. 3Com VCX IP Telecommuting Module supports the **MD5** and **SHA-1** algorithms.

Privacy

Select whether the SNMP request should be encrypted using AES or DES, or not be encrypted at all.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

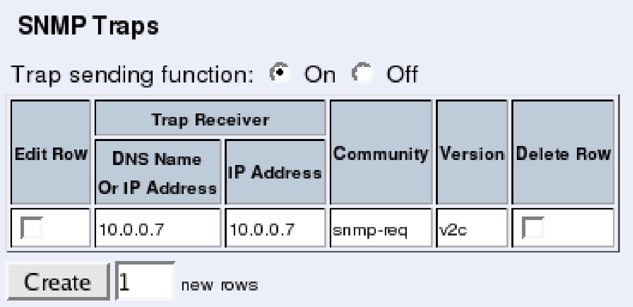
SNMP Traps

If **Trap sending function** is On, the Telecommuting Module will send messages (traps) to the server(s) entered below whenever an SNMP authentication fails or the Telecommuting Module boots. They are also sent when the status is changed for an IPsec tunnel, and when the Telecommuting Module discovers that a new software version is available.

You can also configure the unit to send traps when certain levels are reached (see Resource Monitoring).

SNMP traps are sent from the IP address closest to the receiving SNMP server. If the Telecommuting Module has been assigned more than one IP address on that network, the address given in the **Directly Connected Networks** table will be used.

If the trap sending is disabled, no traps will be sent.



SNMP Traps

Trap sending function: ● On ○ Off

Edit Row	Trap Receiver		Community	Version	Delete Row
	DNS Name Or IP Address	IP Address			
□	10.0.0.7	10.0.0.7	snmp-req	v2c	□

1 new rows

Trap sending function

Select if trap sending (at boot and failed SNMP authentication) should be **On** or **Off**.

Trap receiver

Enter the IP address, or a name in the DNS, of the server to which the Telecommuting Module should send traps. If you enter a DNS name instead of an IP address, you must enter the IP address of a DNS server on the **Basic Configuration** page.

IP address shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Community

Enter the password (community) which the Telecommuting Module should use when sending traps. The community is sent unencrypted over the network.

Version

Select the SNMP version to be used for traps. You can select v1 or v2c.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

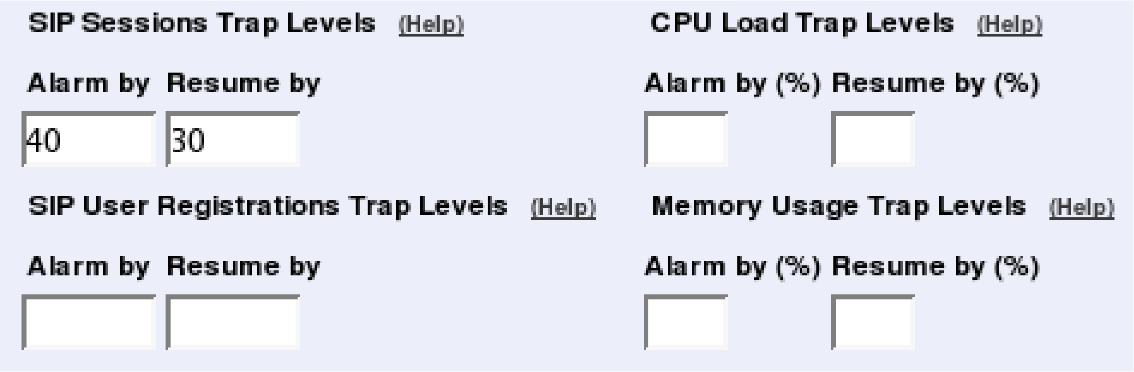
Enter the number of new rows you want to add to the table, and then click on **Create**.

Resource Monitoring

Your Telecommuting Module can send SNMP traps when usage passes certain levels. Set the levels here. The trap receivers are configured in the **SNMP Traps** table.

For each usage, there is an **Alarm by** and a **Resume by** level. When the usage hits the **Alarm by** level, the Telecommuting Module sends a trap about this and locks the trap sending for that usage, which means that as long as the level stays high, no more traps are sent. When the level goes down to below the **Resume by** level, the lock is released. Next time the **Alarm by** level is reached, a new trap is sent.

To avoid excessive trap sending, it is recommended that the **Alarm by** and **Resume by** levels for a resource are not set too close.



SIP Sessions Trap Levels (Help)

Alarm by: 40 Resume by: 30

SIP User Registrations Trap Levels (Help)

Alarm by: Resume by:

CPU Load Trap Levels (Help)

Alarm by (%): Resume by (%):

Memory Usage Trap Levels (Help)

Alarm by (%): Resume by (%):

SIP Sessions Trap Levels

Enter the SIP sessions levels here. When the number of SIP sessions reaches the Alarm by level, an SNMP trap is sent.

SIP User Registrations Trap Levels

Enter the SIP user registrations levels here. When the number of registered SIP users reaches the Alarm by level, an SNMP trap is sent.

CPU Load Trap Levels

Enter the CPU load levels here. When CPU usage increases above the Alarm by limit, an SNMP trap is sent.

Memory Usage Trap Levels

Enter the memory usage levels here. When memory usage increases above the Alarm by limit, an SNMP trap is sent.

Download the 3Com MIB

This link leads to the 3Com-specific MIB (Management Information Base) definition for your 3Com VCX IP Telecommuting Module.

The Telecommuting Module also supports these standard MIBs:

- mibII.system
- mibII.interfaces
- mibII.at
- mibII.ip
- mibII.icmp
- mibII.tcp
- mibII.udp
- mibII.snmp

Save

Saves the SNMP configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

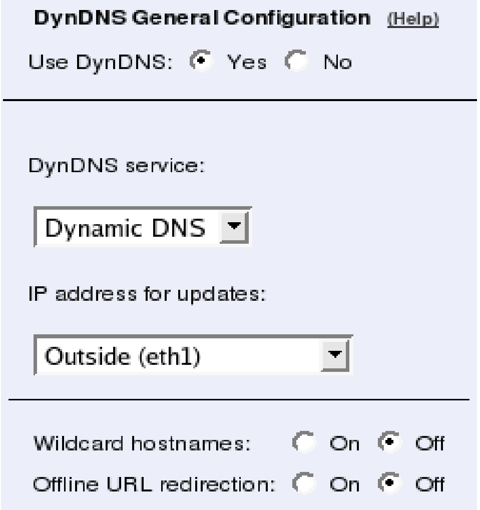
Dynamic DNS update

Usually, static DNS servers are used to associate a domain or host name with an IP address. If the Telecommuting Module gets its public IP address via DHCP or PPPoE, the static DNS servers will not work, as they do not automatically change bindings when the Telecommuting Module get a new IP address.

3Com VCX IP Telecommuting Module supports dynamic DNS update at DynDNS.org. You must purchase the update service at DynDNS.org before you can use it.

DynDNS General Configuration

Here, make settings which the Telecommuting Module will use when updating IP addresses at DynDNS.org. In the descriptions below, the example domain *example.com* is used.



DynDNS General Configuration (Help)

Use DynDNS: ● Yes ○ No

DynDNS service:

Dynamic DNS

IP address for updates:

Outside (eth1)

Wildcard hostnames: ○ On ● Off

Offline URL redirection: ○ On ● Off

Use DynDNS

Select if the Telecommuting Module should use DynDNS services to update IP addresses.

DynDNS service

Select which service you use at DynDNS.

IP address for updates

Select the IP address which the Telecommuting Module should send to dyndns.org. If a dynamic IP address is selected, the Telecommuting Module will update the DynDNS service every time the address changes.

Wildcard hostnames

If you select to turn this feature **On**, all DNS queries for any hostname.*example.com* will return your IP address. If this feature is **Off**, only queries for *example.com* will return your IP address.

Offline URL redirection

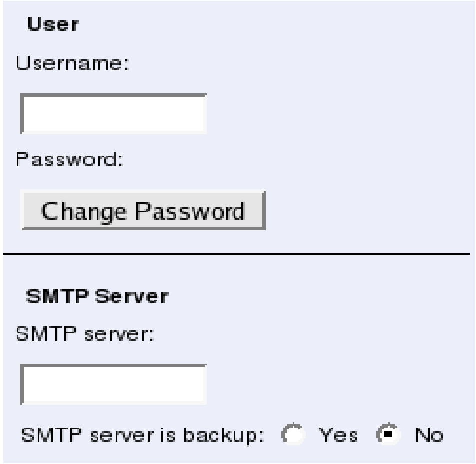
If **Offline URL redirection** is on, queries for your domain will be redirected to another URL if your server is down. The URL is entered on the dyndns.org web site. If no URL is set, queries will be redirected to a general web page at dyndns.org.

This is an add-on service at DynDNS.

User, SMTP Server

Enter user details needed when the Telecommuting Module updates information at dyndns.org.

You can also enter an SMTP server to report to DynDNS.



User

Username:

Password:

Change Password

SMTP Server

SMTP server:

SMTP server is backup: ○ Yes ● No

Username

Enter your DynDNS.org username. This is needed when the Telecommuting Module updates its IP address.

Password

Press the button to enter your DynDNS.org password. This is needed when the Telecommuting Module updates its IP address.

SMTP server

Enter the host name of your SMTP server. This is the name that SMTP DNS queries for *example.com* should return.

You can’t enter an IP address here; neither can you enter a host name that is a CNAME (a kind of DNS alias), but must enter the server’s primary name.

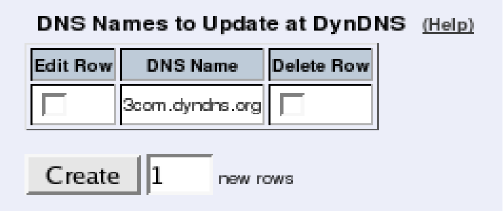
SMTP server is backup

If you selected **No** here, the DynDNS server will assume that the SMTP server entered above is the primary email server for *example.com*.

If you selected **Yes**, the DynDNS server will assume that your primary email server is the one associated with the DNS name *example.com*, and that the SMTP server entered above is a backup server to take over when the primary server is unreachable.

DNS Names to Update at DynDNS

Enumerate the domain and host names that should be connected to the IP address selected above. If **Wildcard hostnames** was selected as On, you only need to enter domain names; the DynDNS server will return the same IP address for every hostname under the domain. If it is Off, you need to enter every hostname separately.



DNS Names to Update at DynDNS (Help)

Edit Row	DNS Name	Delete Row
□	3com.dyndns.org	□

DNS Name

Enter the DNS name to be associated to the Telecommuting Module IP address.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the Dynamic DNS update configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Certificates

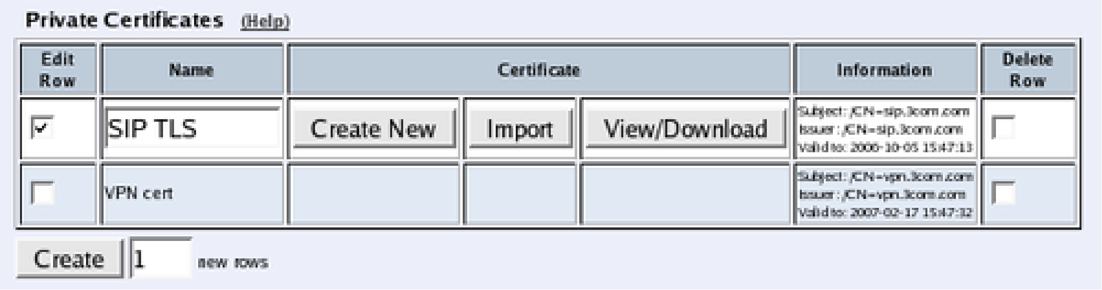
Here, you create X.509 certificates for the Telecommuting Module, to be used for authentication in various applications, like when configuration over HTTPS is performed.

On this page you also upload CA certificates to the Telecommuting Module. For the applications (HTTPS, VPN, RADIUS authentication of road warriors, and SIP over TLS), you select one or more CA certificates to trust.

You do not upload certificates here for IPsec peers where you have the peer's own certificate (as opposed to a CA certificate). These certificates are uploaded on the **IPsec Peers** page.

Private Certificates

Here the private X.509 certificates of the Telecommuting Module are created. You can use the same certificate for all authentication purposes, or create different certificates for the various functions in the Telecommuting Module.



Private Certificates (Help)

Edit Row	Name	Certificate			Information	Delete Row
☑	SIP TLS	Create New	Import	View/Download	Subject: /CN=sip.3com.com Issuer: /CN=sip.3com.com Valid to: 2006-10-05 15:47:13	□
□	VPN cert				Subject: /CN=vpn.3com.com Issuer: /CN=vpn.3com.com Valid to: 2007-02-17 15:47:32	□

Create 1 new rows

Name

Enter a name for this certificate. The name is only used internally in the Telecommuting Module.

Certificate

Create, import or download a private certificate. See more information about creating certificates below. Under **Import**, you upload Telecommuting Module certificates signed by an external CA.

Under **View/Download**, you download the private certificate, and you can also download the key pair.

Information

Information about this certificate, such as the signing CA and expiration date.

Delete Row

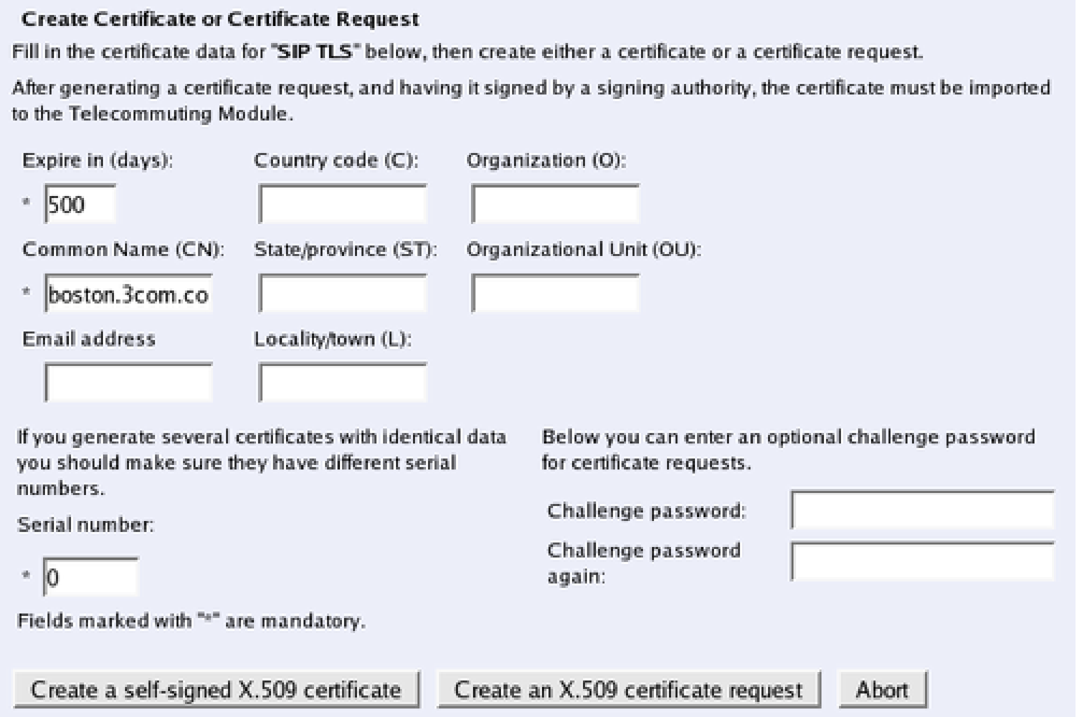
If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Create certificate or certificate request

Press **Create New** to create a new X.509 certificate. A new page with a form appears, requesting information about the Telecommuting Module. Fill in the form to apply for a certificate or create a self-signed certificate. Fields marked * are mandatory.



Create Certificate or Certificate Request

Fill in the certificate data for "SIP TLS" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the Telecommuting Module.

Expire in (days): * 500

Country code (C):

Organization (O):

Common Name (CN): * boston.3com.co

State/province (ST):

Organizational Unit (OU):

Email address

Locality/town (L):

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number: * 0

Fields marked with "*" are mandatory.

Below you can enter an optional challenge password for certificate requests.

Challenge password:

Challenge password again:

Create a self-signed X.509 certificate
Create an X.509 certificate request
Abort

Expire in

The expiration time defines how many days the certificate will last. Default time is 365 days, one year.

Common Name

Here, you enter the host name or IP address of the Telecommuting Module.

Email address

Enter the email address of the Telecommuting Module administrator.

Country code

Here, you enter the country code - not the top domain - for the country where the Telecommuting Module is located. The country code for the USA is US.

State/province

The state or province where the Telecommuting Module is located.

Locality/town

The city or town where the Telecommuting Module is located.

Organization

The name of the organization/company owning the Telecommuting Module.

Organizational Unit

The department using the Telecommuting Module.

Serial number

If you generate more than one certificate with the same information, and you want to give them separate names and treat them as different certificates, you need to give them different serial number. Enter a serial number for this certificate here.

Challenge password

Enter a password. This will be used only when revoking a signed certificate.

Create a self-signed X.509 certificate

By entering the requested information above and pressing this button, you can create a certificate that isn't signed by any certificate authority (CA). Self-signed certificates are for free, while certificates signed by an official CA normally are not. Certificates signed by CAs are automatically accepted by web browsers, while you have to accept self-signed certificates manually when using them in your web browser.

Create an X.509 certificate request

When pressing this button, you make a certificate request which can be sent to a certificate authority for signing. The request is downloaded under **View/Download** on the certificate page. The signed certificate is uploaded under **Import**.

Abort

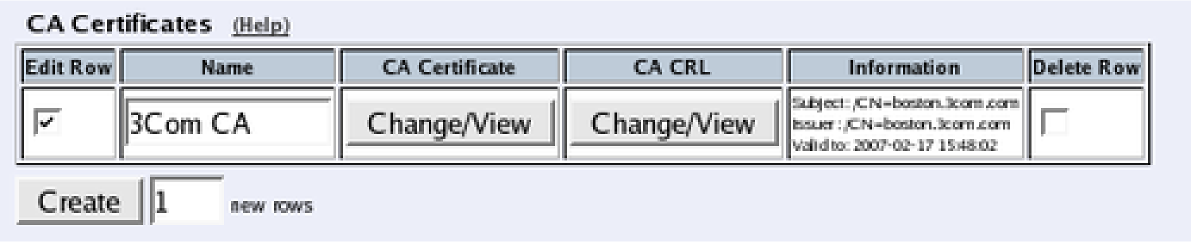
Press the **Abort** button to return to the **Certificates** page without creating a new certificate or certificate request.

CA Certificates

Here, you upload CA certificates and CRLs (Certificate Revocation Lists).

The CAs are used to authenticate peers using IPsec VPN or TLS. Upload one or more CA certificates here, and then select which CAs to trust for each function in the Telecommuting Module.

CRLs are used to let the Telecommuting Module know that some of the certificates signed by a certain CA should not be accepted. This could be useful when laptops with certificates are stolen. See instructions for your CA on how to make a CRL.



CA Certificates (Help)

Edit Row	Name	CA Certificate	CA CRL	Information	Delete Row
☑	3Com CA	Change/View	Change/View	Subject: /CN=boston.3com.com Issuer : /CN=boston.3com.com Valid to: 2007-02-17 15:48:02	□

Name

Enter a name for this CA certificate. The name is only used internally in the Telecommuting Module.

CA Certificate

You upload the CA certificate to the Telecommuting Module, inspect the current certificate, or download it to use somewhere else, by pressing the **Change/View** button.

CA CRL

A CRL (Certificate Revocation List) is used to tell the Telecommuting Module that some certificates issued by this CAs are not valid, even though they may not have expired yet. Upload a CRL for this CA by pressing the **Change/View** button.

Information

Information about this certificate, such as the signing CA and expiration date.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves all Certificates configuration to the preliminary configuration.

Cancel

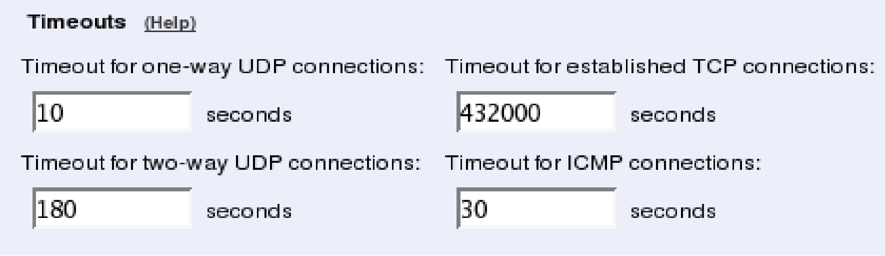
Clears and resets all fields in new rows and resets changes in old rows.

Advanced

Timeouts

The Telecommuting Module saves information (for example NAT information) about all connections made to other units. Here, you can set timeouts for different types of connections. The timeout defines how long the Telecommuting Module should wait after sending or receiving a packet for the connection before it discards the information about the connection.

Long timeouts consume memory for all connections.



Timeouts (Help)

Timeout for one-way UDP connections: 10 seconds

Timeout for established TCP connections: 432000 seconds

Timeout for two-way UDP connections: 180 seconds

Timeout for ICMP connections: 30 seconds

Timeout for one-way UDP connections

The **Timeout for one-way UDP connections** regards UDP connections where packets have only been sent in one direction.

Timeout for two-way UDP connections

The **Timeout for two-way UDP connections** regards UDP connections where packets have been sent in both directions.

Timeout for established TCP connections

The **Timeout for established TCP connections** regards TCP connections where the three-way (SYN, SYN+ACK, ACK) handshake has been completed, which means that the connection is fully established.

Timeout for ICMP connections

The **Timeout for ICMP connections** regards ICMP connections, like ping.

Save

Saves the Advanced configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Telecommuting Module Type

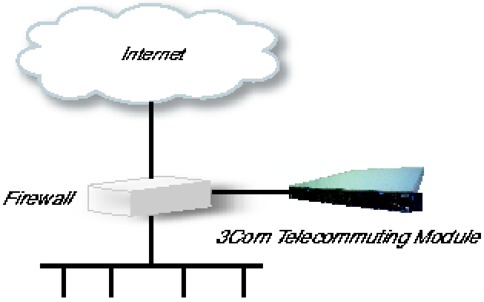
The Telecommuting Module can be connected to your network in different ways, depending on your needs. On this page, you state what configuration you have.

DMZ Configuration

Using this configuration, the Telecommuting Module is located on the DMZ of your firewall, and connected to it with only one interface. The SIP traffic finds its way to the Telecommuting Module using DNS or by setting the Telecommuting Module as an outbound proxy on the clients.

This is the most secure configuration, since all traffic goes through both your firewall and your Telecommuting Module. It is also the most flexible, since all networks connected to any of your firewall's interfaces can be SIP-enabled.

The drawback is that the SIP traffic will pass the firewall twice, which can decrease performance.



On your firewall, you need to open the SIP port (normally UDP port 5060) and a range of UDP ports for RTP traffic between the Telecommuting Module and the Internet as well as between the Telecommuting Module and your internal networks. The SIP traffic finds its way to the Telecommuting Module using DNS or by setting the Telecommuting Module as an outbound proxy on the clients.

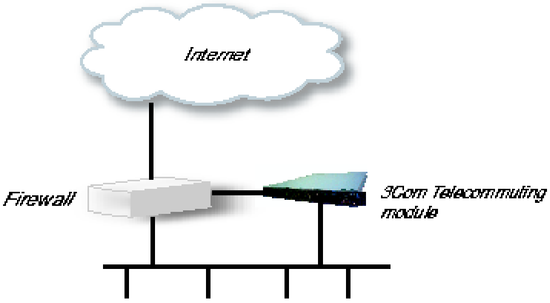
The firewall mustn't use NAT for the traffic between the Telecommuting Module and your internal networks or for the traffic between the Telecommuting Module and the Internet. However, the Telecommuting Module can itself use NAT for traffic to the Internet.

You need to declare your internal network topology on the **Surroundings** page.

DMZ/LAN Configuration

Using this configuration, the Telecommuting Module is located on the DMZ of your firewall, and connected to it with one of the interfaces. The other interfaces are connected to your internal networks. The Telecommuting Module can handle several networks on the internal interface even if they are hidden behind routers.

This configuration is used to enhance the data throughput, since the traffic only needs to pass your firewall once.



On your firewall, you need to open the SIP port (normally UDP port 5060) and a range of UDP ports for RTP traffic between the Telecommuting Module and the Internet. The other interface is connected to your internal network. The Telecommuting Module can handle several networks on the internal interface even if they are hidden behind routers. No networks on other interfaces on the firewall can be handled.

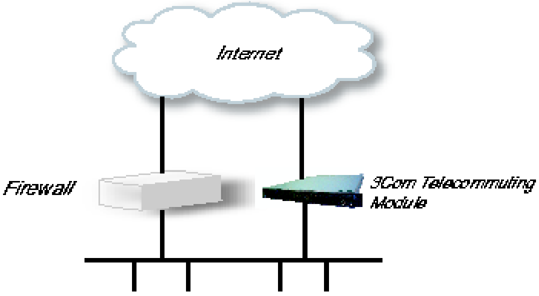
Internal users have to configure the Telecommuting Module as outbound proxy, or an internal proxy has to use the Telecommuting Module as outbound proxy.

The Telecommuting Module derives information about your network topology from the interface configuration.

Standalone Configuration

Using this configuration, the Telecommuting Module is connected to the outside on one interface and your internal networks on the others.

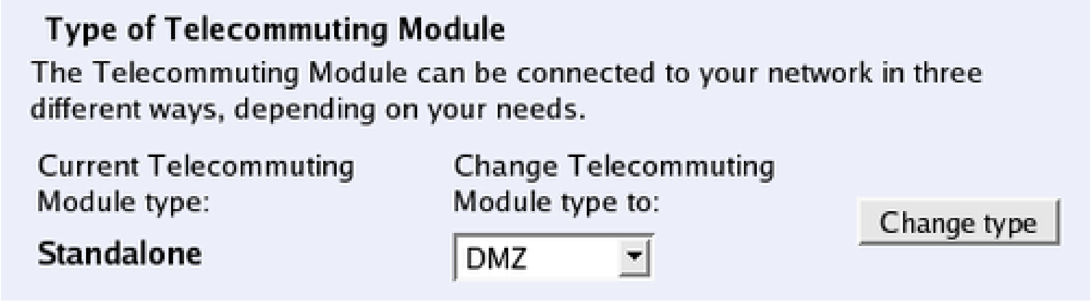
Use this configuration only if your firewall lacks a DMZ interface, or for some other reason cannot be configured for the DMZ or DMZ/LAN alternatives.



Internal users have to configure the Telecommuting Module as outbound proxy, or an internal proxy has to use the Telecommuting Module as outbound proxy. No change in the firewall configuration is needed.

The Telecommuting Module derives information about your network topology from the interface configuration.

Telecommuting Module Type configuration



Type of Telecommuting Module

The Telecommuting Module can be connected to your network in three different ways, depending on your needs.

Current Telecommuting Module type: **Standalone**

Change Telecommuting Module type to: DMZ

Current Telecommuting Module Type

Shows which type is currently active.

Change Telecommuting Module Type to

Select a new Telecommuting Module Type here.

Change type

Press the **Change type** button to set the new Telecommuting Module Type. This setting, like others, must be applied on the **Save/Load Configuration** page before it affects the Telecommuting Module functionality.

Chapter 7. Administration

Under Administration, you

- apply your configuration
- define administrator users and change their passwords
- save the preliminary configuration to file
- load a saved configuration
- view the configuration
- reboot your 3Com VCX IP Telecommuting Module
- restart the SIP module on your 3Com VCX IP Telecommuting Module
- upgrade your 3Com VCX IP Telecommuting Module
- set table formats
- set date, time, and time zone (manually or via NTP)

Save/Load Configuration

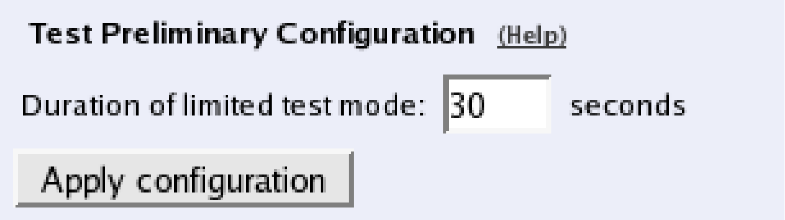
Here, you work with the preliminary and permanent configurations, save them and load new configurations from previously saved configurations.

Test Preliminary Configuration

The settings you make in the web GUI will not be used automatically, but you must apply them first. When there are settings which are not yet applied, a warning about this will be shown on the web pages.

When **Apply configuration** is pressed, the Telecommuting Module will test the configuration before you make it permanent.

During test, the Telecommuting Module waits for you to press one of the three buttons displayed. If you never see the three buttons, something in your preliminary configuration (now tested) is wrong, which makes it impossible for you to access the configuration web interface.



Test Preliminary Configuration (Help)

Duration of limited test mode: 30 seconds

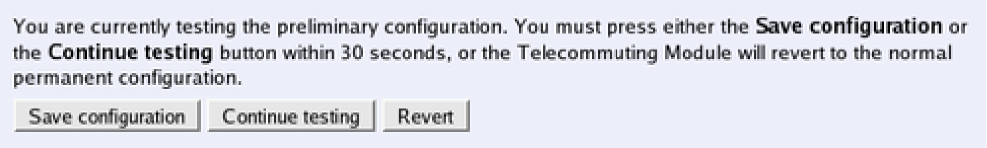
Duration of limited test mode

Here, you enter the time limit for the testing. If you do not press any button within this time, the Telecommuting Module will assume that some part of your preliminary configuration makes connecting impossible. When the timeout is reached, the Telecommuting Module automatically reverts to the old permanent configuration. If this occurs, you will be informed when trying to press a button.

Apply configuration

Saves the preliminary configuration to the permanent configuration and puts it into use. You can test your preliminary configuration before finalizing it.

Three buttons are displayed during the test:



You are currently testing the preliminary configuration. You must press either the **Save configuration** or the **Continue testing** button within 30 seconds, or the Telecommuting Module will revert to the normal permanent configuration.

Save configuration saves your preliminary configuration to the permanent configuration and puts it into use.

Continue testing shows a new page with only the other two buttons.

Revert cancels this test of the preliminary configuration without saving.

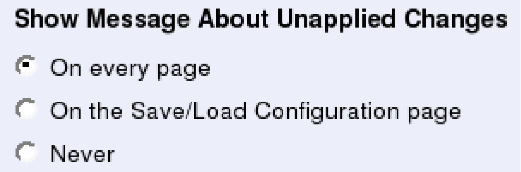
If you do not press any button within the time limit, the Telecommuting Module will revert to the old permanent configuration, just as if you had pressed **Revert**. This is useful if you happen to configure your Telecommuting Module so it isn't accessible from your browser.

After the timeout, pressing either of the three buttons will show a new page which will inform you that the test run was aborted.

Restarting the Telecommuting Module by cycling the power also cancels the test.

Show Message About Unapplied Changes

When there are settings which are not yet applied, a warning about this will be shown on the web pages. Select here where this message should be shown. The options are **On every page**, **On the Save/Load Configuration page** (this page) and **Never**.



Show Message About Unapplied Changes

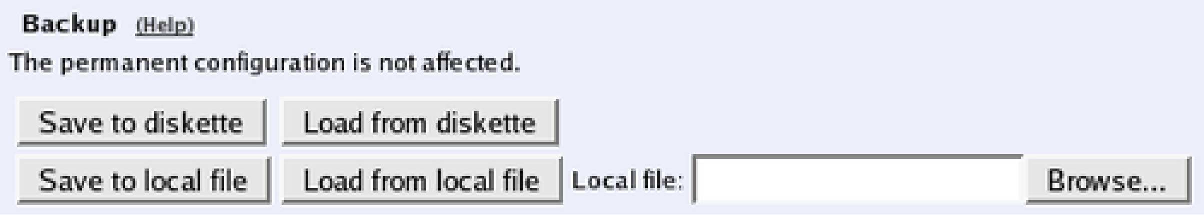
● On every page

○ On the Save/Load Configuration page

○ Never

Backup

All configurations can be saved to and loaded from diskette or file. This does not affect the permanent configuration.



Backup (Help)

The permanent configuration is not affected.

Local file:

Save to diskette

Insert a formatted diskette into the Telecommuting Module's floppy drive and press **Save to diskette** to save the preliminary configuration. Do not remove the diskette until the light on the floppy drive goes out.

Check that you get a confirmation of the saving. If not, the diskette may be faulty.

Load from diskette

Insert the diskette with the saved configuration into the Telecommuting Module's floppy drive and press **Load from diskette**. Do not remove the diskette until the light on the floppy drive goes out. The contents of the diskette are now loaded in the preliminary configuration.

Save to local file

Press **Save to local file** to save the preliminary configuration to the file you have selected. A new window is opened where you enter the name of the file.

Load from local file

Press **Load from local file** to load a new preliminary configuration from the file you have selected.

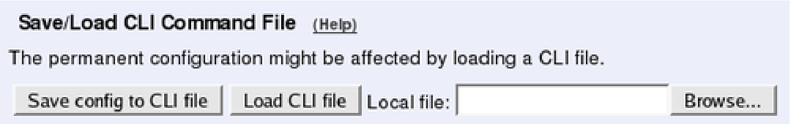
Browse

Browse is used to scan your local disk. The web browser opens a new window where you can search among files and directories. Go to the right directory and select the file you want to upload.

Save/Load CLI Command File

All configurations can be saved to and loaded from a CLI file (see chapter 18, Command Line Reference, for more information about the CLI). You can also edit the CLI file before it is uploaded again.

Uploading a CLI file might affect the permanent configuration, as the CLI file can contain commands that applies the configuration.



Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file

Press **Save config to CLI file** to save the preliminary configuration to the file you have selected. A new window is opened where you enter the name of the file.

Load CLI file

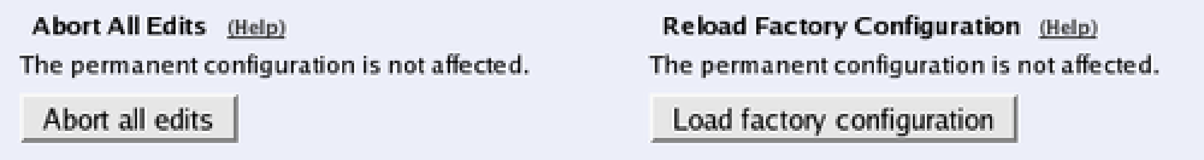
Press **Load CLI file** to upload a CLI file to the Telecommuting Module.

Browse

Browse is used to scan your local disk. The web browser opens a new window where you can search among files and directories. Go to the right directory and select the file you want to upload.

Revert to Old Configurations

You can revert to old configurations of the Telecommuting Module, either back to the last configuration successfully applied, or to the configuration delivered with your Telecommuting Module from the factory.



Abort All Edits (Help)

The permanent configuration is not affected.

Reload Factory Configuration (Help)

The permanent configuration is not affected.

Abort All Edits

Abort all edits copies the permanent configuration to the preliminary configuration. All changes made in the preliminary configuration are deleted.

Reload Factory Configuration

The factory configuration is the standard configuration that is delivered with a Telecommuting Module. Click on this button to load this configuration into the preliminary configuration. The permanent configuration is not affected.

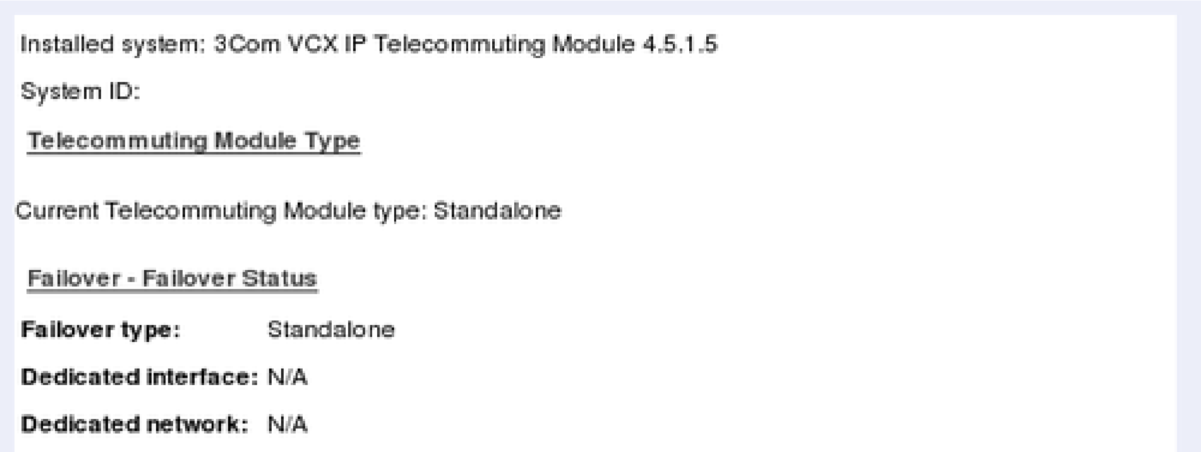
Show Configuration

Shows both the preliminary and permanent configurations, in that order. Before the preliminary configuration, you see the Telecommuting Module's version, serial number, the time zone and table format you selected.

If there are any differences between the preliminary and the permanent configuration, the message "This setting has been changed but not applied." will be shown in red at the setting in question, in the Preliminary section. If there are any errors in the preliminary configuration, this will also be marked in red in the Preliminary section.

The heading before each table for the preliminary configuration is clickable and accesses the corresponding configuration page.

Print this list from your web browser and store it in a safe place.



Installed system: 3Com VCX IP Telecommuting Module 4.5.1.5

System ID:

Telecommuting Module Type

Current Telecommuting Module type: Standalone

Failover - Failover Status

Failover type: Standalone

Dedicated interface: N/A

Dedicated network: N/A

User Administration

On the **User Administration** page, you change the administration password for the *admin* account on your Telecommuting Module and create other administrator user accounts. The characters in the password are displayed as little stars. Remember that the password is sent unencrypted over the network if you use HTTP instead of HTTPS.

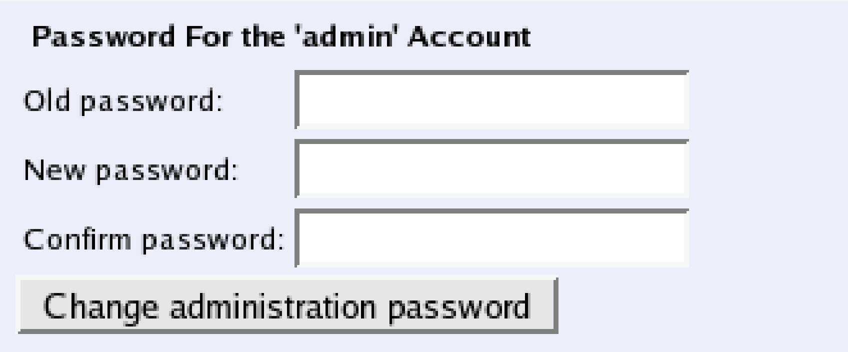
Settings made on this page (the admin password and other accounts) will not be included when saving the configuration to file. This means that you cannot move accounts defined on one Telecommuting Module onto another one.

You can authenticate administrators using a RADIUS server instead of a local password (select this on the **Access Control** page under **Basic Configuration**). When RADIUS is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

More information about how to configure the RADIUS server to authenticate administrators can be found in the RADIUS section.

Password For the ’admin’ Account

The *admin* user is predefined. That user can make changes, load configurations, apply configurations and log on the Telecommuting Module via the serial cable. You can’t remove this user or change its privileges, only change its password.



Password For the 'admin' Account

Old password:

New password:

Confirm password:

Old password

Enter the old password for the *admin* user.

New password, Confirm password

Enter the new password in both fields. You must enter the exact same password in both fields, to make sure that you did not make a mistake.

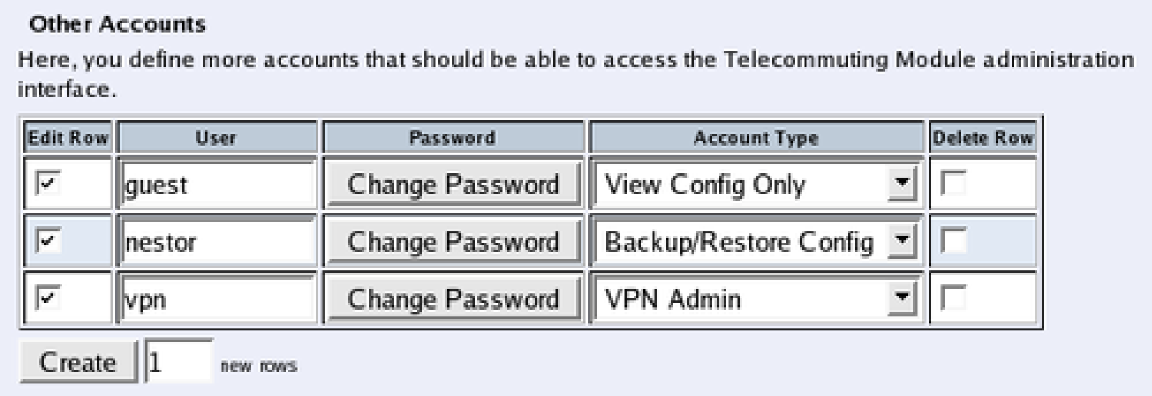
Change administration password

Click on this button to change the password for the *admin* user. The new password is now saved on the Telecommuting Module.

Other Accounts

Here, you define other user accounts that can access the Telecommuting Module. A user account can be restricted to only look at settings, or to change only some settings. Changes of configuration are logged by user name.

Changes in restrictions for an existing user account are immediate. The exception is changes for a currently logged on user, for which the changes will have effect the next time he/she logs on.



Other Accounts

Here, you define more accounts that should be able to access the Telecommuting Module administration interface.

Edit Row	User	Password	Account Type	Delete Row
☑	guest	Change Password	View Config Only	□
☑	nestor	Change Password	Backup/Restore Config	□
☑	vpn	Change Password	VPN Admin	□

User

Enter the user name for this account. The name is used when the user logs on and for logging the changes.

Password

Press the **Change password** button to enter the password for this user.

Account Type

Select what privileges this user should have.

Full Access means that the user can make any changes to the configuration. This is the same privileges as the *admin* user has in the web GUI, but only the *admin* user can log on via the serial cable.

Backup/Restore Config means that the user can download the configuration to file, and upload a configuration file to the Telecommuting Module. The user is also allowed to apply configurations.

VPN Admin means that the user can make any changes on the **Virtual Private Networks** pages and apply configurations, but can’t change any other configuration.

VPN Renegotiator means that the user is allowed to press the **Renegotiate IPsec tunnels** button to negotiate new IPsec tunnels, but can’t change any configuration.

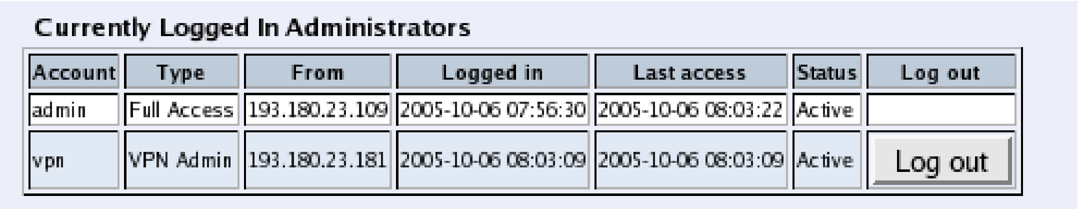
SIP Admin means that the user can make any changes on the **SIP Services** and **SIP Traffic** pages and apply configurations, but can’t change any other configuration.

View Config Only means that the user can view any configuration and make log searches, but can’t change any configuration.

Off means that the user is not allowed to log on to the web interface of the Telecommuting Module.

Currently Logged In Administrators

Here, all users logged on the Telecommuting Module web interface are shown. If your user has full access, you can log out other users here.



Currently Logged In Administrators

Account	Type	From	Logged in	Last access	Status	Log out
admin	Full Access	193.180.23.109	2005-10-06 07:56:30	2005-10-06 08:03:22	Active	
vpn	VPN Admin	193.180.23.181	2005-10-06 08:03:09	2005-10-06 08:03:09	Active	Log out

Account

The name of the logged on user.

Type

Here, the account type for the user is shown. The account type tells you the user’s access rights for the Telecommuting Module web interface.

From

Here you see from which IP address the user connected to the Telecommuting Module.

Logged In

Here you see when the user logged on to the Telecommuting Module.

Last Access

Here you see when the user last accessed the Telecommuting Module web interface. Accesses could be a change of a parameter, a change of web page or a log search.

Status

Here you see if the user is active or idle. The Telecommuting Module marks a user as idle if the user has not accessed the web interface in ten minutes.

Log Out

If your user has full access to the web interface, you can log out other users. However, if you do not change their password (or change the Account type to Off), they can just log on again.

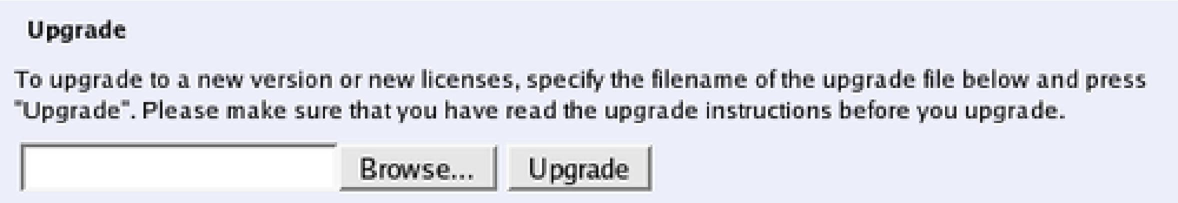
Upgrade

Read these instructions carefully before upgrading. You find version upgrades for 3Com VCX IP Telecommuting Module at http://www.3com.com/voip/. The upgrade is signed with GNU Privacy Guard. When 3Com VCX IP Telecommuting Module is upgraded, it automatically checks the signing before accepting the upgrade.

You should always upgrade your Telecommuting Module to the latest version.

Here, you also upgrade with extension modules (e.g. QoS) and SIP licenses. Upgrading with modules and licenses is exactly the same procedure as upgrading to a new version.

You save the upgrade to a file on your workstation or network file system. When upgrading, select **Upgrade**.



Upgrade

To upgrade to a new version or new licenses, specify the filename of the upgrade file below and press "Upgrade". Please make sure that you have read the upgrade instructions before you upgrade.

Upgrade

This is the procedure to follow when upgrading an 3Com VCX IP Telecommuting Module.

Step 1

First save the upgrade to a file on your workstation. Enter the file name and path in the box or press **Browse** to search the disk. When you have selected a file, press **Upgrade**. The Telecommuting Module will read the upgrade file and check that it was correctly signed and is compatible with the current Telecommuting Module version.

Step 2

If the upgrade file is correct, a text will appear at the top of the web page, informing about what version the upgrade is. Two new buttons will also be shown; **Apply upgrade** and **Remove upgrade**. You can still load new upgrades replacing the old one, which is useful if you for example have selected an upgrade which is too old.

Apply upgrade

Pressing **Apply upgrade** will make the Telecommuting Module install the new upgrade.

Remove upgrade

Remove upgrade removes the loaded upgrade from the Telecommuting Module. The upgrade will not be installed.

Step 3

If **Apply upgrade** was pressed, the buttons **Try the upgrade** and **Remove upgrade** will appear.

Try the upgrade

Try the upgrade will reboot the Telecommuting Module and test the loaded upgrade. When the reboot is done, log on to continue upgrading the Telecommuting Module.

Remove upgrade

Remove upgrade removes the loaded upgrade from the Telecommuting Module. The upgrade will not be installed.

Step 4

When you have pressed **Try the upgrade** and the Telecommuting Module has rebooted, you will see two buttons on top of every web page: **Accept upgrade** and **Abort upgrade**.

Now, you can choose to make the upgrade permanent or to revert to the old version. You can check the configuration, but no changes can be done before the upgrade is permanent. If the Telecommuting Module is rebooted before the upgrade is made permanent, it will revert to the old version.

Accept upgrade

Accept upgrade will complete the upgrade. When you have accepted the upgrade, you must also go to **Save/Load Configuration** and **Apply configuration**, i. e. the new upgrade.

Abort upgrade

Abort upgrade aborts the upgrade. The Telecommuting Module will revert to the old version.

Downgrade

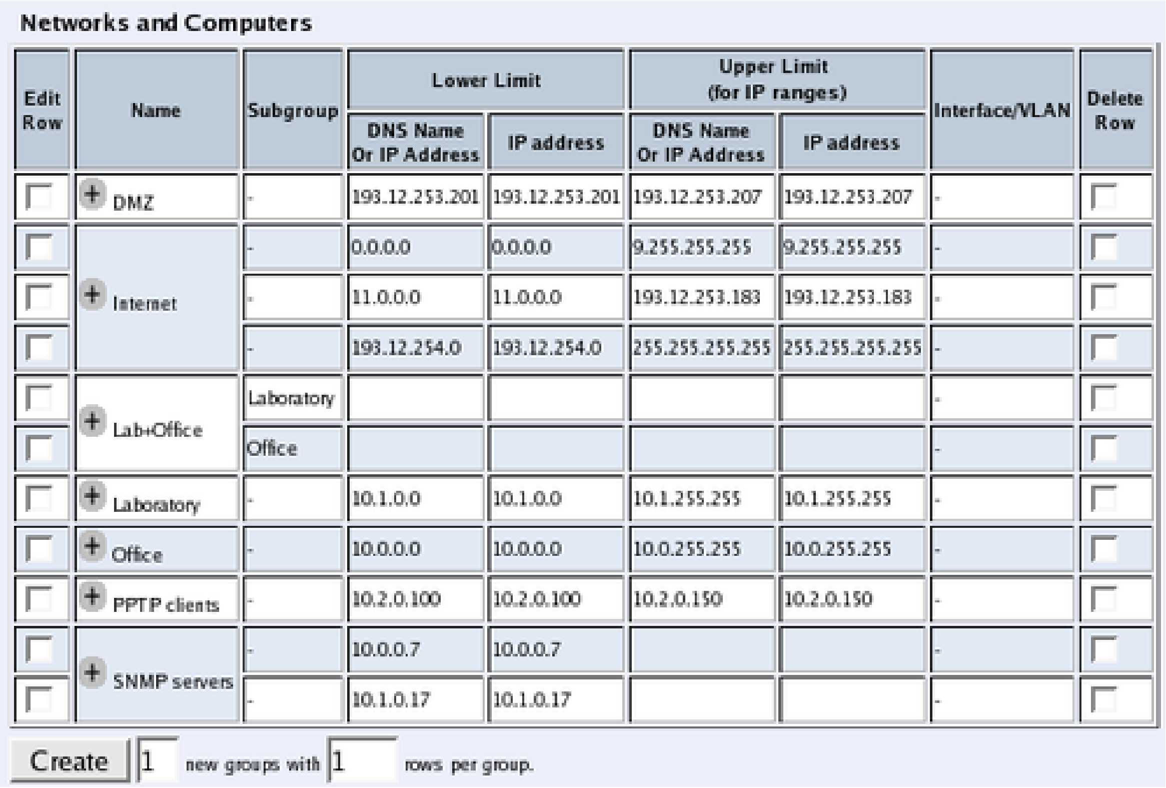
If the Telecommuting Module has been upgraded before, it is possible to downgrade to the previous version.

When you downgrade, the Telecommuting Module will revert to the configuration it had before upgrading. All configuration changes made after the upgrade will be lost.

When you want to upgrade, the upgrade file must be uploaded again.

Table Look

There are two alternatives for tables in 3Com VCX IP Telecommuting Module: Either you can change the contents of the table directly, or else you must click on a box in the **Edit Row** column to allow the row to be changed. The image below shows how tables with an **Edit Row** column can look.



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name Or IP Address	IP address	DNS Name Or IP Address	IP address		
□	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	□
□	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	□
□		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	□
□		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	□
□	+ Lab+Office	Laboratory					-	□
□		Office					-	□
□	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	□
□	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	□
□	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	□
□	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	□
□		-	10.1.0.17	10.1.0.17			-	□

Create [1] new groups with [1] rows per group.

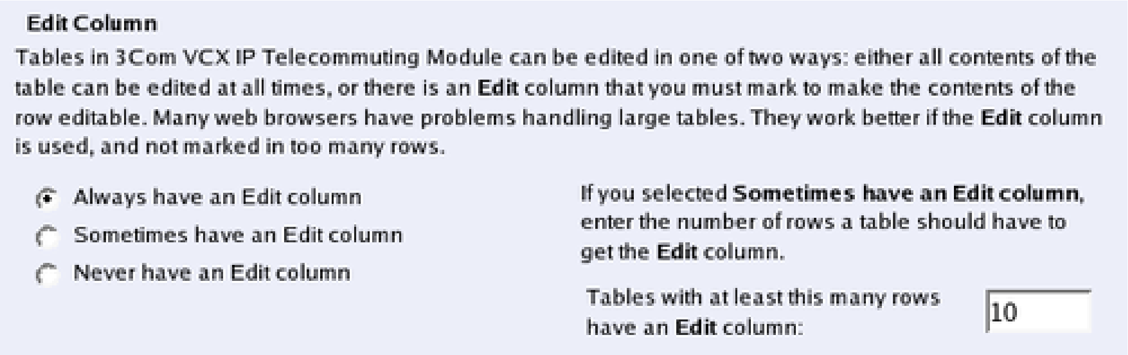
To change a row, click in the **Edit Row** box for that row and click on **Save**, **Add new rows**, or the tab for the desired configuration page. The page is updated so that you can change the configurations on the row. You can select several rows to change.

With an Edit Row column, tables with many rows are loaded faster, provided that only few of the Edit Row boxes are checked.

Edit Column

Select if all, some or none of the Telecommuting Module tables should have an Edit Row column. If you select that some tables have an Edit Row column, you also enter the size required to add the Edit Row column.

If a table has an Edit Row column, and the **Edit Row** check box is not checked for one row, this row will still be editable if there are any errors on the row.



Edit Column

Tables in 3Com VCX IP Telecommuting Module can be edited in one of two ways: either all contents of the table can be edited at all times, or there is an **Edit** column that you must mark to make the contents of the row editable. Many web browsers have problems handling large tables. They work better if the **Edit** column is used, and not marked in too many rows.

● Always have an Edit column
○ Sometimes have an Edit column
○ Never have an Edit column

If you selected **Sometimes have an Edit column**, enter the number of rows a table should have to get the **Edit** column.

Tables with at least this many rows have an **Edit** column: [10]

Always have an Edit column

Regardless of the table size, all tables will have an Edit Row column.

Sometimes have an Edit column

Only the tables of the size entered below will have an Edit Row column.

Never have an Edit column

Regardless of the table size, no table will have an Edit Row column.

Tables with at least this many rows have an Edit column

This is an additional setting which only takes effect if you selected **Sometimes have an Edit column** above. Tables with at least the number of rows as you enter in the box will have an **Edit Row** column. Tables with less rows than this are changeable directly.

The standard setting for new 3Com VCX IP Telecommuting Modules is Tables with at least **10** rows have an Edit Row column.

It is not advisable to enter a value higher than 15 here, or the web browser won't be able to satisfactorily manage the tables.

Save

Saves the Table Look configuration to the preliminary configuration. The change takes effect immediately.

Cancel

Reverts to the previous table configuration.

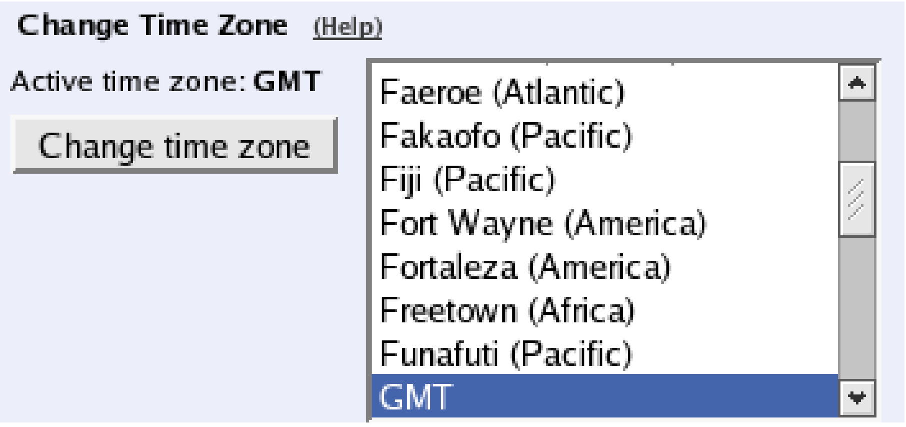
Date and Time

Set the Telecommuting Module clock to ensure that the information in the logs has the right date and time. The date and time are displayed at the bottom of all pages. You can set the date and time manually or let the Telecommuting Module get the correct time from an NTP server.

Note that the Telecommuting Module will use these time settings when deciding whether a time class is active or not. If you change settings, configuration controlled by time classes will be affected.

Change Time Zone

Before you change the time in the Telecommuting Module, check that it uses the correct time zone. A change of time zone only affects the time displayed on the Telecommuting Module web pages; the Telecommuting Module clock is not changed. An effect of a time zone change is that time classes are applied differently, as they are used according to the time shown on the web pages.



Change Time Zone

Active time zone: GMT

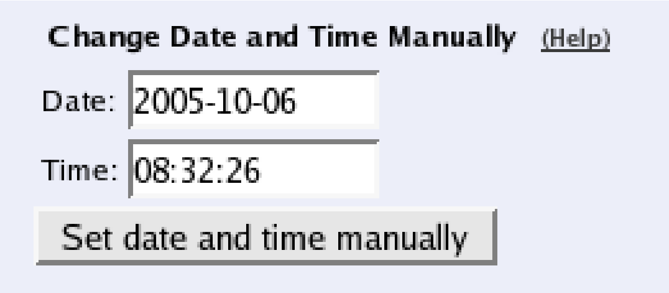
Active time zone shows the current time zone setting. Change time zone by selecting one in the left-hand box and press the **Change time zone** button.

Preferrably, select a city in your country as opposed to selecting a GMT time zone. With the location selection, the Telecommuting Module will also compensate for things like Daylight Saving Time.

Change Date and Time Manually

Here you change the Telecommuting Module clock manually. When you change time here, there will be a time gap in the log files (if you change time forwards) or the same time will be shown twice (if you change time backwards).

N.B. Before you change time here, make sure that the Telecommuting Module uses the correct time zone above.



Change Date and Time Manually

Date: 2005-10-06

Time: 08:32:26

Date

The date is written as four digits for the year, two for the month and two for the day. The punctuation between year, month and day must be dashes (-).

Time

Time is written as two digits for the hour, two digits for the minute and two digits for the second, although seconds can be left out. The punctuation between hours, minutes and seconds must be colon (:) or period (.). A 24-hour clock is used.

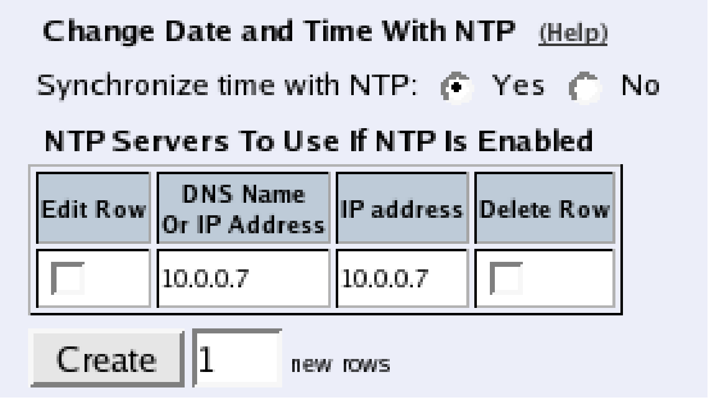
Set date and time manually

Click on **Set date and time manually** to change the clock in the Telecommuting Module to what you entered in the **Date** and **Time** fields.

Change Date and Time With NTP

Instead of setting the time manually, you can let the Telecommuting Module get the correct time from an NTP server. The time for synchronizing will be notably shorter if the Telecommuting Module time is approximately correct when NTP is activated.

N.B. Before you change time here, make sure that the Telecommuting Module uses the correct time zone above.



Change Date and Time With NTP (Help)

Synchronize time with NTP: ● Yes ○ No

NTP Servers To Use If NTP Is Enabled

Edit Row	DNS Name Or IP Address	IP address	Delete Row
□	10.0.0.7	10.0.0.7	□

Synchronize time with NTP

Here, select if NTP synchronizing should be enabled or not.

Enter servers to sync with in the table below.

Dynamic

If an interface will receive its IP address from a DHCP server, the Telecommuting Module can also get information about its NTP server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

NTP Servers To Use If NTP Is Enabled

DNS Name Or IP Address

The name/IP address of the NTP server to which the Telecommuting Module should connect. If a name is entered, you must enter the IP address for a name server on the **Basic Configuration** page.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves all Date and Time configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

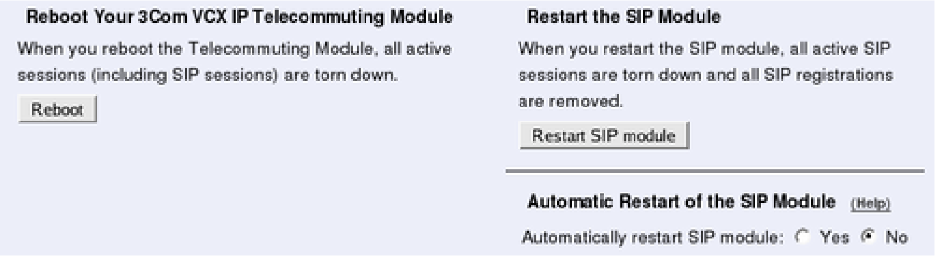
Restart

Here, you can reboot the Telecommuting Module or restart certain modules.

When the Telecommuting Module is rebooted, all active sessions, including SIP sessions (SIP calls, video conferences etc), will be torn down. SIP user registrations are not affected.

When the SIP module is restarted, all active SIP sessions (SIP calls, video conferences etc) will be torn down and all SIP user registrations will be removed.

N.B! The reboot/restart will be instantaneous when the button is pressed.



Reboot Your 3Com VCX IP Telecommuting Module

When you reboot the Telecommuting Module, all active sessions (including SIP sessions) are torn down.

Restart the SIP Module

When you restart the SIP module, all active SIP sessions are torn down and all SIP registrations are removed.

Automatic Restart of the SIP Module

Automatically restart SIP module: ○ Yes ● No

Reboot Your 3Com VCX IP Telecommuting Module

When this button is pressed, the Telecommuting Module will immediately reboot.

All active sessions, including SIP sessions, will be torn down at the reboot.

Restart the SIP Module

When this button is pressed, the SIP module of the Telecommuting Module will restart and all SIP registrations will be removed.

All active SIP sessions will be torn down and all SIP registrations will be removed at the restart.

Automatic Restart of the SIP Module

You can make the Telecommuting Module monitor the SIP module. If the module stops responding, it will be restarted.

This restart will not have the same effect as when you press the **Restart SIP module** button: all active SIP sessions are torn down, but SIP registrations will not be removed. If the module is not restarted, ongoing calls will usually be unharmed, but no new calls can be set up.

For this monitoring to work, the Telecommuting Module must be set up to respond to SIP requests via UDP.

Chapter 8. Network Configuration

Under **Network Configuration**, you configure:

- Network groups which are used for the Telecommuting Module configuration
- The Telecommuting Module's IP addresses on all network interfaces
- Routings for the networks so that computers behind routers can be contacted
- VLAN settings
- PPPoE settings
- The Telecommuting Module network environment (only for the DMZ type)

Networks and Computers

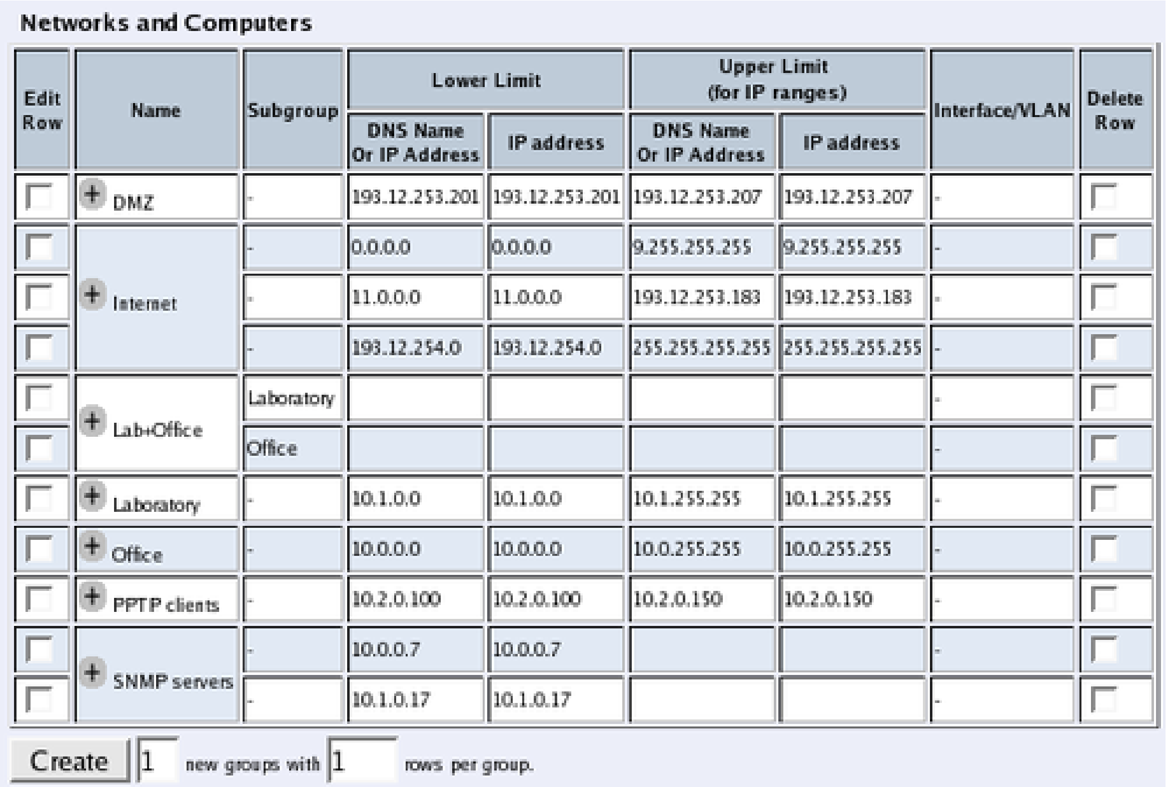
Here, you name groups of computers and networks. Sometimes it can be useful to give a group of computers a network name, such as Administration. If you want to group some computers, this can be done here, even if they do not have consecutive IP addresses. You can also include a subgroup when defining a new network group.

The names are used when you configure **Surroundings**, **Filtering** and **Local Registrar**.

Every group of computers which can reach each other without having to pass through the *firewall* needs a separate network group.

The rows are sorted in alphabetical order, except that all upper case letters are sorted before lower case letters (B comes before a).

When using an already defined group as a subgroup, select the name of the group under **Subgroup**. Set **Interface/VLAN** to '-' and leave the other fields empty.



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name Or IP Address	IP address	DNS Name Or IP Address	IP address		
☐	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	☐
☐	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	☐
☐		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	☐
☐		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	☐
☐	+ Lab+Office	Laboratory					-	☐
☐		Office					-	☐
☐	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	☐
☐	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	☐
☐	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	☐
☐	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	☐
☐		-	10.1.0.17	10.1.0.17			-	☐

Name

Enter a name for the group of computers. You can use this name when you change configuration on the pages mentioned above. A group can consist of several rows of IP addresses or series of IP addresses. By clicking on the plus sign beside the name, you add more rows where you can specify more IP addresses for this group.

Subgroup

An already defined group can be used as a subgroup to new groups. Select the old group here and leave the fields for **DNS name** empty. Select '-' as **Interface**. If you don't want to use a subgroup, select '-' here.

Lower Limit

DNS Name Or IP Address

Enter the DNS name or IP address of the network or computer. For computers in an IP range that you want to give a network name, enter the first IP address in the range. **DNS Name Or IP Address** must not be empty if you are not using a subgroup.

IP address

The IP address of the object you entered in the **DNS Name Or IP Address** field is displayed here. This field is not updated until you click on **Look up all IP addresses again** or make changes in the **DNS Name Or IP Address** field.

Upper Limit

DNS Name Or IP Address

Here, enter the last DNS name/IP address of the network or group. For computers in an IP range that you want to give a network name, enter the last IP address in the seriesrange. The IP address in **Upper Limit** must be at least as high as the one in **Lower Limit**. If this field is left empty, only the IP address in **Lower Limit** is used. If you use a subgroup, leave this field empty.

IP address

The IP address of the object you entered in the **DNS Name Or IP Address** field is displayed here. This field is not updated until you click on **Look up all IP addresses again** or make changes in the **DNS Name Or IP Address** field.

Interface/VLAN

Here, you can select an interface or a VLAN to restrict the IP range.

If '-' is chosen, the group will consist of all IP addresses in the interval between **Lower Limit** and **Upper Limit**, regardless of what interface they are connected to. By selecting an interface or a VLAN, you constrain the group to consist only of the IP addresses in the interval that really are connected to the selected interface/VLAN.

For example, if 10.20.0.0 - 10.20.0.255 are IP addresses behind the interface DMZ-1 and the lower and upper limits are 10.10.10.20 and 255.255.255.255 respectively, choosing DMZ-1 as Interface will cause the group to consist of the IP addresses 10.20.0.0 - 10.20.0.255, being the IP addresses in the interval actually connected to the selected interface.

If you have selected a subgroup, the **Interface/VLAN** should be '-'. If you want to define a network group at the remote side of a VPN connection, the **Interface/VLAN** should be '-'.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new groups and rows you want to add to the table, and then click on **Create**.

Save

Saves the Networks and Computers configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and reset changes in old rows.

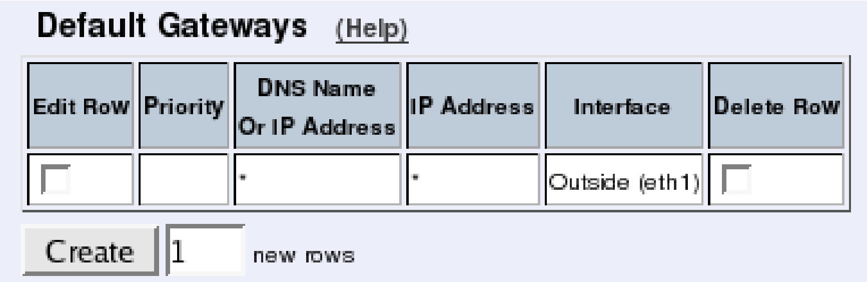
Default Gateway

Main Default Gateways

The **Default gateway** is the IP address of the router that is used to contact the outside world. This IP address is usually the firewall. **Default gateway** must be an IP address from one of the Directly Connected Networks of the Telecommuting Module's interfaces. See appendix D, Definitions of Terms, for further description of routers/gateways.

The Telecommuting Module must have at least one default gateway to work.

You can enter more than one default gateway. The Telecommuting Module will use one of them until it stops responding, and then switch to the next one.



Default Gateways (Help)

Edit Row	Priority	DNS Name Or IP Address	IP Address	Interface	Delete Row
□		*	*	Outside (eth1)	□

Priority

If you entered more than one default gateway, you can assign a priority to each of them. The Telecommuting Module will use the gateway with the highest priority (lowest number) when it works. If it stops working, the Telecommuting Module will switch to the next in priority, while checking the first for availability. When the first gateway works again, the Telecommuting Module will switch back to using that.

Dynamic

If an interface will receive its IP address from a DHCP server, the Telecommuting Module will get its default gateway from the server. In this case, select the corresponding IP address here.

DNS Name Or IP Address

Enter the DNS name or IP address for the default gateway. If an interface will receive its IP address from a DHCP server, the Telecommuting Module will get its default gateway from the server. In this case, leave this field empty.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Interface

Select the interface connected to the Telecommuting Module default gateway.

Delete Row

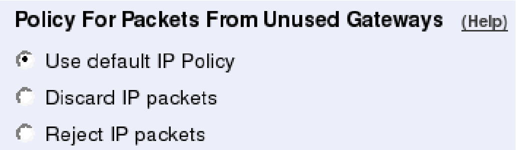
If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Policy For Packets From Unused Gateways

This policy controls how packets from the currently unused gateway(s) should be treated. The packet can be allowed (subject to the rest of the configuration) or discarded.


Policy For Packets From Unused Gateways (Help)

● Use default IP Policy

○ Discard IP packets

○ Reject IP packets

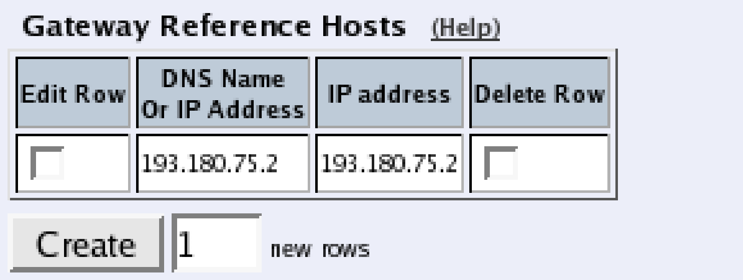
The **Discard IP packets** selection means that the Telecommuting Module ignores the IP packets without replying that the packet did not arrive.

The **Allow IP packets** selection makes the Telecommuting Module use the rest of the configuration to decide if the packet should be allowed.

Gateway Reference Hosts

The gateway reference hosts are used by the Telecommuting Module to check if the gateways are alive. For each reference host, test ping packets are sent, using the different gateways.

Reference hosts are not needed if you have entered a single default gateway.


Gateway Reference Hosts (Help)

Edit Row	DNS Name Or IP Address	IP address	Delete Row
□	193.180.75.2	193.180.75.2	□

DNS Name Or IP Address

Enter the DNS name or IP address for the reference host. The reference host must be located on the other side of the default gateway.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the Default Gateway configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and reset changes in old rows.

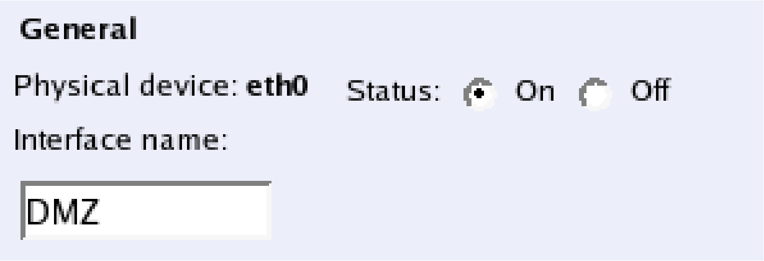
Interface (Network Interface 1 and 2)

There is a page for each network interface (Network Interface 1 and 2) on the Telecommuting Module. Select a page to make configuration for that interface. There is also a page where configuration for all interfaces can be viewed and changed.

Here, you set the interface name, whether the interface is on or off, the IP address, alias, and static routing.

For each interface, go to **Directly Connected Networks** and state the IP address of the Telecommuting Module and the size of the network connected to this interface.

General



General

Physical device: eth0 Status: ● On ○ Off

Interface name:

DMZ

Physical device

Physical device tells the physical device name of the network interface.

Status

Specify if this network interface is **On** or **Off**. If the interface is off, all configuration on this page is ignored, and the Telecommuting Module will behave as if this interface wasn't present.

Interface name

The network **Interface name** is only used internally in the Telecommuting Module, e. g. when configuring **Networks and Computers**.

Obtain IP Address Dynamically

Specify if this network interface should obtain its IP address from a DHCP or PPPoE server instead of an address entered on this page. If **DHCP client ON** is selected, the Telecommuting Module will send out a DHCP request when you apply the configuration and at boot. The request is sent out to the network connected to this interface. If no IP address is obtained, the Telecommuting Module will keep on sending requests until an address lease is received.

The Telecommuting Module will accept an IP address and a netmask via DHCP. It will also accept a default gateway, if you configured for that in the **Main Default Gateways** table on the **Default Gateway** page.

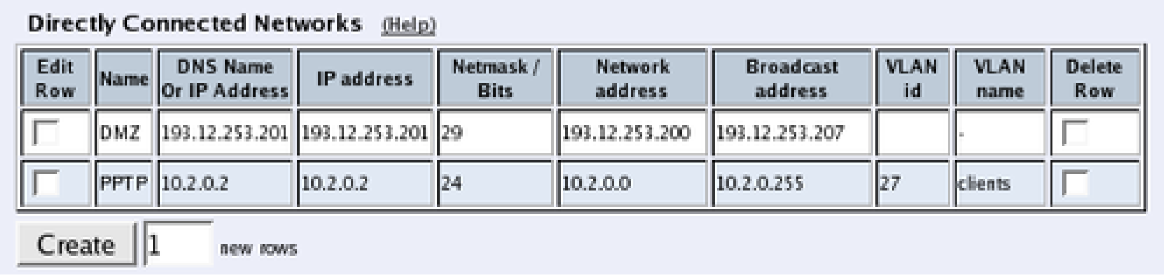
If **PPPoE client ON** is selected, the Telecommuting Module will send out a PPPoE request when you apply the configuration and at boot. To obtain an IP address via PPPoE, you also need to enter configuration on the **PPPoE** page.

More than one interface can obtain its IP address dynamically.

Directly Connected Networks

The Telecommuting Module must have an IP address on every network to which it is directly connected. This applies to all networks on the same physical network to which this interface is connected.

When the DHCP client is on, there must be a directly connected network with "*" as the **DNS name/IP address**, and where the **Netmask/bits** field is left empty. No other directly connected networks are allowed for this interface.



Directly Connected Networks (Help)

Edit Row	Name	DNS Name Or IP Address	IP address	Netmask / Bits	Network address	Broadcast address	VLAN id	VLAN name	Delete Row
□	DMZ	193.12.253.201	193.12.253.201	29	193.12.253.200	193.12.253.207		-	□
□	PPTP	10.2.0.2	10.2.0.2	24	10.2.0.0	10.2.0.255	27	clients	□

Name

A name for this IP address. You can use this name when configuring VPN. This name is only used internally in the Telecommuting Module.

DNS Name Or IP Address

The name/IP address of the Telecommuting Module on this network interface on this directly connected network. If a name is entered, you must enter the IP address for a name server on the **Basic Configuration** page.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Netmask/Bits

Enter the mask of the network where the **DNS Name Or IP Address** applies.

Network address

The IP address of the network where the **DNS Name Or IP Address** applies.

Broadcast address

Shows the broadcast address of the network in the **Network address** field.

VLAN Id

VLANs are used for clustering IP ranges into logical networks. A VLAN id is simply a number, which identifies the VLAN uniquely within your network.

Enter a VLAN id for this network. You don't need to use a named VLAN (defined on the **VLAN** page).

VLAN Name

If you entered the VLAN id of a named VLAN, the name will show here.

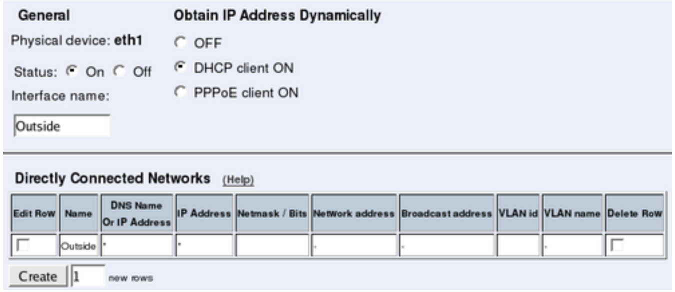
Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

If the interface should obtain its IP address from a DHCP server, the settings should be like in the image below. With a DHCP IP, no aliases can be defined for the interface.



General

Physical device: **eth1**

Status: ● On ○ Off

Interface name: Outside

Obtain IP Address Dynamically

○ OFF

● DHCP client ON

○ PPPoE client ON

Directly Connected Networks (Help)

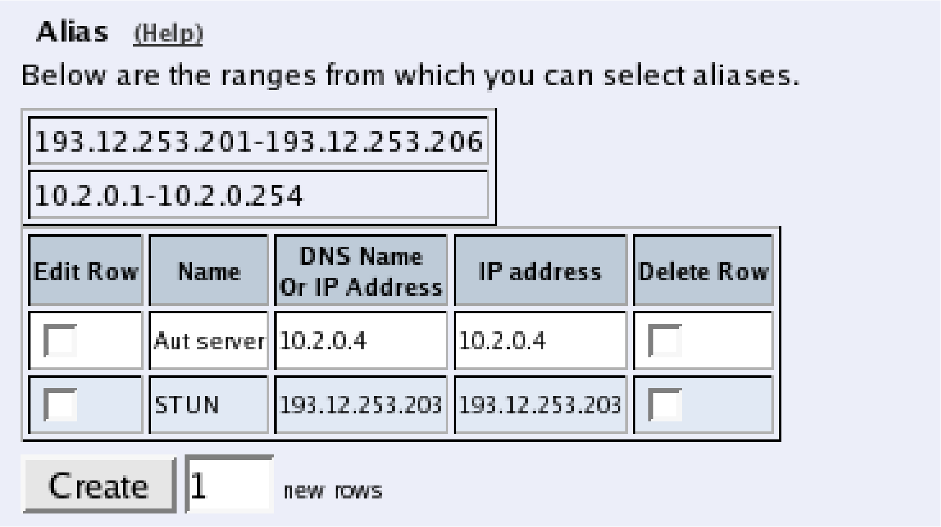
Edit Row	Name	DNS Name Or IP Address	IP Address	Netmask / Bits	Network address	Broadcast address	VLAN id	VLAN name	Delete Row
□	Outside								□

Alias

3Com VCX IP Telecommuting Module can use extra IP addresses, aliases, on its interfaces. All alias IP addresses must belong to one of the **Directly Connected Networks** you have specified.

Aliases are necessary for setting up a STUN server.

If the interface obtains its IP address dynamically, no aliases can be defined.



Alias (Help)

Below are the ranges from which you can select aliases.

193.12.253.201-193.12.253.206
10.2.0.1-10.2.0.254

Edit Row	Name	DNS Name Or IP Address	IP address	Delete Row
□	Aut server	10.2.0.4	10.2.0.4	□
□	STUN	193.12.253.203	193.12.253.203	□

Name

Enter the name of your alias. This name is only used internally in the Telecommuting Module.

DNS Name Or IP Address

Enter the IP address of this alias, or a name in the DNS. If you enter a DNS name instead of an IP address, you must enter the IP address of a DNS server on the **Basic Configuration** page.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

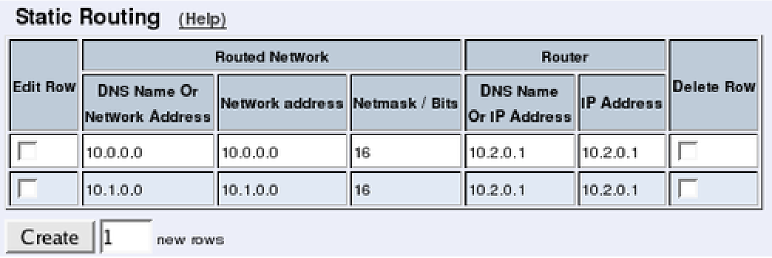
Enter the number of new rows you want to add to the table, and then click on **Create**.

Static Routing

If there is a router between the Telecommuting Module and a computer network which the Telecommuting Module is serving, you must name the router and the network here. The table is sorted by network number and network mask.

The **Default gateway**, configured on the **Default Gateway** page, will automatically be entered in this table on the corresponding interface page, when added to the **Main Default Gateways** table.

If the interface obtains its IP address dynamically, no other static routes can be defined.



Static Routing (Help)

Edit Row	Routed Network			Router		Delete Row
	DNS Name Or Network Address	Network address	Netmask / Bits	DNS Name Or IP Address	IP Address	
□	10.0.0.0	10.0.0.0	16	10.2.0.1	10.2.0.1	□
□	10.1.0.0	10.1.0.0	16	10.2.0.1	10.2.0.1	□

Create 1 new rows

Routed network

Enter the DNS name or IP address of the routed network under **DNS Name Or Network Address**.

The IP address of the routed network is shown under **Network address**.

In the **Netmask/Bits** field, enter the netmask of the network.

Router

The name or IP address of the router that will be used for routing to the network. If there are several routers between the Telecommuting Module and the network, fill in the router *closest to the Telecommuting Module*.

If an interface will receive its IP address from a DHCP server, the Telecommuting Module will get its default gateway from the server. In this case, select the corresponding IP address under **Dynamic**.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves all Interface configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

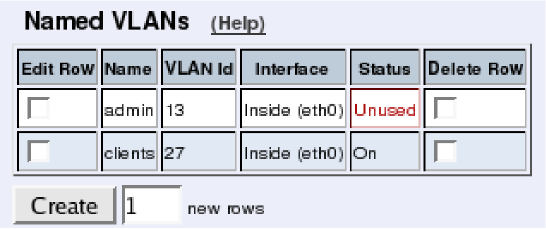
VLAN

VLANs are used for clustering IP ranges into logical networks. A VLAN id is simply a number, which identifies the VLAN uniquely within your network.

Named VLANs

Here, you can list the VLANs you wish to use and give them names, to make administration easier.

Named VLANs can also be selected instead of interfaces on the **Networks and Computers** page.



Named VLANs (Help)

Edit Row	Name	VLAN Id	Interface	Status	Delete Row
□	admin	13	Inside (eth0)	Unused	□
□	clients	27	Inside (eth0)	On	□

Create 1 new rows

Name

The name of this VLAN. The name is only used in the Telecommuting Module web interface to help you keep track of the different VLANs.

VLAN Id

Enter a VLAN id. A VLAN id is just a number. All packets for this VLAN are then marked with this number, enabling all network devices to recognize and route packets for the VLAN.

Interface

Select an interface for this VLAN.

Status

The status for this VLAN. Status can be **On** (the VLAN is used on an active interface), **Off** (the VLAN is used on an inactive interface) and **Unused** (no **Directly Connected Networks** has been selected for this VLAN).

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves all VLAN configuration to the preliminary configuration.

Cancel

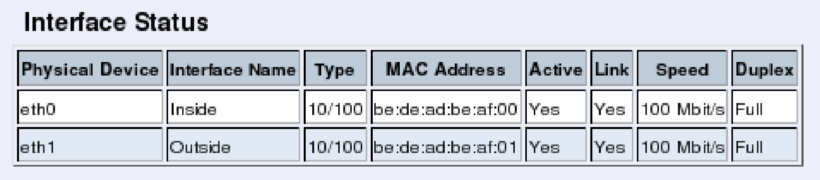
Clears and resets all fields in new rows and resets changes in old rows.

Interface Status

On this page, status about the physical interfaces and links are shown.

Status of dynamic IP addresses is also shown here.

Interface Status



Interface Status

Physical Device	Interface Name	Type	MAC Address	Active	Link	Speed	Duplex
eth0	Inside	10/100	be:de:ad:be:af:00	Yes	Yes	100 Mbit/s	Full
eth1	Outside	10/100	be:de:ad:be:af:01	Yes	Yes	100 Mbit/s	Full

Physical Device

The name of the physical network interface.

Interface Name

The name you gave this interface.

Type

Here the speed options for the interface are shown.

MAC Address

The MAC address of the interface.

Active

Shows if the interface is activated or not.

Link

Here you can see if the interface has physical link to the network.

Speed

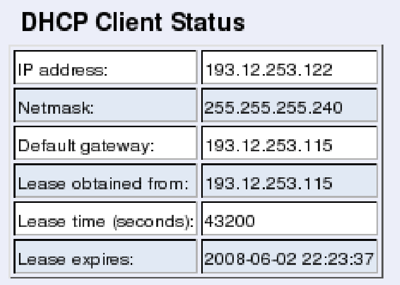
Here you can see the negotiated speed on the interface network.

Duplex

Here you can see the negotiated duplex for the interface.

DHCP Client Status

When an interface is configured to obtain its IP via DHCP, the **DHCP Client Status** section is shown. Here you find information about the DHCP lease.



DHCP Client Status

IP address:	193.12.253.122
Netmask:	255.255.255.240
Default gateway:	193.12.253.115
Lease obtained from:	193.12.253.115
Lease time (seconds):	43200
Lease expires:	2008-06-02 22:23:37

IP address

The IP address obtained via DHCP.

Netmask

The netmask for the network on which the IP address is.

Default gateway

Default gateway for the network on which the IP address is.

Lease obtained from

The DHCP server which served the IP address to the Telecommuting Module.

Lease time

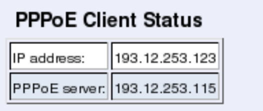
The time interval (in seconds) which the lease can be held.

Lease expires

The time when this lease expires. The Telecommuting Module will renew the lease automatically.

PPPoE Client Status

When an interface is configured to obtain its IP via PPPoE, the **PPPoE Client Status** section is shown. Here you find information about the PPPoE address.



PPPoE Client Status

IP address:	193.12.253.123
PPPoE server:	193.12.253.115

IP address

The IP address of the Telecommuting Module obtained via PPPoE.

PPPoE server

The PPPoE server which leased the IP address.

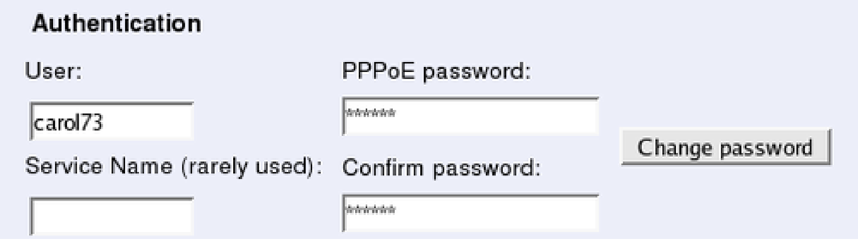
PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a modification of PPP and is used to assign an IP address to a computer as long as it is connected to the PPPoE server. When it disconnects, it instantly loses the IP address.

Many Internet providers use PPPoE instead of DHCP to distribute IP addresses.

Authentication

The Telecommuting Module must be authenticated to get an IP address. Here, you enter authentication information for the Telecommuting Module to use.



User: carol73

Service Name (rarely used):

PPPoE password: ******

Confirm password: ******

User

Enter the user name which the Telecommuting Module should use to identify itself to the PPPoE server.

Service Name

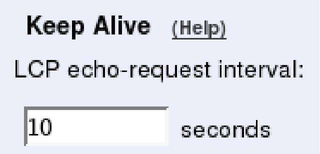
If your PPPoE server supports this, you can ask for a certain service. This parameter is rarely used.

PPPoE password, Confirm password

Enter the password for the user above. You must enter the same password in both fields. Press the **Change password** button to change to the entered password.

Keep Alive

The Telecommuting Module can check the status of the PPPoE connection by sending LCP echo requests to the PPPoE server with regular intervals. If the server does not reply to three consecutive requests, the connection is assumed to be down, and the Telecommuting Module starts a new PPPoE negotiation.



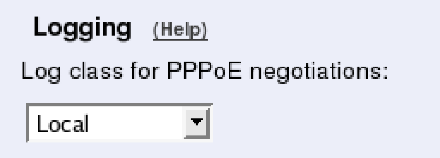
LCP echo-request interval: 10 seconds

LCP echo-request interval

Enter the interval (in seconds) between two requests. Leave the field empty to turn this function off.

Logging

The PPPoE negotiations generate log messages. Here, you can select how to log these messages.



Log class for PPPoE negotiations: Local

Log class for PPPoE negotiations

Select a log class for PPPoE negotiations. Select from the log classes defined on the **Log Classes** page.

Save

Saves all PPPoE configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Surroundings

State the topology around the Telecommuting Module on this page. Which type of topology is needed depends on which Telecommuting Module Type was selected.

Surroundings

Settings in the **Surroundings** table are only required when the Telecommuting Module has been made the **DMZ** (or **LAN**) type.

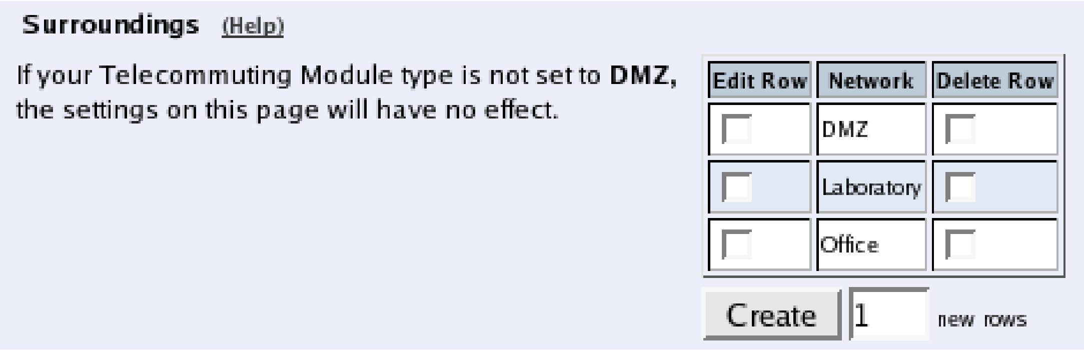
The Telecommuting Module must know what the networks around it looks like. On this page, you list all networks which the Telecommuting Module should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the firewall connected to the Telecommuting Module should be grouped in one network. When you are finished, there should be one line for each of your firewall's network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Surroundings, no ports for RTP sessions will be opened, since the Telecommuting Module assumes that they are both on the same side of the firewall.

For DMZ and LAN SIParators, at least one network should be listed here. If no networks are listed, the Telecommuting Module will not perform NAT for any traffic.



Surroundings (Help)

If your Telecommuting Module type is not set to **DMZ**, the settings on this page will have no effect.

Edit Row	Network	Delete Row
□	DMZ	□
□	Laboratory	□
□	Office	□

Network

Select a network. The alternatives are the networks you defined on the **Networks and Computers** page.

Additional Negotiators

Sometimes you have SIP devices on a different network that needs to negotiate for this network. This happens when there is a SIP server on one network, and SIP-unaware phones on another. In this case, select the phone network under Network, and the SIP server as an Additional Negotiator. Select from the networks defined on the **Networks and Computers** page.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

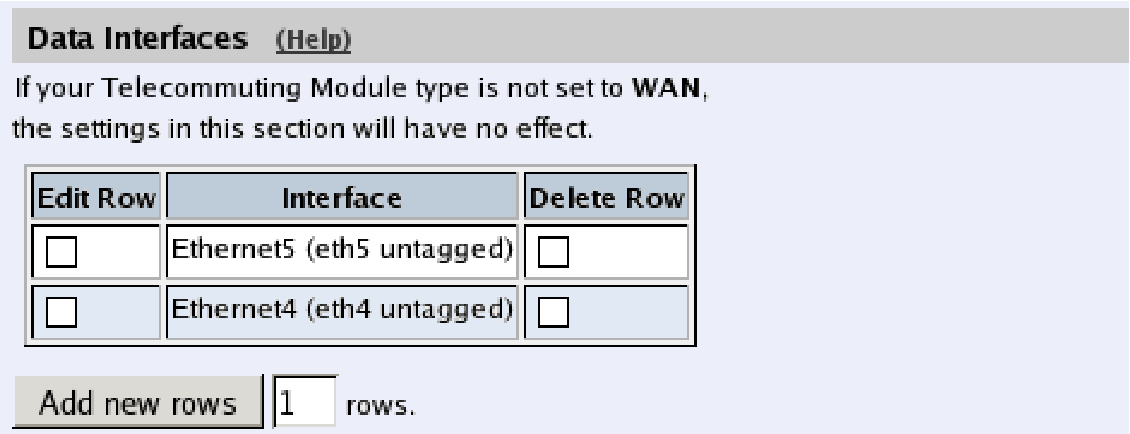
Data Interfaces

Settings in the **Data Interfaces** table are only required when the Telecommuting Module has been made the **WAN** type.

Between the Data Interfaces listed here, the Telecommuting Module will act as a plain router, and only forward traffic, with the exception that QoS will be performed if configured for the traffic in question.

The traffic sent between Data Interfaces will not be logged by the Telecommuting Module.

The Telecommuting Module will only send SIP traffic between the other interfaces.



Data Interfaces (Help)

If your Telecommuting Module type is not set to **WAN**, the settings in this section will have no effect.

Edit Row	Interface	Delete Row
□	Ethernet5 (eth5 untagged)	□
□	Ethernet4 (eth4 untagged)	□

Interface

Select a data interface here.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves all Surroundings configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

Chapter 9. Logging

3Com VCX IP Telecommuting Module can log different types of traffic, attempts to connect and other events. You can select to have the logs stored on the Telecommuting Module's local hard drive, in which case they can be queried. When the Telecommuting Module's hard drive gets full, it removes the oldest data to make space for saving new data.

You can also clear the logs manually by running the installation program (see the chapter titled Basic Administration) and select to **Reset the rest of the configuration** and **3. Revert to the factory configuration**. NB: This will clear the logs, remove all configuration on the Telecommuting Module and then apply the configuration set during the running of the installation program.

For traffic that uses the TCP protocol, only the first packet is logged, the one that initiates the connection. For the UDP and ICMP protocols, all packets are logged. In this section, you specify what you want to log and alarm and study the logs. Logging of events is also configured under **Access Control**.

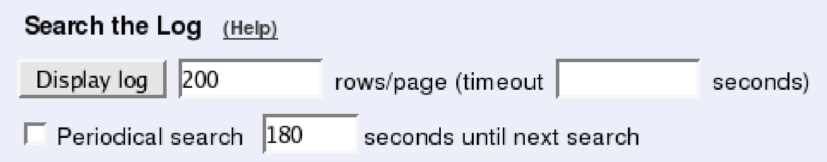
Display Log

On this page, you can view the logs. You select the type of traffic you want to study by selecting which packets should be displayed.

Search the Log

Extracts from the log can be displayed in your web browser for troubleshooting or monitoring.

Below the search form, you can also export log extracts to a file.



Search the Log (Help)

Display log 200 rows/page (timeout seconds)

□ Periodical search 180 seconds until next search

Display log

For screen display, enter the desired number of lines per page and press **Display log**.

If you enter a large number of lines, and there are only a few entries per day of the event you selected, the Telecommuting Module will keep on searching through the entire log. You can limit this by entering a timeout in seconds, after which the Telecommuting Module should stop searching regardless of progress.

Periodical search

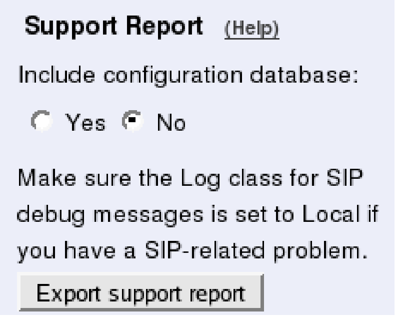
Periodical search will cause new events to appear automatically in the log display. You enter the time interval for updating in the **Seconds until next search** field. This will only affect log display on your screen.

Support Report

When you press Export support report, the Telecommuting Module will create a compressed file with a log for the time period selected, and configuration files. This is the preferred way of sending information to the 3Com support team.

If the time interval entered does not contain any log files, the Telecommuting Module will display an error message. Check that you entered the correct date.

Units without a hard drive (Ingate SIParator 19) rotate out the logs quickly, as there is a very limited space to keep them. This could be a reason for the Support Report not containing any logs. In this case, make the test again and download the Support Report directly after that.



Support Report (Help)

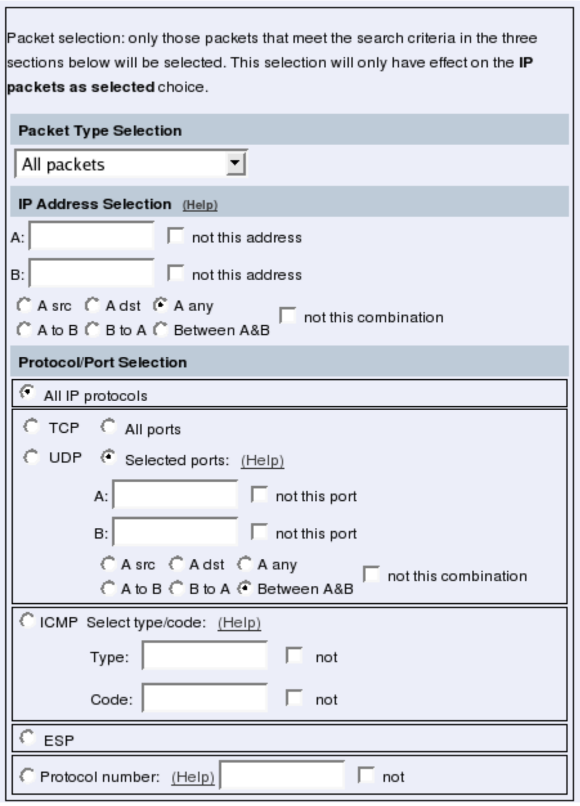
Include configuration database:

○ Yes ● No

Make sure the Log class for SIP debug messages is set to Local if you have a SIP-related problem.

Packet Selection

You can select packets by IP addresses, IP protocols and whether they were allowed to pass the Telecommuting Module or not. Only packets matching all three criteria are shown.



Packet selection: only those packets that meet the search criteria in the three sections below will be selected. This selection will only have effect on the **IP packets as selected** choice.

Packet Type Selection

All packets

IP Address Selection (Help)

A: □ not this address

B: □ not this address

○ A src ○ A dst ● A any ○ A to B ○ B to A ○ Between A&B □ not this combination

Protocol/Port Selection

● All IP protocols

○ TCP ○ All ports

○ UDP ● Selected ports: (Help)

A: □ not this port

B: □ not this port

○ A src ○ A dst ○ A any ○ A to B ○ B to A ● Between A&B □ not this combination

○ ICMP Select type/code: (Help)

Type: □ not

Code: □ not

○ ESP

○ Protocol number: (Help) □ not

Packet Type Selection

You can limit the selection to only allowed packets or rejected/discarded packets, or a subset of these. For example, you can select allowed, un-NAT:ed packets only.

IP Address Selection

You can limit the selection by specifying certain IP addresses.

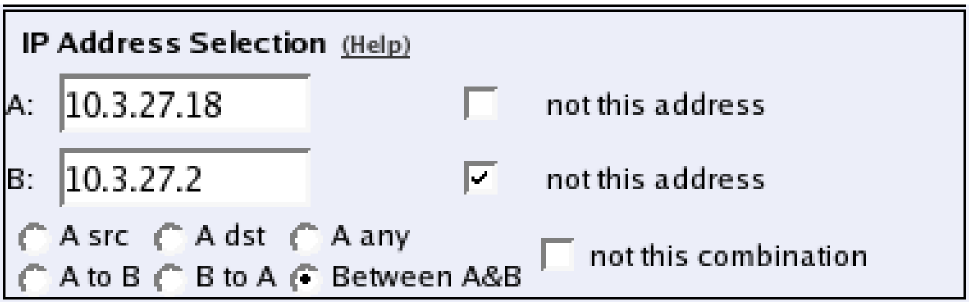
In these fields, enter a single IP address (e. g., 10.3.27.3), a range of IP addresses (e. g., 10.3.27.1-10.3.28.254), an IP address followed by a netmask (e. g.,10.3.27.0/24), a combination of these, or nothing at all. If a field is empty, all IP addresses are selected.

If you want to study all traffic except the one to or from a specific computer or group of computers, enter the IP address(es) here and mark the "not this address" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the IP address in field A matches. Field B is ignored.
A dst	Packets to the IP address in field A matches. Field B is ignored.
A any	Packets to or from the IP address in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to study all packets to or from 10.3.27.18, except those to the file server 10.3.27.2, you should fill in the form like this:



IP Address Selection (Help)

A: 10.3.27.18 □ not this address

B: 10.3.27.2 ☑ not this address

○ A src ○ A dst ○ A any

○ A to B ○ B to A ● Between A&B □ not this combination

Protocol/Port Selection

You can limit the selection by specifying certain protocols.

All IP protocols

No restriction regarding protocols.

TCP/UDP

When selecting TCP or UDP, you can choose all packets or packets to certain ports only.

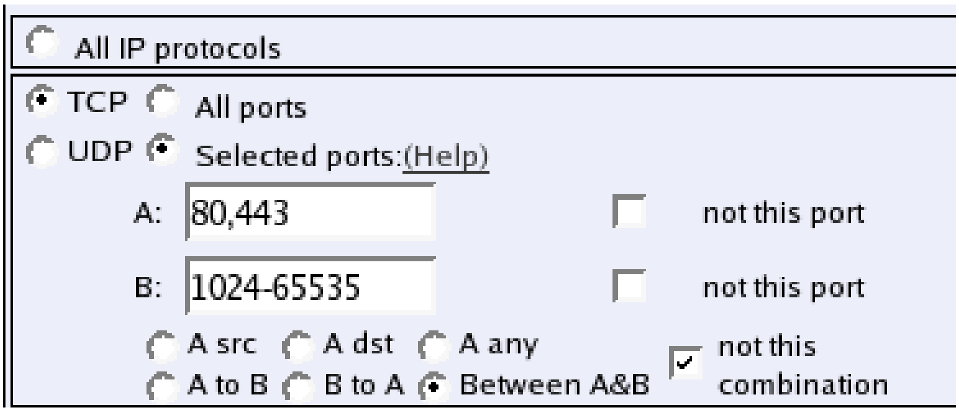
In these fields, you can enter a single port number (32), a range of port numbers (1-1023), a list of port numbers and ranges separated by commas (53, 1024-65535) or nothing at all. If the field is empty, any port will match. See appendix G, Lists of ports, ICMP and protocols, for more information on port numbers.

If you want to study all traffic except the one to or from a specific port or group of ports, enter the port number(s) here and mark the "not this port" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the port number in field A matches. Field B is ignored.
A dst	Packets to the port number in field A matches. Field B is ignored.
A any	Packets to or from the port number in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to search for all packets to a web server, but not packets on the "normal" client and server ports in your environment, fill in the form like this:



○ All IP protocols

● TCP ○ All ports

○ UDP ● Selected ports:(Help)

A: 80,443 □ not this port

B: 1024-65535 □ not this port

○ A src ○ A dst ○ A any ☑ not this combination

○ A to B ○ B to A ● Between A&B

ICMP

ICMP packets contain a type field and a code field. When searching for ICMP packets, you can select all packets or only those matching certain criteria.

In the type and code fields, you can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e. g., 5, 10-20) or nothing at all. If the field is empty, any type or code will match. See appendix G, Lists of ports, ICMP and protocols, for more information on ICMP types and codes.

If you want to study all traffic except the one of a certain type/code, enter the type/code number(s) here and mark the "not" box.

ESP

ESP is an authentication/encryption protocol. Select this if you want to search for encrypted packets.

Note that you must have selected a log class which saves to local file, for encrypted packets, to be able to display them here.

Protocol number

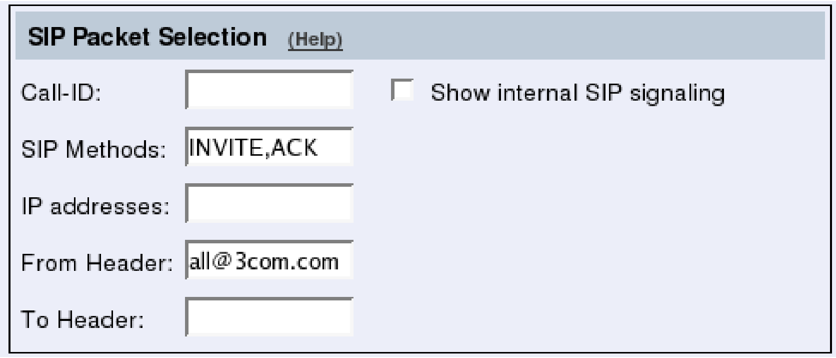
Here, you enter the number(s) of the protocols you want to search for. You can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e. g., 5, 10-20) or nothing at all. If the field is empty, any protocol will match. See appendix C, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols, for more information on protocol numbers.

If you want to study all traffic except the one over a certain protocol or protocols, enter the protocol number(s) here and mark the "not" box.

SIP Packet Selection

In this section, you can filter out certain SIP messages based on Call-ID, SIP method, sending or receiving IP address and the content of the To and From headers.

This selection will only have effect on the SIP choices **SIP signaling** and **SIP packets** under Show This.



SIP Packet Selection (Help)

Call-ID: ☐ Show internal SIP signaling

SIP Methods: INVITE,ACK

IP addresses:

From Header: all@3com.com

To Header:

Call-ID

Enter the Call-ID for the event you want to examine. Matching is done only on entire Call-IDs (no substrings).

SIP Methods

Enter the SIP methods that should be displayed, separated by commas. If you enter INVITE, REGISTER, the log will show all INVITE and REGISTER requests, and all responses for these requests. Note that if you want to see ACKs for a call, you have to enter that method as well as INVITE to see the entire call setup.

IP addresses

Enter one or more IP addresses for which you want to see SIP traffic. For the IP addresses entered, all SIP signaling received from and sent to the addresses will be shown.

From Header

Enter one or more URIs that appear in the From headers for the event you want to examine. The From headers typically contain usernames and domains, like *george@ingate.com*.

To Header

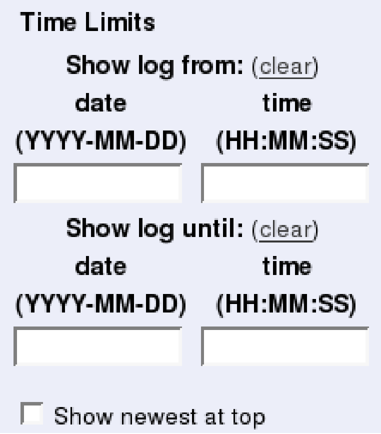
Enter one or more URIs that appear in the To headers for the event you want to examine. The To headers typically contain usernames and domains, like *george@ingate.com*.

Show internal SIP signaling

The Telecommuting Module often loops SIP messages to itself when processing and routing SIP signaling. Normally, the looped messages are not shown, but when this checkbox is checked, the log will display all steps in the message processing.

Time Limits

On the right-hand side of the boxes, select time interval and order for the log display.



Time Limits

Show log from: (clear)

date	time
(YYYY-MM-DD)	(HH:MM:SS)

Show log until: (clear)

date	time
(YYYY-MM-DD)	(HH:MM:SS)

□ Show newest at top

Show log from

You can limit the selection by a time interval.

The date is written as a year with two or four digits, month (01-12) and day (01-31). The optional punctuation between year, month and day must be dash (-). Time is written as two digits for the hour, two digits for the minute and possibly two digits for the second, although the seconds can be left out. The optional punctuation between hours, minutes and seconds must be colon (:) or period (.).

You can enter a date, a time or both to set a start time for the log display. If you leave the date field blank and enter a time in the corresponding time field, today’s date is used. If you leave the time field blank and enter a date in the date field, the time is set to 00:00:00. If both fields are left blank, all events back to the log start will be displayed.

Show log until

You can enter a date, a time or both to set an end time for the log display. If you leave the date field blank and enter a time in the corresponding time field, today’s date is used. If you leave the time field blank and enter a date in the date field, the time is set to 23:59:59. If both fields are left blank, all events until the latest log event will be displayed.

Show newest at top

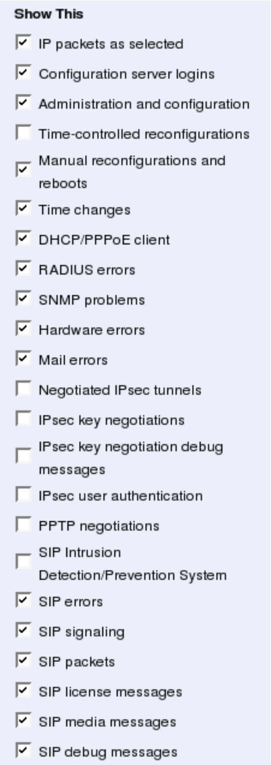
Choosing Show newest at top will display the log in reverse order, i. e., the latest log event will be displayed first.

Periodical search

Periodical search will cause new events to appear automatically in the log display. You enter the time interval for updating in the **Seconds until next search** field. This will only affect log display on your screen.

Show This

You can select the events you want to search for. NB: You must select **IP packets as selected** to get a log display of the packets selected in the boxes.

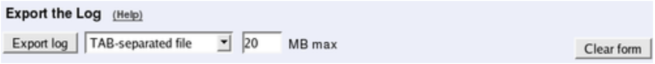


Show This

☑ IP packets as selected
☑ Configuration server logins
☑ Administration and configuration
□ Time-controlled reconfigurations
☑ Manual reconfigurations and reboots
☑ Time changes
☑ DHCP/PPPoE client
☑ RADIUS errors
☑ SNMP problems
☑ Hardware errors
☑ Mail errors
□ Negotiated IPsec tunnels
□ IPsec key negotiations
□ IPsec key negotiation debug messages
□ IPsec user authentication
□ PPTP negotiations
□ SIP Intrusion Detection/Prevention System
☑ SIP errors
☑ SIP signaling
☑ SIP packets
☑ SIP license messages
☑ SIP media messages
☑ SIP debug messages

Export the Log

Extracts from the log can be exported to a text file for processing in external tools.



Export the Log (Help)

Export log | TAB-separated file | 20 MB max | Clear form

You can also save the log to a file. Enter the maximum size of the log file. If you must have the latest log events, select **Show newest at top**.

You can choose between different file formats; TAB-separated file, comma-separated file and WELF (WebTrends Enhanced Log Format). These are text formats, which means that you can import the files in a text editor for analysis. TAB- and comma-separated files contain all information from the log file. WELF is an open standard used by several log analyzer tools. However, all WELF compatible syslog messages will not be exported.

WELF uses the Telecommuting Module name you enter on the **Basic Configuration** page. Some WELF applications have licenses restricted to a certain number of Telecommuting Modules. This can cause trouble if you change the name of your Telecommuting Module.

If you export a log to WELF with **Show newest at top** selected, this may become troublesome when using some WELF applications, which cannot handle events in reverse order.

Press **Export log** and enter the file name and path to export to file.

Clear form

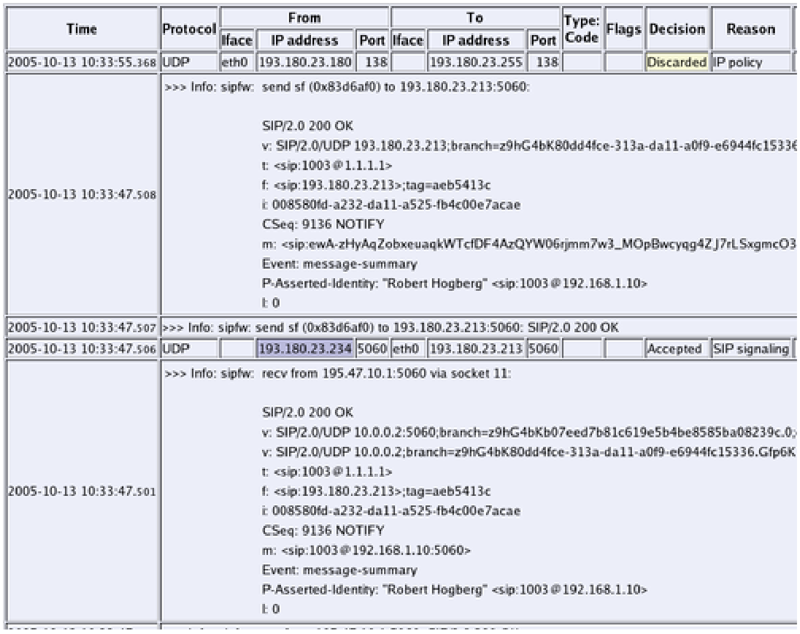
Resets the form.

The log

The log shows every packet and event on a separate row.

The rows displaying IP packets show the date and time, type of protocol, from interface, computer and port, to interface, computer and port, ICMP type for ICMP traffic, flags, whether the packet was accepted, rejected or discarded, and the reason for this. For TCP traffic, and for UDP traffic which is session managed, only the connection packet is displayed. SIP media streams are not logged.

The Telecommuting Module's own IP address is displayed in the log with a purple background color. Rejected and discarded packets are displayed with a yellowish background.



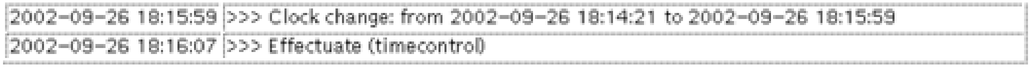
```
Time                     Protocol  From                          To                            Type: Flags Decision  Reason
                                   Iface IP address      Port    Iface IP address      Port    Code
2005-10-13 10:33:55.368  UDP       eth0  193.180.23.180  138           193.180.23.255  138                 Discarded IP policy
2005-10-13 10:33:47.508  >>> Info: sipfw:  send sf (0x83d6af0) to 193.180.23.213:5060:

                                   SIP/2.0 200 OK
                                   v: SIP/2.0/UDP 193.180.23.213;branch=z9hG4bK80dd4fce-313a-da11-a0f9-e6944fc15336
                                   t: <sip:1003@1.1.1.1>
                                   f: <sip:193.180.23.213>;tag=aeb5413c
                                   i: 008580fd-a232-da11-a525-fb4c00e7acae
                                   CSeq: 9136 NOTIFY
                                   m: <sip:ewA-zHyAqZobxeuaqkWTcfDF4AzQYW06rjmm7w3_MOpBwcyqg4ZJ7rLSxgmcO3
                                   Event: message-summary
                                   P-Asserted-Identity: "Robert Hogberg" <sip:1003@192.168.1.10>
                                   l: 0
2005-10-13 10:33:47.507  >>> Info: sipfw: send sf (0x83d6af0) to 193.180.23.213:5060: SIP/2.0 200 OK
2005-10-13 10:33:47.506  UDP             193.180.23.234  5060    eth0  193.180.23.213  5060                Accepted  SIP signaling
2005-10-13 10:33:47.501  >>> Info: sipfw:  recv from 195.47.10.1:5060 via socket 11:

                                   SIP/2.0 200 OK
                                   v: SIP/2.0/UDP 10.0.0.2:5060;branch=z9hG4bKb07eed7b81c619e5b4be8585ba08239c.0;
                                   v: SIP/2.0/UDP 10.0.0.2;branch=z9hG4bK80dd4fce-313a-da11-a0f9-e6944fc15336.Gfp6K
                                   t: <sip:1003@1.1.1.1>
                                   f: <sip:193.180.23.213>;tag=aeb5413c
                                   i: 008580fd-a232-da11-a525-fb4c00e7acae
                                   CSeq: 9136 NOTIFY
                                   m: <sip:1003@192.168.1.10:5060>
                                   Event: message-summary
                                   P-Asserted-Identity: "Robert Hogberg" <sip:1003@192.168.1.10>
                                   l: 0
```

The following flags are used:

S	SYN	Request for connection
A	ACK	Response to a previous packet
U	URG	Contains out-of-band data
P	PUSH	Packets that must be delivered quickly
F	FIN	Disconnect request
R	RST	Reset - response to incorrect packet

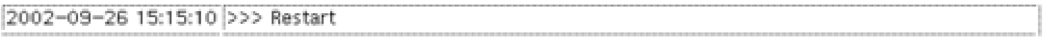
For more information on flags, see RFC 793.

When the clock is reset, the log shows this on a separate line like this:



```
2002-09-26 18:15:59 >>> Clock change: from 2002-09-26 18:14:21 to 2002-09-26 18:15:59
2002-09-26 18:16:07 >>> Effectuate (timecontrol)
```

If the Telecommuting Module is restarted, the log shows this on a line like this:



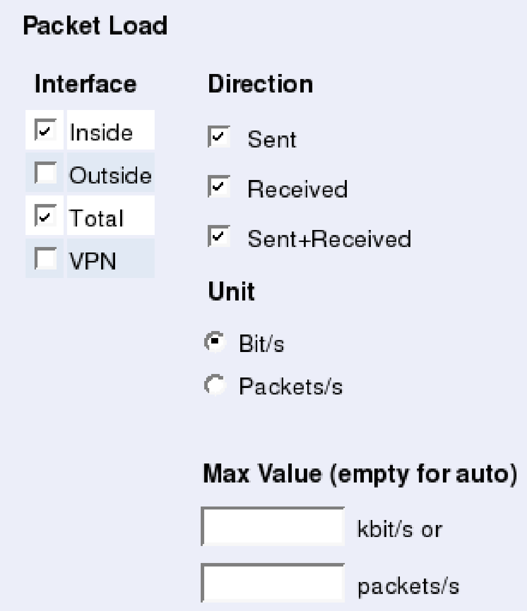
```
2002-09-26 15:15:10 >>> Restart
```

Display Load

On this page, you can see statistics on the traffic load to and from the Telecommuting Module's interfaces and the memory and CPU load.

Once every 10 seconds, the load on all interfaces is scanned and saved to a local file. Every file contains 240 samples and a file generation consists of 42 files and has a size of approximately 20 MB. The first generation of files contains samples for the last week (approximately). Every new file generation is created by merging two consecutive samples, enabling the storing of samples for the double time period in the same disk space. Merging the samples include calculation of the minimum, average and maximum values for the time interval covered by the samples. After ten generations (about 3 years) the samples are deleted.

Packet Load



Packet Load

Interface

☑ Inside
□ Outside
☑ Total
□ VPN

Direction

☑ Sent
☑ Received
☑ Sent+Received

Unit

● Bit/s
○ Packets/s

Max Value (empty for auto)

______ kbit/s or
______ packets/s

Interface

You can select one or more of the Telecommuting Module's interfaces or the total traffic. Selecting more than one interface will generate one graph per interface. You can also select to view only VPN traffic.

Direction

Select one or more of **Sent**, **Received** and **Sent+Received**. Each selection generates a separate graph in the diagram.

Unit

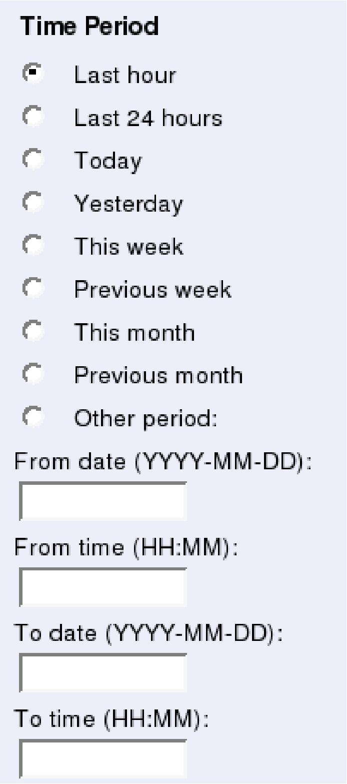
Select between displaying packets/second or bits/second. The graphs may look different, because all packets aren't the same size.

Max Value

Enter the maximum value to show in the diagram. If no value is entered, the diagram automatically scales to a suitable value.

Time Period

Select a time period or enter a period of your own choice in the bottom fields. The date is written as a year with two or four digits, month (01-12) and day (01-31). The optional punctuation between year, month and day must be dash (-). Time is written as two digits for the hour, two digits for the minute and possibly two digits for the second, although the seconds can be left out. The optional punctuation between hours, minutes and seconds must be colon (:) or period (.).



Time Period

● Last hour

○ Last 24 hours

○ Today

○ Yesterday

○ This week

○ Previous week

○ This month

○ Previous month

○ Other period:

From date (YYYY-MM-DD):

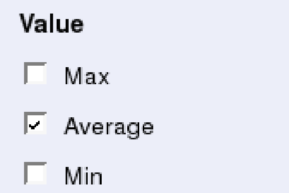
From time (HH:MM):

To date (YYYY-MM-DD):

To time (HH:MM):

Value

Select maximum, average or minimum value of each sample period. If viewing load for time periods within the last week, all three selections will result in the same graph.



Value

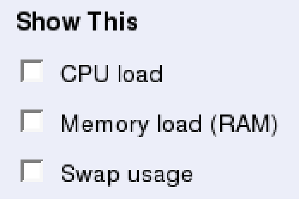
☐ Max

☑ Average

☐ Min

Show This

The Telecommuting Module also stores load values for CPU, memory and swap usage. These values can also be shown in the diagram. Check the boxes for the values to be shown. Each selection generates a separate graph in the diagram.



Show This

☐ CPU load

☐ Memory load (RAM)

☐ Swap usage

The Diagram

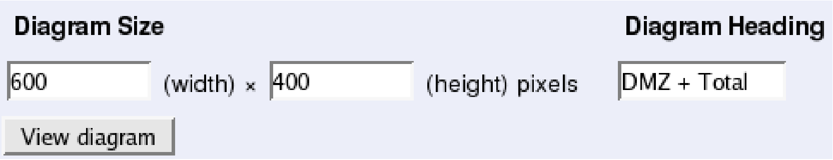


Diagram Size

600 (width) × 400 (height) pixels

Diagram Heading

DMZ + Total

Diagram Size

Enter the desired width and height of the resulting load diagram.

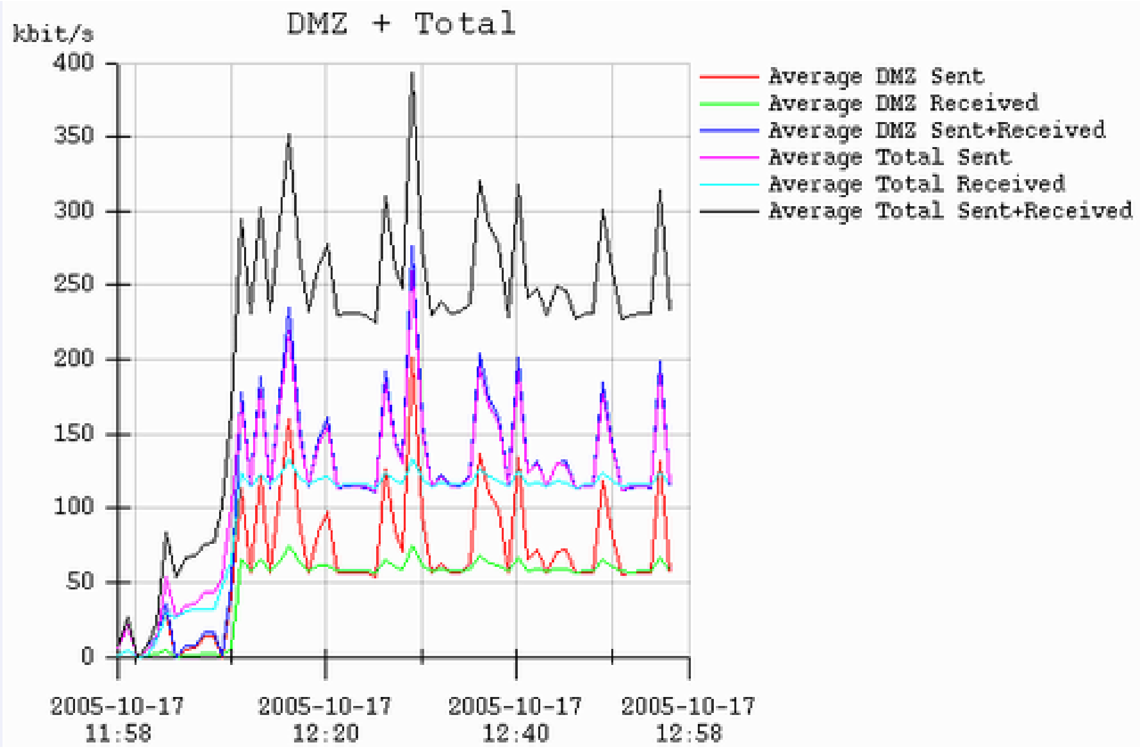
Diagram Heading

You can enter a heading for the load diagram. This is useful if you view several diagrams and save them.

View diagram

Creates a diagram at the top of the page.

For each combination of selections, a graph will be generated. Example: You selected **eth0** and **Total** as interfaces, and **Sent**, **Received** and **Sent+Received** as directions. This will generate a total of six graphs of different colours in the diagram.



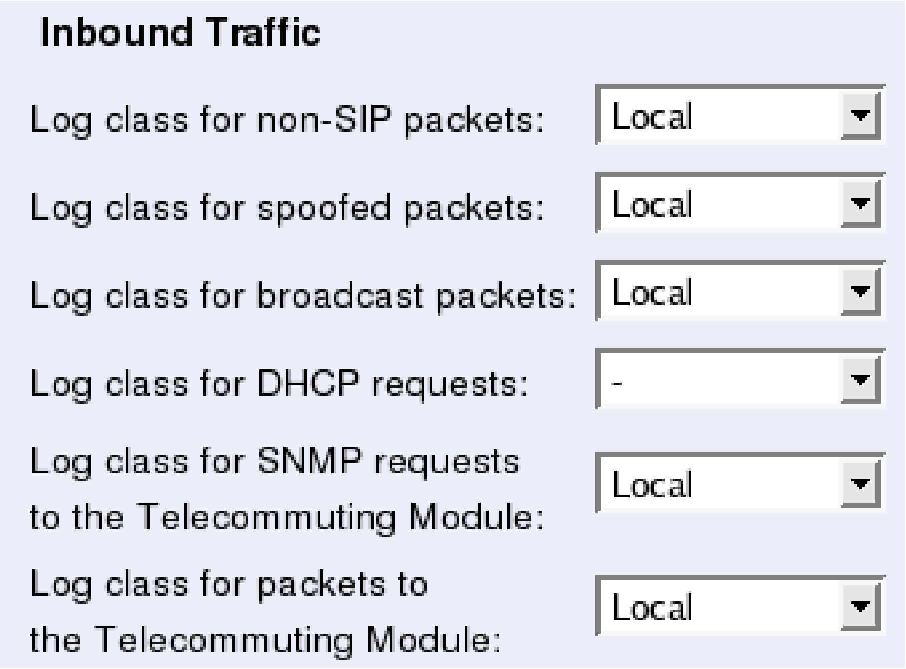
Logging Configuration

Your 3Com VCX IP Telecommuting Module generates log messages for various events and for the traffic to and through the Telecommuting Module. Here, you select log classes to state what to do with the log messages.

When an IP packet is received by the Telecommuting Module, a log message is generated, containing sender and receiver IP addresses and other information such as the protocol used and if the packet was allowed, rejected or discarded. The Telecommuting Module then uses the log settings for Configuration Transport and Log class for non-SIP packets to know how to process the log message.

The Telecommuting Module also produces log messages for SIP-related and VPN-related events as well as administrator events (when the administrator logs on or when a setting is changed). Here, you configure what will happen to these log messages.

Inbound Traffic



Inbound Traffic

Log class for non-SIP packets: Local

Log class for spoofed packets: Local

Log class for broadcast packets: Local

Log class for DHCP requests: -

Log class for SNMP requests to the Telecommuting Module: Local

Log class for packets to the Telecommuting Module: Local

Log class for non-SIP packets

Here, you select a log class for packets which are neither SIP packets, SIP session media streams, or Telecommuting Module administration traffic and are therefore processed by the **IP policy** (discard or reject) that you selected on the **Basic Configuration** page.

Log class for spoofed packets

Here, you select a log class for packets with obviously spoofed addresses. A spoofed IP address can be a non-existing IP address on a network connection or packets where the sender or receiver address is an IP address in the range 127.0.0.0 - 127.255.255.255.

Log class for broadcast packets

Here, you select a log class for broadcast packets. Broadcast is a method of sending packets when you don’t know the actual recipient. The packets are sent to all computers on the network. See appendix D, Definitions of Terms for more information about broadcast.

Log class for DHCP requests

Here, you select a log class for DHCP requests. DHCP is a protocol used for dynamic allocation of IP addresses. Requests are sent by broadcast from computers wanting an IP address to a DHCP server. The Telecommuting Module logs all DHCP related packets using the log class you select here. There are usually a lot of these packets, so we recommend using the log class "None", meaning that no packets are logged at all.

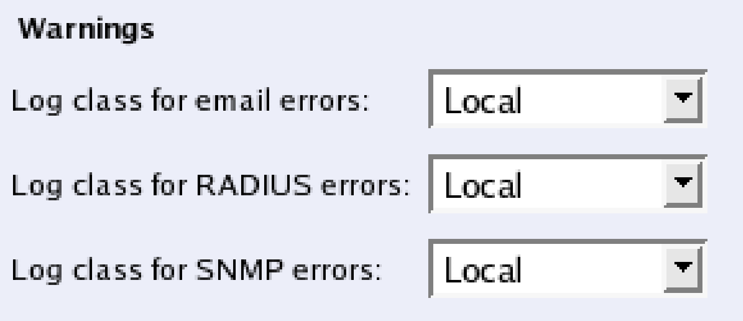
Log class for SNMP requests to the Telecommuting Module

Here, you select a log class for SNMP requests to the Telecommuting Module. *SNMP* is a protocol for monitoring network equipment such as firewalls and routers.

Log class for packets to the Telecommuting Module

Here, you select a log class for traffic addressed to the Telecommuting Module itself. Even if you select not to log this traffic, the configuration traffic to the Telecommuting Module will be logged according to the log class set on the **Access Control** page.

Warnings



Warnings

Log class for email errors: Local

Log class for RADIUS errors: Local

Log class for SNMP errors: Local

Log class for email errors

If the Telecommuting Module is unable to send email messages, for example, if the mail server won't reply, the Telecommuting Module generates a log message. Here, you select a log class for these messages.

Log class for RADIUS errors

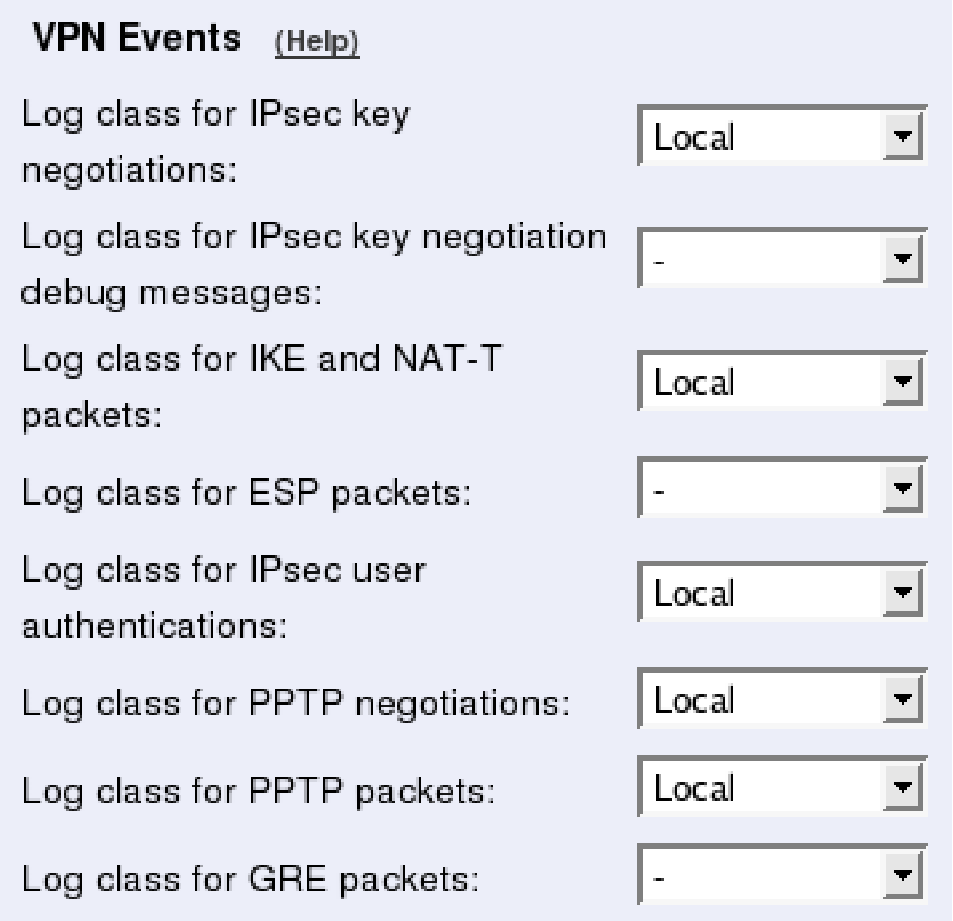
Radiusmux (see the RADIUS section in the chapter titled Basic Configuration) generates messages for incomprehensible RADIUS server responses and for denying logins on account of permissions (a user defined for road warriors is not automatically allowed to log onto the configuration server). Here, you select a log class for these messages.

Log class for SNMP errors

The Telecommuting Module generates messages about SNMP errors. Here, you select a log class for these messages.

VPN Events

The same settings can also be found on the **IPsec Settings** and **PPTP** pages under **Virtual Private Networks**.



VPN Events (Help)

Log class for IPsec key negotiations:	Local
Log class for IPsec key negotiation debug messages:	-
Log class for IKE and NAT-T packets:	Local
Log class for ESP packets:	-
Log class for IPsec user authentications:	Local
Log class for PPTP negotiations:	Local
Log class for PPTP packets:	Local
Log class for GRE packets:	-

Log class for IPsec key negotiations

Here, you set the log class for new negotiations of IPsec connection keys.

Log class for IPsec key negotiation debug messages

Here, you set the log class for debug information about negotiations of IPsec connection keys.

Log class for ESP packets

Specify what log class the Telecommuting Module should use for encrypted packets (ESP packets to the Telecommuting Module). Logging of encrypted packets will generate a lot of log events.

Log class for IKE and NAT-T packets

Here, you set the log class for the packets used for IKE key negotiations and for NAT-T packets. As they both use the same port on the Telecommuting Module, it will log both using the same log class.

Log class for IPsec user authentications

Here, you set the log class for Telecommuting Module messages about road warrior authentications via RADIUS and their disconnections.

Log class for PPTP negotiations

The Telecommuting Module generates log messages about the progress of the PPTP negotiations. Here, you select a log class for these messages.

Log class for PPTP packets

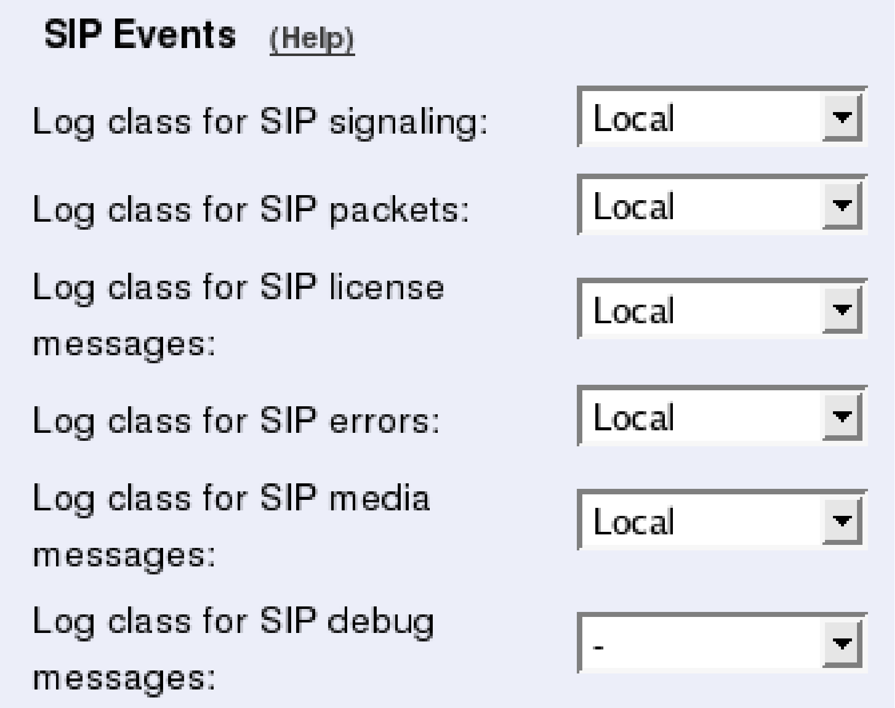
PPTP clients wanting to establish a VPN tunnel connects to the Telecommuting Module on port 1723. Here, you select a log class for these packets.

Log class for GRE packets

The encrypted traffic through the VPN tunnel is sent as GRE packets. Here, you select a log class for these packets.

SIP Events

The same settings can also be found on the **Basic Settings** page under **SIP Services**.



SIP Events (Help)

Log class for SIP signaling:	Local
Log class for SIP packets:	Local
Log class for SIP license messages:	Local
Log class for SIP errors:	Local
Log class for SIP media messages:	Local
Log class for SIP debug messages:	-

Log class for SIP signaling

For each SIP packet, the Telecommuting Module generates a message, containing the sender and receiver of the packet and what type of packet it is. Select a log class for these log messages.

Log class for SIP packets

The Telecommuting Module logs all SIP packets (one SIP packet is many lines). Select a log class for the SIP packets.

Log class for SIP license messages

The Telecommuting Module logs license messages. Select a log class for these messages.

Log class for SIP errors

The Telecommuting Module sends a message if there are any SIP errors. Select a log class for these log messages.

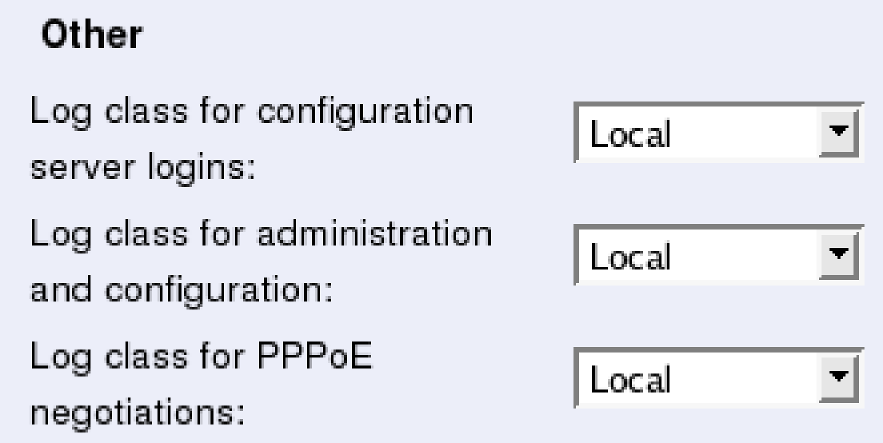
Log class for SIP media messages

The Telecommuting Module creates log messages about when media streams are set up and torn down. Select a log class for these messages.

Log class for SIP debug messages

The Telecommuting Module logs a lot of status messages, for example the SIP initiation phase of a reboot. Select a log class for these messages.

Other



Other

Log class for configuration server logins: Local

Log class for administration and configuration: Local

Log class for PPPoE negotiations: Local

Log class for configuration server logins

Each time a user logs onto the Telecommuting Module configuration server, a message is generated, containing information about the type of login and more. Here, you select a log class for these messages.

Log class for administration and configuration

Each time a user logs onto the Telecommuting Module configuration server, a message is generated, containing information about the type of login and more. Here, you select a log class for these messages.

Log class for PPPoE negotiations

The Telecommuting Module generates log messages for its own PPPoE negotiations. Here, you select a log class for these messages.

Save

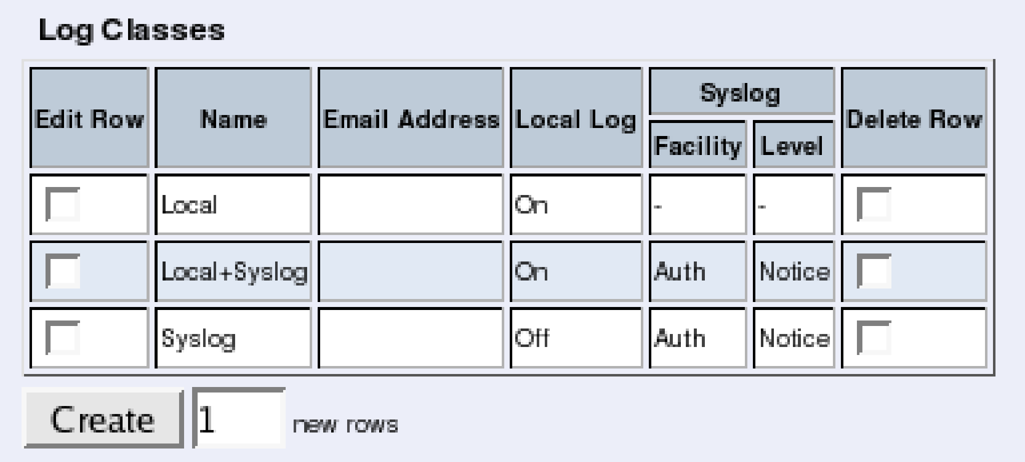
Saves the Logging Configuration configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Log Classes

Log classes determine the handling of traffic logs, other event logs and alarms. You can select no logging, log to a local file (on the Telecommuting Module), send the log messages via syslog to a syslog server and send the log messages as emails. When configuring logging on all other pages, you select between the different log classes defined here.



Log Classes

Edit Row	Name	Email Address	Local Log	Syslog		Delete Row
				Facility	Level	
□	Local		On	-	-	□
□	Local+Syslog		On	Auth	Notice	□
□	Syslog		Off	Auth	Notice	□

Name

Here, you give the log class a **Name**.

Email Address

The Telecommuting Module may also send the log messages by email to one or more email addresses. Enter the addresses here (separated by comma). You must specify a mail server on the **Log Sending** page for the Telecommuting Module to send the emails properly.

Local Log

Select to save log messages to a local file on the Telecommuting Module. Locally saved logs can be searched on the **Display Log** page. **On** will cause the log messages using this log class to be saved to file. **Off** will cause the log messages not to be saved on the Telecommuting Module and thus also not possible to search under **Display Log**.

Syslog

Syslog sends log messages to a syslog server. You enter the IP address of the syslog server on the **Log Sending** page. Select **Facility** and **Level** for the syslog message. See your syslog server manual for more information on facility and level. Selecting **None** for both **Facility** and **Level** turns the syslog alternative off. **None** must be selected for both or none of **Facility** and **Level**. The Telecommuting Module will display a red warning text until both or none of them are **None**.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

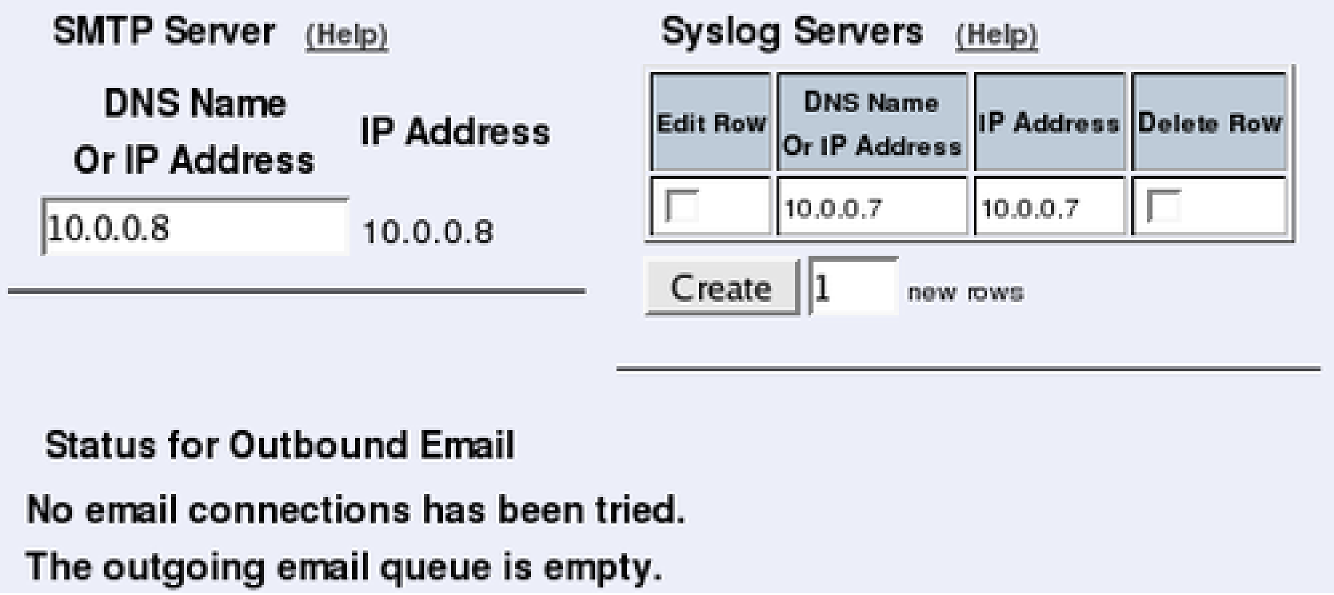
Saves the Log Classes configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

Log Sending

In 3Com VCX IP Telecommuting Module, there are two ways of sending log messages automatically to somewhere outside the box; to send to a syslog server and to send an email to an email address. If either method is used, the Telecommuting Module must know where to send this. On this page, servers for log sending are configured.



SMTP Server (Help)

DNS Name Or IP Address	IP Address
10.0.0.8	10.0.0.8

Syslog Servers (Help)

Edit Row	DNS Name Or IP Address	IP Address	Delete Row
□	10.0.0.7	10.0.0.7	□

1 new rows

Status for Outbound Email

No email connections has been tried.

The outgoing email queue is empty.

SMTP Server

Here, you set an SMTP server for the log messages that the Telecommuting Module generates. This server will send the email messages to the email addresses set on the **Log Classes** page. If the connection between the Telecommuting Module and the SMTP server isn't working, an error message will be shown on this page, and be logged according to the log class set on the **Logging Configuration** page. However, no error message will be shown here if the primary SMTP server can't connect to other mail servers. Therefore you should test if email log messages to the addresses set under **Log Classes** really reach their destination addresses.

Every log message does not create a separate email; the Telecommuting Module collects log messages and sends them every 5 minutes. The first message is sent within a minute.

Email sent from the Telecommuting Module has the From address "3Com VCX IP Telecommuting Module".

Enter the DNS name or IP address of the SMTP server.

Status for Outbound Email

A message is shown here if the Telecommuting Module can't connect to the mail server selected under **SMTP Server**, or if other errors concerning email occur. .

Syslog Servers

Here, you enter one or more syslog servers for the syslog messages that the Telecommuting Module generates. This is the computer which receives and stores the syslog log messages.

Dynamic

If an interface will receive its IP address from a DHCP server, the Telecommuting Module can also get information about its syslog server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

DNS Name Or IP Address

Enter the DNS name or IP address for the syslog server.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the configuration for Log Sending to the preliminary configuration.

Cancel

Reverts the fields to the previous configuration.

Chapter 10. SIP Services

SIP (Session Initiation Protocol) is a protocol for creating and terminating various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP takes care of the initiation, modification and termination of a session with one or more participants. The protocol makes it possible for the participants to agree on what media types they should share. You can find more information about SIP in appendix A, More About SIP, and in RFC 3261.

The SIP module in the 3Com VCX IP Telecommuting Module handles SIP requests for users who have registered on the Telecommuting Module itself or a machine connected to the Telecommuting Module (see also Local Registrar). The Telecommuting Module receives the request via the firewall (or, for the Standalone type, directly from the clients) and processes it. When the SIP negotiation is finished, the Telecommuting Module lets the media streams of this SIP session through. All media streams pass through the Telecommuting Module if the clients are located on different firewall interfaces.

Administration of SIP

To enable the SIP function of the Telecommuting Module, you must at least configure on the **Basic Settings** page.

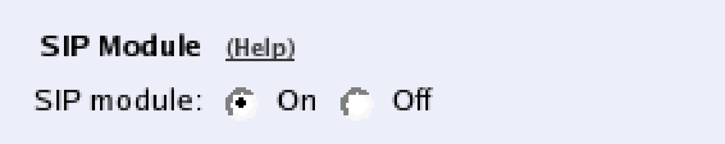
These SIP functions are configured in the **SIP Services** section:

- SIP module on/off
- SIP logging
- Port range for SIP media
- Interoperability settings
- SIP timeouts
- Remote SIP Connectivity (requires a Remote SIP Connectivity Module)

Basic Settings

Here, you make basic settings for the Telecommuting Module SIP management.

SIP Module



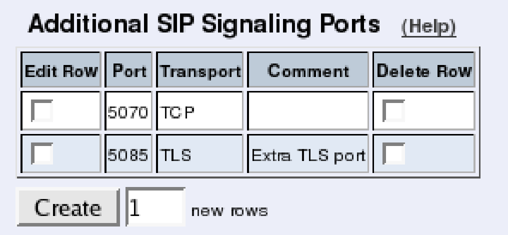
SIP Module (Help)

SIP module: ● On ○ Off

Here, select whether the SIP module should be enabled or disabled. If you select to **Disable SIP module**, no other SIP settings will have any effect.

Additional SIP Signaling Ports

Normally, the Telecommuting Module listens for SIP signaling on ports 5060 (UDP and TCP) and 5061 (TLS). You can make it listen for SIP signaling on additional ports. When ports are added here, they are reserved for SIP signaling on all the Telecommuting Module IP addresses.



Additional SIP Signaling Ports (Help)

Edit Row	Port	Transport	Comment	Delete Row
□	5070	TCP		□
□	5085	TLS	Extra TLS port	□

Create 1 new rows

Port

Enter an additional port on which the Telecommuting Module should listen for SIP signaling. The Telecommuting Module will then receive SIP signaling on this port for all its IP addresses.

SIP signaling over TLS cannot be received on a Telecommuting Module port which is used for something else, like configuration of the Telecommuting Module.

Transport

Select which SIP signaling transports should be allowed on this port.

Comment

Enter a comment to remind yourself why you added the port.

Delete Row

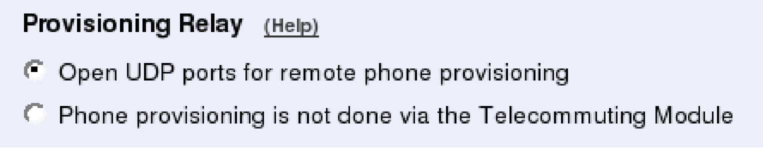
If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Provisioning Relay

Remote phones usually need to access your PBX for provisioning. For many phones, the provisioning server is the same as their registrar, which means that it is the IP address of the Telecommuting Module. To enable provisioning, the Telecommuting Module can open ports for this traffic.



Provisioning Relay (Help)

● Open UDP ports for remote phone provisioning

○ Phone provisioning is not done via the Telecommuting Module

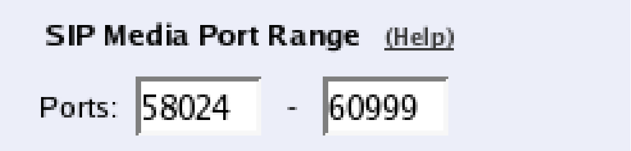
Select if the Telecommuting Module should open ports for provisioning traffic, or if the phones get their settings in another way.

SIP Media Port Range

State a port interval which the Telecommuting Module should use for SIP media streams. You can use any high ports except 4500 (reserved for NAT-T) and 65097-65200 (reserved for RADIUS).

Note! A change in the port interval will make the SIP module restart when the configuration change is applied.

When the SIP module is restarted, all active SIP sessions (SIP calls, video conferences etc) will be torn down and all SIP user registrations will be removed.



SIP Media Port Range (Help)

Ports: 58024 - 60999

Enter the lower and upper limit of the port range that the Telecommuting Module should use for media streams. The upper limit must be at least as high as the lower limit.

Public IP address for NATed Telecommuting Module

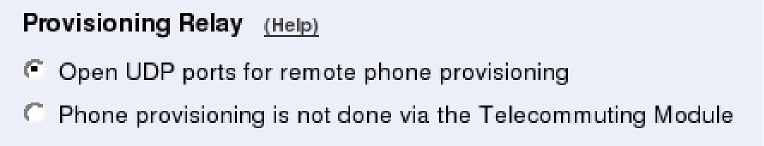
Sometimes, the Telecommuting Module is located behind a NAT box that is not SIP-aware. This will make signaling go awry, with the result that in many cases there will be voice in only one direction.

This can be corrected by entering the public IP address that the Telecommuting Module will appear to have. When sending SIP signaling towards its default gateway, the Telecommuting Module will use that IP address instead of its private one, which will get media to the right place.

Note that the NATing device must also be configured to forward SIP signaling on that IP address to the Telecommuting Module.

If nothing is entered here, the Telecommuting Module will use its own IP addresses.

This setting is not supported for the Standalone configuration.



Provisioning Relay (Help)

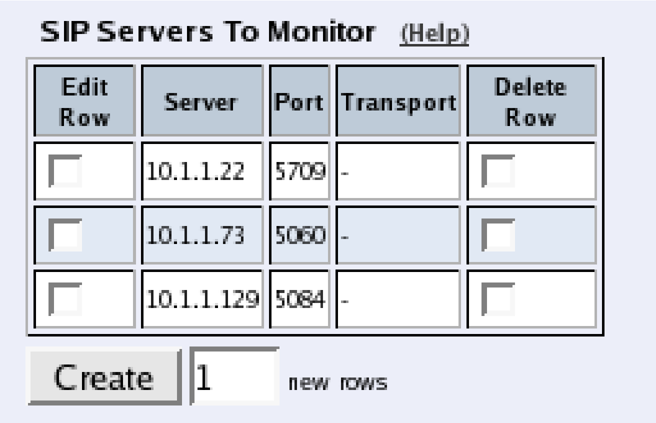
● Open UDP ports for remote phone provisioning

○ Phone provisioning is not done via the Telecommuting Module

SIP Servers To Monitor

Your Telecommuting Module can be made to monitor SIP servers, to check that they are alive. The information is used by the Telecommuting Module when SIP signaling should be passed on to the server in question. This is useful when a domain resolves to several individual hosts; the Telecommuting Module will know immediately if one of them is down, which will speed up the call connection.

The SIP server must respond with a SIP packet to OPTIONS packets to be monitored in this way.



SIP Servers To Monitor (Help)

Edit Row	Server	Port	Transport	Delete Row
□	10.1.1.22	5709	-	□
□	10.1.1.73	5060	-	□
□	10.1.1.129	5084	-	□

Server

Enter the host name, domain name, or IP address of the server to be monitored.

Port

Enter the port to be monitored on that host. This should be the port to use for SIP signaling.

Transport

Select the transport to be monitored on that host. This should be the transport to use for SIP signaling.

Delete Row

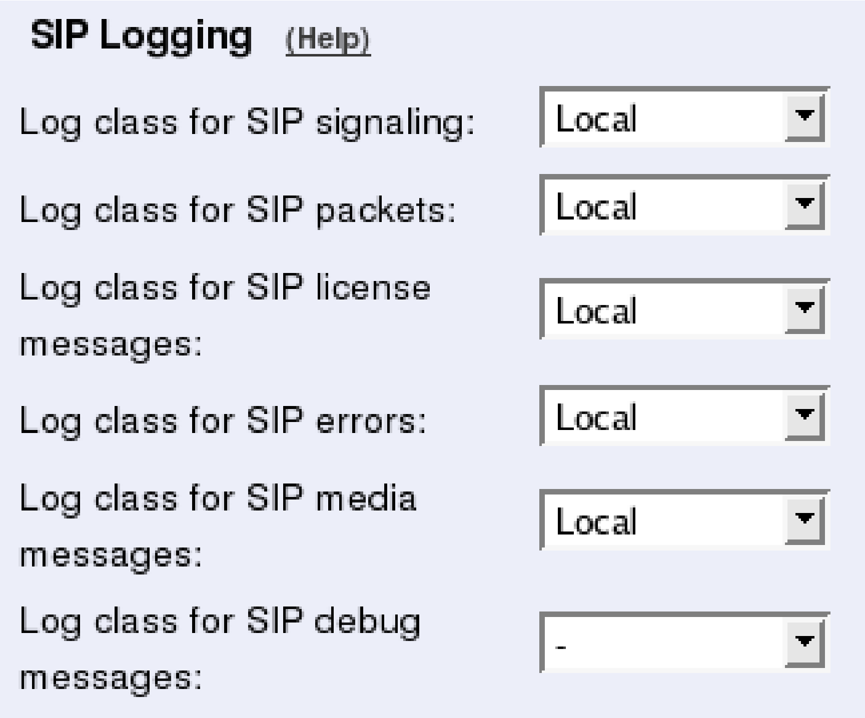
If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

SIP Logging

The same settings can also be found on the **Logging Configuration** page under **Logging**.



SIP Logging

Log class for SIP signaling: Local

Log class for SIP packets: Local

Log class for SIP license messages: Local

Log class for SIP errors: Local

Log class for SIP media messages: Local

Log class for SIP debug messages: -

Log class for SIP signaling

For each SIP packet, the Telecommuting Module generates a message, containing the sender and receiver of the packet and what type of packet it is. Select a log class for these log messages.

Log class for SIP packets

The Telecommuting Module logs all SIP packets (one SIP packet is many lines). Select a log class for the SIP packets.

Log class for SIP license messages

The Telecommuting Module logs license messages. Select a log class for these messages.

Log class for SIP errors

The Telecommuting Module sends a message if there are any SIP errors. Select a log class for these log messages.

Log class for SIP media messages

The Telecommuting Module creates log messages about when media streams are set up and torn down. Select a log class for these messages.

Log class for SIP debug messages

The Telecommuting Module logs a lot of status messages, for example the SIP initiation phase of a reboot. Select a log class for these messages.

Save

Saves the Basic Settings configuration to the preliminary configuration.

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

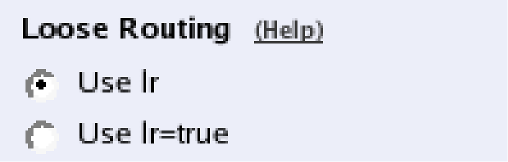
Interoperability

The SIP standard is still young and under considerable development. As an effect, several implementations of the standard omits parts of it, or makes guesses as to what will be accepted.

3Com VCX IP Telecommuting Module adheres rather well to the standard (RFC 3261) per default, but you can also adjust the configuration to make more allowing for known issues in various SIP implementations.

Loose Routing

The Telecommuting Module uses the parameter "lr" in its SIP signaling to announce to other SIP devices that it uses loose routing. Some other SIP implementations incorrectly expect the lr parameter to be followed by a value, i.e. "lr=true". If you select that the Telecommuting Module should add this value to its SIP signaling, it will work with these implementations, too. This could affect its interaction with other SIP devices that conform to the SIP standard very strictly.



Loose Routing (Help)

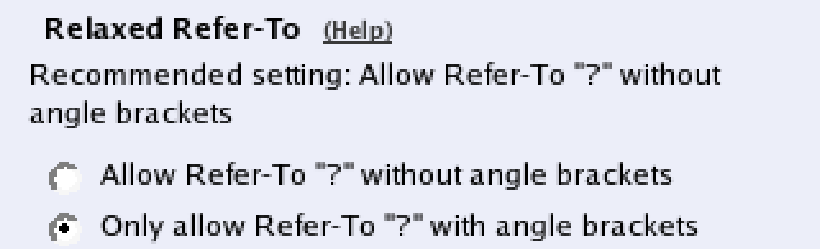
● Use lr

○ Use lr=true

Select to use **lr** or **lr=true**.

Relaxed Refer-To

The SIP standard requires that a Refer-To header with a question mark in it must be contained within angle brackets. Some clients do not honor this.



Relaxed Refer-To (Help)

Recommended setting: Allow Refer-To "?" without angle brackets

○ Allow Refer-To "?" without angle brackets

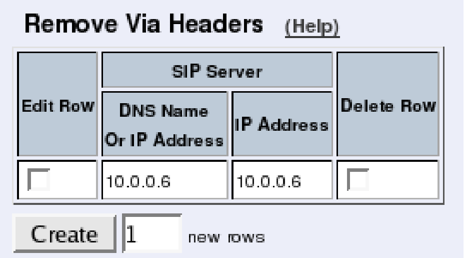
● Only allow Refer-To "?" with angle brackets

Select whether the Telecommuting Module should accept Refer-To headers without angle brackets, but containing question marks. The recommended setting is **Only allow Refer-To "?" with angle brackets**.

Remove Via Headers

Some SIP servers won't accept requests with more than one Via header. To be able to communicate via these servers, you can select to remove all Via headers but one in requests to those servers. The Via headers are added again when the reply passes the Telecommuting Module.

Here, list servers that won't accept more than one Via header in SIP requests.



Remove Via Headers (Help)

Edit Row	SIP Server		Delete Row
	DNS Name Or IP Address	IP Address	
□	10.0.0.6	10.0.0.6	□

SIP Server

Enter the DNS name or IP address for the SIP servers that won't accept more than one Via header.

Delete Row

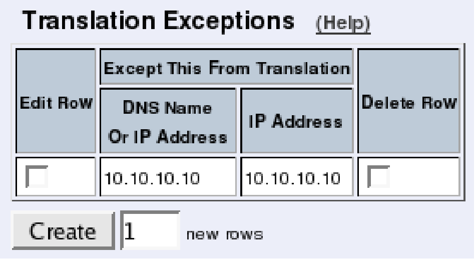
If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Translation Exceptions

Usually, the Telecommuting Module rewrites IP addresses in the SIP signaling to hide it for the receiver. For some reasons, you might want to except certain IP addresses from being rewritten. Enter those IP addresses in the table.



Translation Exceptions (Help)

Edit Row	Except This From Translation		Delete Row
	DNS Name Or IP Address	IP Address	
□	10.10.10.10	10.10.10.10	□

Except this from translation

Enter the DNS name or IP address to be excepted from IP address translation. If you enter a DNS name, the corresponding IP address will be excepted from translation.

Delete Row

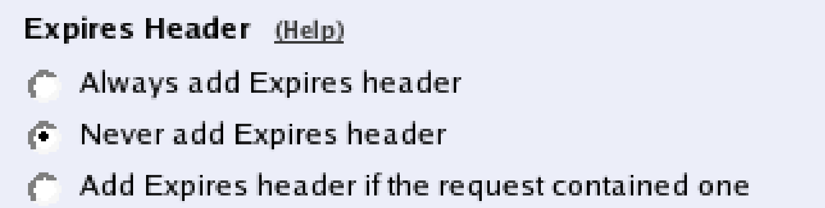
If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Expires Header

Some SIP clients don’t understand the expires: parameter in the Contact header. To set the expiration time for those clients, you can make the Telecommuting Module add to REGISTER request replies an Expires header with the expires value in it.



Expires Header (Help)

○ Always add Expires header

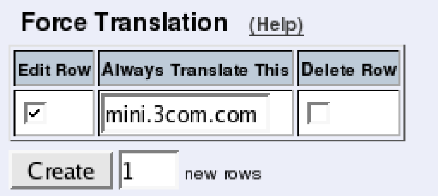
● Never add Expires header

○ Add Expires header if the request contained one

Select to **Always add Expires header**, **Never add Expires header**, or **Add Expires header if the request contained one**. The last means that the Telecommuting Module will add an Expires header to the response if the request from the client contained one.

Force Translation

Normally, the Telecommuting Module does not translate domain names in Contact and Via headers, but lets them through without modification. However, there are situations when domains should be translated. Enter domain names that should be translated in this table.



Force Translation (Help)

Edit Row	Always Translate This	Delete Row
☑	mini.3com.com	□

Create 1 new rows

Always Translate This

Enter the domain that should always be translated. Wherever this domain is present in the Contact and Via header URIs, it will be replaced with the Telecommuting Module’s own IP address.

Delete Row

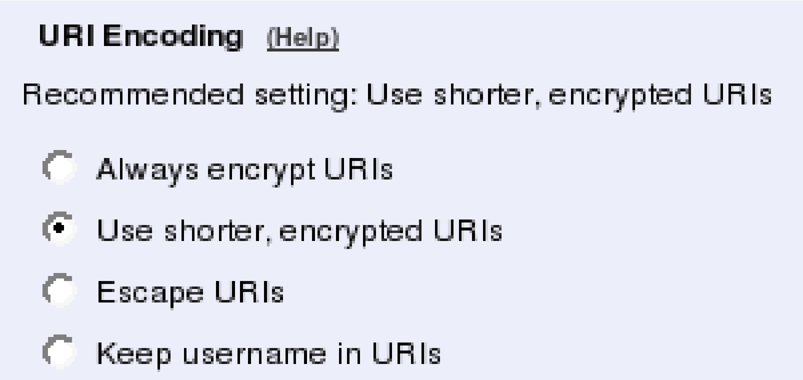
If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

URI Encoding

When registering a SIP client on one side of the Telecommuting Module to a SIP server on the other side, the Contact header is normally encrypted and rewritten. By doing this, we make it possible for the SIP server to track when the same user is sending requests from different places. It is possible to turn encryption and rewriting off, and to shorten the encrypted URI in Contact headers passing through the Telecommuting Module.



URI Encoding

Recommended setting: Use shorter, encrypted URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

○ Escape URIs

○ Keep username in URIs

Select what to do with Contact headers.

Always encrypt URIs will make the Telecommuting Module encrypt the entire Contact header URI.

Use shorter, encrypted URIs will make the Telecommuting Module generate a random string for the incoming Contact URI. This will then be used as the username part of the outgoing Contact header URI.

When you select this, the Telecommuting Module makes no checks of incoming SIP URIs. It becomes possible in theory to trick the Telecommuting Module to send SIP packets anywhere, so security is drastically reduced.

Escape URIs will make the Telecommuting Module escape the entire original URI and use that as the username part of the outgoing Contact.

The encryption of a Contact URI is changed when the Call-ID changes, when the client gets a new IP address, or when the user changes its Contact URI.

When you select this, the Telecommuting Module makes no checks of incoming SIP URIs. It becomes possible in theory to trick the Telecommuting Module to send SIP packets anywhere, so security is drastically reduced.

Keep username in URIs will make the Telecommuting Module keep the original username pare of the Contact URI, and only replace the domain part.

When you select this, it will be impossible for the remote SIP server to tell if requests for a certain user belong to one or several clients, as it has no means of telling the client registrations for a user apart. This means that if a user registers from two clients, and then unregisters from one of them, the SIP server will remove its only registration record for that user.

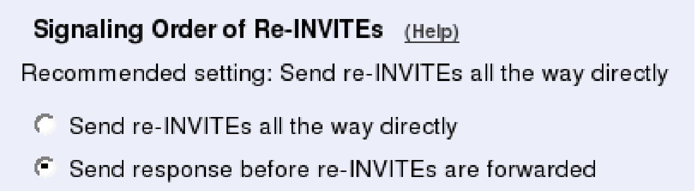
The Telecommuting Module also makes no checks of incoming SIP URIs. It becomes possible in theory to trick the Telecommuting Module to send SIP packets anywhere, so security is drastically reduced.

Signaling Order of Re-INVITEs

When the Telecommuting Module acts as a B2BUA (e.g. almost always when performing SIP Trunking), it normally handles re-INVITEs by forwarding them and waiting for a response, just as for the original INVITE.

With some SIP devices, this can cause problems. For these situations, the Telecommuting Module can instead handle the re-INVITEs hop by hop, meaning that it sends a "200 OK" response back before forwarding the INVITE to the next SIP device.

The consequence will be that the Telecommuting Module will re-use the old SDP from the other end when sending the 200. For dialogs where the re-INVITE is used to change codec or some other RTP parameter, the recommended way is to send re-INVITEs all the way directly.



Signaling Order of Re-INVITEs (Help)

Recommended setting: Send re-INVITEs all the way directly

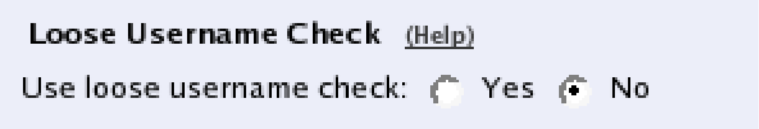
○ Send re-INVITEs all the way directly

● Send response before re-INVITEs are forwarded

Select if the INVITEs should be sent all the way, or be processed hop by hop.

Loose Username Check

Normally, the Telecommuting Module checks that the authentication username equals the username in the From header. Some clients use their whole address as authentication username (ie: user@host.com), which means that the username "user" in the From header is compared with the authentication username "user@host.com". This authentication will fail. With this function, "@host.com" is stripped from the authentication username.



Loose Username Check (Help)

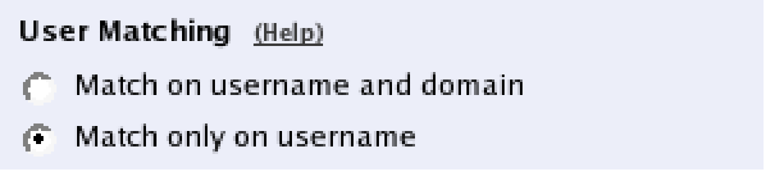
Use loose username check: ○ Yes ● No

Select if the entire SIP address or only the username should be used as the authentication name.

User Matching

Here, you can select to match on username only or username as well as domain.

If you match on username only, users with the same username will be treated as the same, even when they are under different domains.



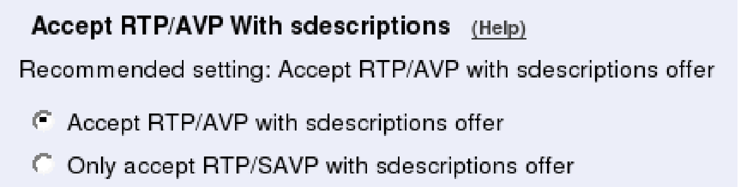
User Matching (Help)

○ Match on username and domain

● Match only on username

Accept RTP/AVP With sdescriptions

When sdescriptions are used, they should be presented as "RTP/SAVP" in the SDP offer sent by the client. Some clients choose to code them as "RTP/AVP" instead, to make clients, unaware of sdescriptions, to accept the SDP as an offer. Select here if the Telecommuting Module should accept incoming offers where sdescriptions are presented as "RTP/AVP" offers.



Accept RTP/AVP With sdescriptions (Help)

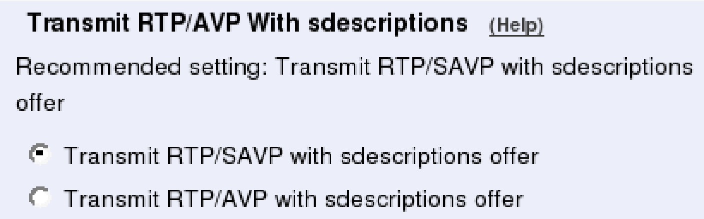
Recommended setting: Accept RTP/AVP with sdescriptions offer

● Accept RTP/AVP with sdescriptions offer

○ Only accept RTP/SAVP with sdescriptions offer

Transmit RTP/AVP With sdescriptions

When sdescriptions are used, they should be presented as "RTP/SAVP" in the SDP offer sent by the client. Some clients can't understand the "RTP/SAVP" notation. In these cases, you might want to offer them as "RTP/AVP" instead. This violates the standard, but makes the offer compatible with clients unaware of sdescriptions. Select here if the Telecommuting Module should present outgoing offers where sdescriptions are presented as "RTP/AVP" or as "RTP/SAVP".



Transmit RTP/AVP With sdescriptions (Help)

Recommended setting: Transmit RTP/SAVP with sdescriptions offer

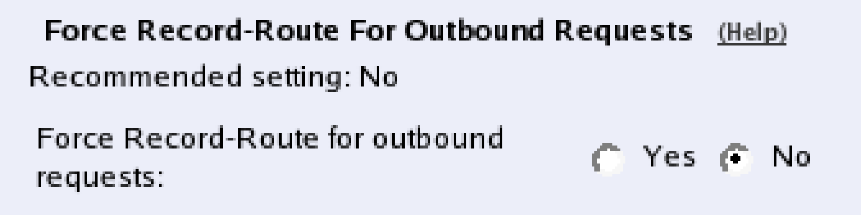
● Transmit RTP/SAVP with sdescriptions offer

○ Transmit RTP/AVP with sdescriptions offer

Force Record-Route for Outbound Requests

Here, you select if the Telecommuting Module should add a Record-Route header to all requests received by the Telecommuting Module, but whose Request-URI does not contain one of its **Local SIP Domains**.

The Record-Route header makes all subsequent SIP signaling for this session to be routed via the Telecommuting Module even if it is not the shortest route.



Force Record-Route For Outbound Requests (Help)

Recommended setting: No

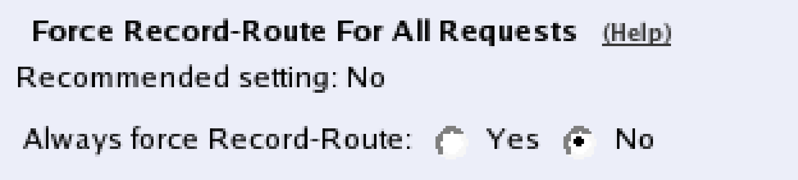
Force Record-Route for outbound requests: ○ Yes ● No

Here, you select to add Record-Route headers for outbound requests or not.

Force Record-Route for All Requests

Here, you select if the Telecommuting Module should add a Record-Route header to all requests received by the Telecommuting Module, which should be passed on to another client/server.

The Record-Route header makes all subsequent SIP signaling for this session to be routed via the Telecommuting Module even if it is not the shortest route.



Force Record-Route For All Requests (Help)

Recommended setting: No

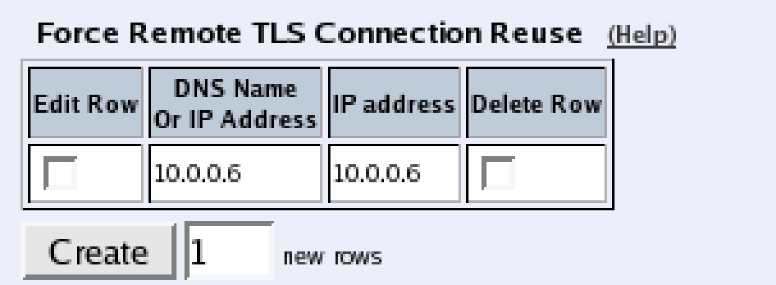
Always force Record-Route: ○ Yes ● No

Here, you select to add Record-Route headers for all requests or not.

Force Remote TLS Connection Reuse

Enter SIP servers to which the Telecommuting Module connects using TLS. For the listed servers, the Telecommuting Module will use the actual source port for the TLS connection instead of port 5061.

This is useful in the SIP signaling, where port numbers are used in Via and Route headers.



Force Remote TLS Connection Reuse (Help)

Edit Row	DNS Name Or IP Address	IP address	Delete Row
□	10.0.0.6	10.0.0.6	□

Create 1 new rows

DNS Name Or IP Address

Enter the DNS name or IP address for a SIP server for which the Telecommuting Module should reuse TLS ports.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Delete Row

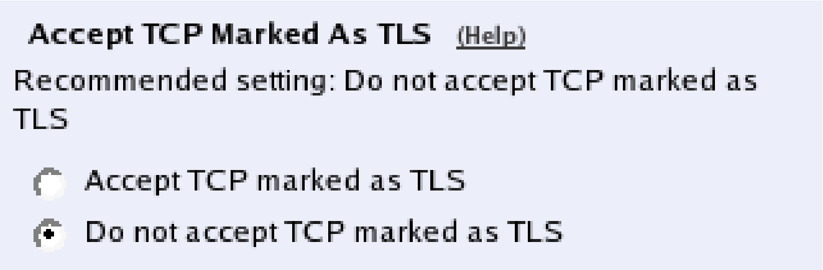
If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Accept TCP Marked As TLS

When a TLS accelerator is used, SIP packets can be sent to the Telecommuting Module via TCP, but the packet content will look as if TLS was used.



Accept TCP Marked As TLS (Help)

Recommended setting: Do not accept TCP marked as TLS

○ Accept TCP marked as TLS

● Do not accept TCP marked as TLS

Select if TCP packets with TLS content should be accepted. The recommended setting is not to accept them.

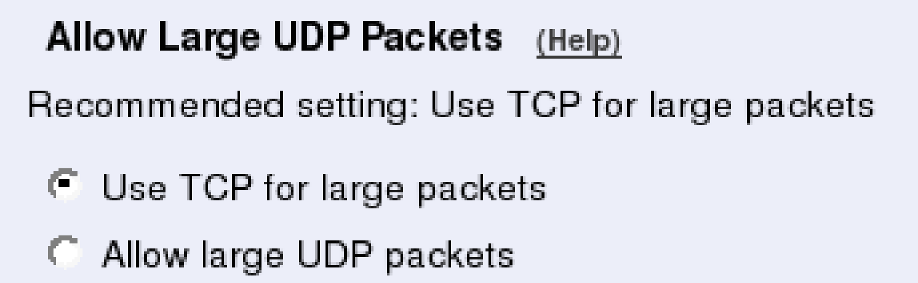
Allow Large UDP Packets

Sometimes, the SIP signaling UDP packets get larger than the standard (RFC 3261) allows. There are two ways to handle this; either send large UDP packets, which may become fragmented into several packets, or use TCP.

Some SIP devices may not be able to receive TCP packets, which is a violation of RFC 3261. This means that you have to allow large UDP packets (larger than 1300 byte), but to do this violates section 18.1.1 in RFC 3261.

Note that there also may be SIP devices that cannot handle fragmented UDP packets, even though this also violates RFC 3261.

This setting only affects SIP signaling packets.



Allow Large UDP Packets (Help)

Recommended setting: Use TCP for large packets

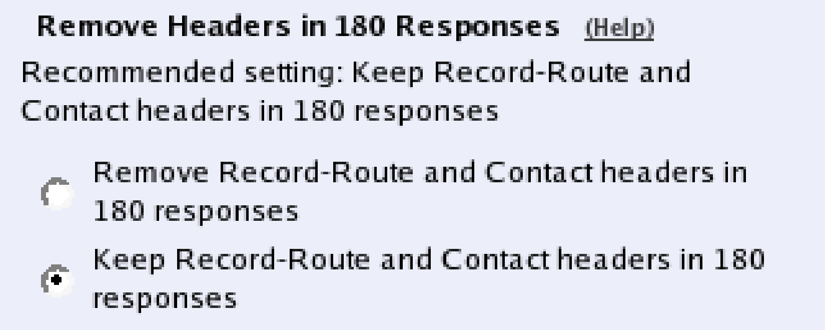
● Use TCP for large packets

○ Allow large UDP packets

Select if large UDP packets should be allowed. The recommended setting is to use TCP when the packets become too large.

Remove Headers in 180 Responses

Some SIP servers require that the Contact and Record-Route headers are removed from 180 responses.



Remove Headers in 180 Responses (Help)

Recommended setting: Keep Record-Route and Contact headers in 180 responses

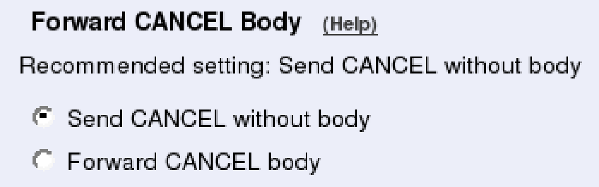
○ Remove Record-Route and Contact headers in 180 responses

● Keep Record-Route and Contact headers in 180 responses

Select if the Telecommuting Module should remove these headers in 180 responses. The recommended setting is to keep the headers.

Forward CANCEL Body

Normally, a CANCEL request does not contain a body. There are some systems which put a body in these requests. As every SIP proxy generates a new CANCEL instead of just forwarding the incoming request, any body in the incoming request is usually dropped. Select here if the Telecommuting Module should forward any CANCEL body when the CANCEL itself is forwarded.



Forward CANCEL Body (Help)

Recommended setting: Send CANCEL without body

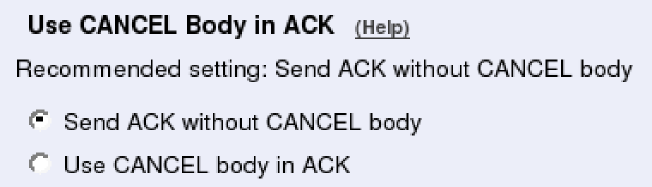
● Send CANCEL without body

○ Forward CANCEL body

Use CANCEL Body In ACK

Normally, a CANCEL request does not contain a body. There are some systems which put a body in these requests. As every SIP proxy generates a new CANCEL instead of just forwarding the incoming request, any body in the incoming request is usually dropped.

For INVITE requests, an ACK is always required. Some systems require that the body from the CANCEL should also be used in the ACK. Select here if the Telecommuting Module should use the CANCEL body in the ACK.



Use CANCEL Body in ACK (Help)

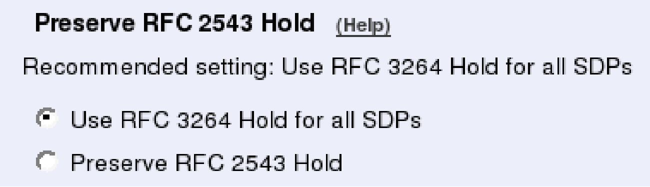
Recommended setting: Send ACK without CANCEL body

● Send ACK without CANCEL body

○ Use CANCEL body in ACK

Preserve RFC 2543 Hold

sendonly streams are defined differently in RFC 2543 and RFC 3264. The Telecommuting Module uses the RFC 3264 way, and converts SDPs when the old behaviour is seen. In particular, the c= line is modified, as was not defined in RFC 2543. Some clients aren’t updated to RFC 3264 yet and will not understand what happens.



Preserve RFC 2543 Hold (Help)

Recommended setting: Use RFC 3264 Hold for all SDPs

● Use RFC 3264 Hold for all SDPs

○ Preserve RFC 2543 Hold

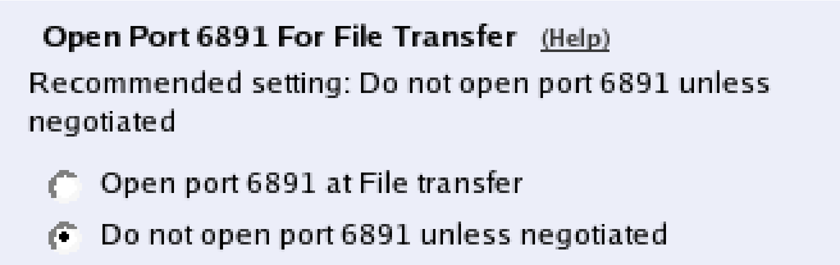
When Use RFC 3264 Hold is selected, the c= line with address 0.0.0.0 will be rewritten. When Use RFC 2543 Hold is selected, the c= line with address 0.0.0.0 will be left unmodified.

Open Port 6891 For File Transfer

Messenger clients do not always use the ports that are negotiated in the SIP signaling. In particular, the File Transfer function always uses the same port, regardless of what is negotiated. To make File Transfer work through the Telecommuting Module you must open port 6891, the Messenger File Transfer port.

You only need to do this if File Transfers are made between clients on different networks; if transfers are always only made between clients on the same network, no extra ports need to be opened.

Note: If more than one Messenger client performs file transfer through the Telecommuting Module at the same time, they could end up sending to each other's peers instead of their own. An attacker could possibly use this to intercept transfered files; don't use this mechanism to transfer sensistive data.



Open Port 6891 For File Transfer (Help)

Recommended setting: Do not open port 6891 unless negotiated

○ Open port 6891 at File transfer

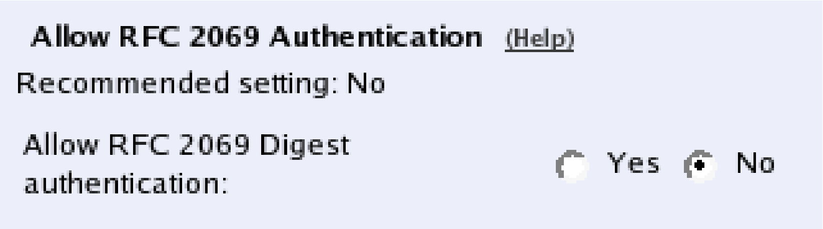
● Do not open port 6891 unless negotiated

Here, you select to open port 6891 automatically or not. The recommended setting is not to open it unless negotiated.

Allow RFC 2069 Authentication

Some SIP units can't handle Digest authentication as described in RFC 2617, but they still do authentication. 3Com VCX IP Telecommuting Module can allow the simpler form of authentication described in RFC 2069 to be able to interoperate with these units.

To allow this can decrease security. Use it only if units in your system need it.



Allow RFC 2069 Authentication (Help)

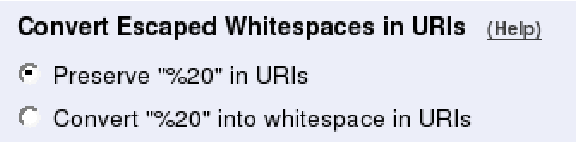
Recommended setting: No

Allow RFC 2069 Digest authentication: ○ Yes ● No

Select if authentication according to RFC 2069 should be allowed (**On**) or not (**Off**). It is recommended to keep this setting off.

Convert Escaped Whitespaces in URIs

Sometimes, whitespaces in incoming URIs are escaped, which make them look like "%20". This is most common in URIs in the Refer-To header used by the *REFER* method. As some other SIP devices cannot properly decrypt these escaped whitespaces, the Telecommuting Module can be made to convert them back to normal whitespaces.



Convert Escaped Whitespaces in URIs (Help)

● Preserve "%20" in URIs

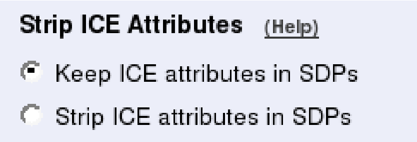
○ Convert "%20" into whitespace in URIs

Select if "%20" should be converted into a whitespace or preserved in URIs.

Strip ICE Attributes

Some SIP clients, like Microsoft Communicator 2007, seem to prefer ICE "a=candidate" attributes in SDP over other information, and it doesn't perform STUN tests as it is supposed to in order to verify the connection. This may sometimes result in no media.

A way to avoid this is to make the Telecommuting Module remove these attributes for all requests.



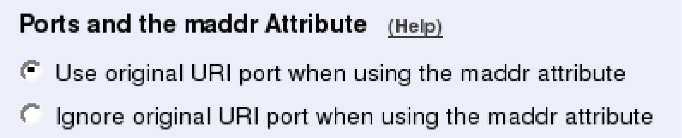
Strip ICE Attributes (Help)

● Keep ICE attributes in SDPs

○ Strip ICE attributes in SDPs

Ports and the maddr Attribute

The maddr attribute is used to point to a specific IP address, regardless of what the domain/IP address in the main URI should point to. This attribute only applies to the domain/IP address part according to RFC 3261, and other parameters in the original URI (like the port and transport) will still be used. However, some user agents expect that the maddr attribute will reset other URI parameters.



Ports and the maddr Attribute (Help)

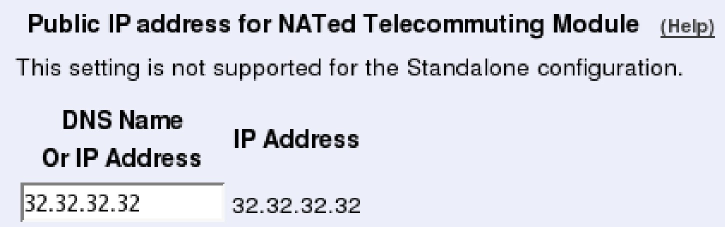
● Use original URI port when using the maddr attribute

○ Ignore original URI port when using the maddr attribute

Select if the Telecommuting Module should use the original URI parameters (as is defined in RFC 3261) or if the port stated in the original URI should be ignored.

Keep User-Agent Header When Acting as B2BUA

Usually, when the Telecommuting Module acts as a back to back user agent (B2BUA), it replaces the original User-Agent header with its own. This might cause problems if the other endpoint chooses what to do based on the User-Agent field and what is known about different user agent capabilities.



Public IP address for NATed Telecommuting Module (Help)

This setting is not supported for the Standalone configuration.

DNS Name Or IP Address	IP Address
32.32.32.32	32.32.32.32

Select if the Telecommuting Module should rewrite the User-Agent field or not.

Save

Saves the Interoperability configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

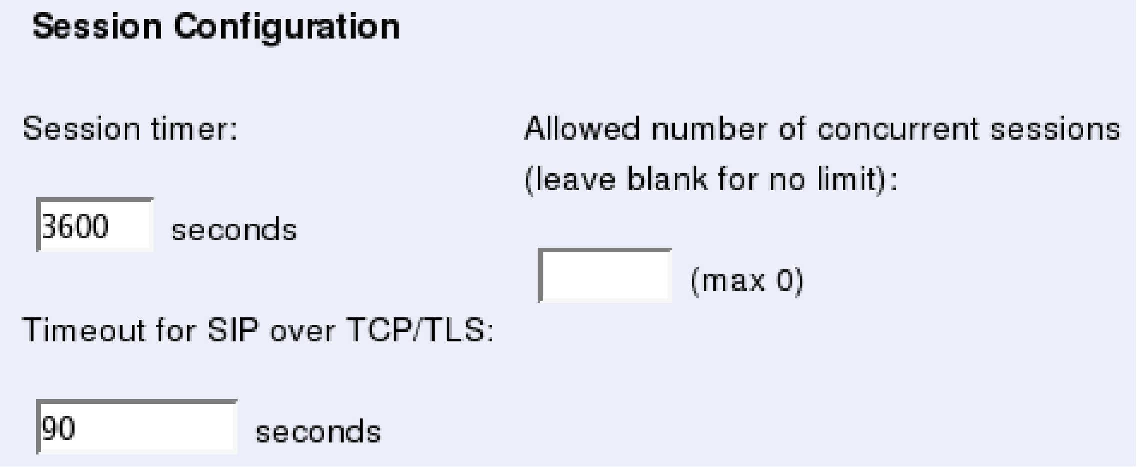
This button will only be visible if a DNS server has been configured.

Sessions and Media

Here, settings are made for the SIP timeouts and sessions negotiated via the Telecommuting Module.

Note that no DTMF settings are needed in the Telecommuting Module.

Session Configuration



Session Configuration

Session timer: 3600 seconds

Timeout for SIP over TCP/TLS: 90 seconds

Allowed number of concurrent sessions (leave blank for no limit): (max 0)

Session timer

Enter the maximum time for a SIP initiated connection. When the timeout is reached, the Telecommuting Module discards the media streams. The clients won't notice, as the connection is still active, but you won't hear anything as no media streams are let through. To avoid this, clients can regularly ask for new timeouts.

The Session timer must be at least 90 seconds to comply with the Min-SE requirement (RFC 4028).

Timeout for SIP over TCP/TLS

The **Timeout for SIP over TCP/TLS** decides how long a SIP connection over TCP with the Telecommuting Module may exist without having received a complete SIP request.

"0" or an empty field means that SIP over TCP or TLS cannot be used to the Telecommuting Module.

Allowed number of concurrent sessions

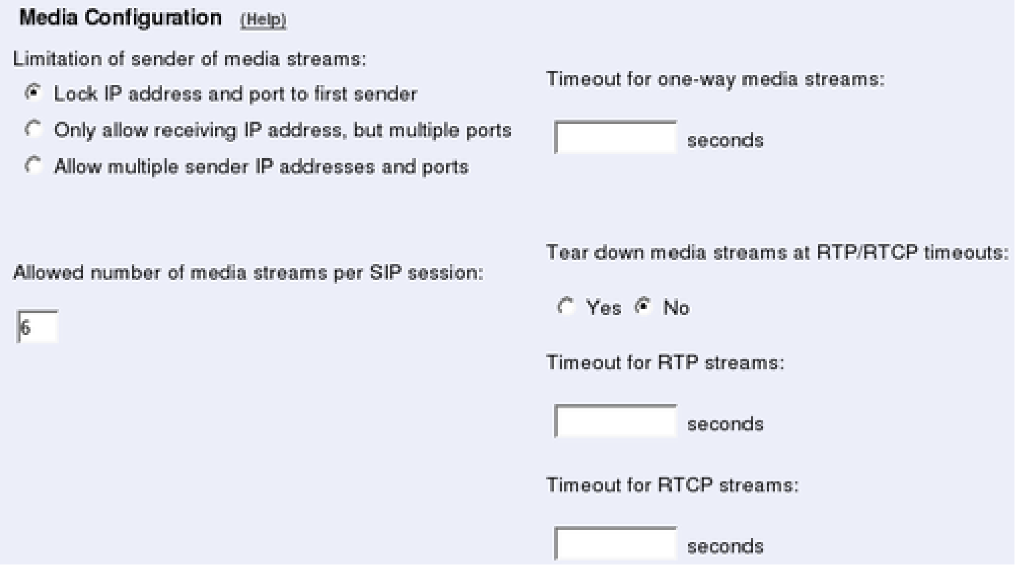
Enter the number of concurrent SIP sessions which the Telecommuting Module should handle.

Leave the field empty to allow as many sessions as there are SIP traversal licenses on the Telecommuting Module (number displayed inside parantheses). You can purchase additional SIP traversal licenses from your retailer.

Media Configuration

3Com VCX IP Telecommuting Module supports UDP and TCP media streams.

Set limitations for the media streams through the Telecommuting Module.



Media Configuration (Help)

Limitation of sender of media streams:

● Lock IP address and port to first sender

○ Only allow receiving IP address, but multiple ports

○ Allow multiple sender IP addresses and ports

Allowed number of media streams per SIP session: 6

Timeout for one-way media streams: seconds

Tear down media streams at RTP/RTCP timeouts: ○ Yes ● No

Timeout for RTP streams: seconds

Timeout for RTCP streams: seconds

Limitation of sender of media streams

This setting allows you to define who can send media in a SIP call. This is never negotiated in the SIP signaling, and can theoretically be a completely different unit from the one receiving the media.

The Telecommuting Module usually locks a media stream to the first sender IP address and port (for security reasons). Some SIP clients change ports during the first media stream packets, which will block the media stream from being let through the Telecommuting Module. There are also scenarios where the media stream sender is changed to an entirely new sender.

You can select for the Telecommuting Module to **Lock IP address and port to first sender**, which will render the behaviour described above. **Only allow receiving IP address, but multiple ports** will allow media only from the IP address which will receive the media stream in the opposite direction, but allow for port changes on that IP address. **Allow multiple sender IP addresses and ports** lets the media stream through even if ports and/or IP addresses change.

Allowed number of media streams per SIP session

Enter the number of media streams a single SIP session can handle. This restriction is primarily made for preventing DOS attacks.

Timeout for one-way media streams

This setting is used by the Telecommuting Module to detect when media is only sent in one direction. If no media packets are received in one direction during the configured number of seconds, the Telecommuting Module creates a log message about this.

Tear down media streams at RTP/RTCP timeout

Here, you select if the Telecommuting Module should tear down media streams when the **Timeout for RTP streams** and **Timeout for RTCP streams** have been reached.

When the media streams are torn down, the session is still not terminated by the Telecommuting Module. This means that there will be no SIP messages sent out (like a BYE) to indicate that the streams were torn down.

Timeout for RTP streams

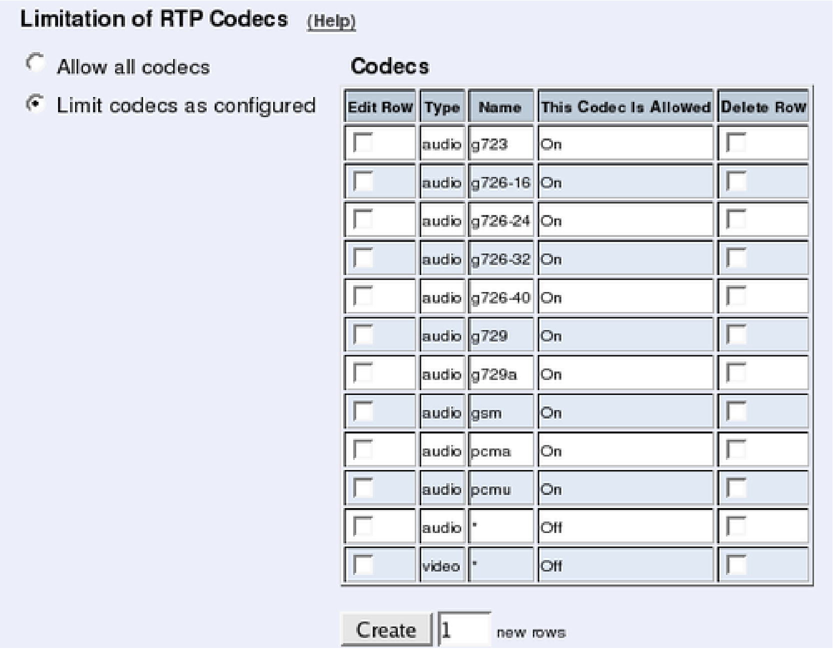
This setting is used by the Telecommuting Module to detect a closed media session, even when no signaling for this was made. If no RTP packets are received during the configured number of seconds, the Telecommuting Module creates a log message about this. If **Tear down media streams at timeout** was selected, the Telecommuting Module will also tear down the session when the RTP and RTCP timeouts have been reached.

Timeout for RTCP streams

This setting is used by the Telecommuting Module to detect a closed media session, even when no signaling for this was made. If no RTCP packets are received during the configured number of seconds, the Telecommuting Module creates a log message about this. If **Tear down media streams at timeout** was selected, the Telecommuting Module will also tear down the session when the RTP and RTCP timeouts have been reached.

Limitation of RTP Codecs

You might want to limit the use of some media codecs. There can be several reasons for this: some endpoints do not support the codecs, too many codec offers make the SIP request packet too large (which causes it to be fragmented), they consume too much bandwidth, or you want to allow only codecs with good enough voice quality.



Limitation of RTP Codecs (Help)

○ Allow all codecs

● Limit codecs as configured

Codecs

Edit Row	Type	Name	This Codec Is Allowed	Delete Row
□	audio	g723	On	□
□	audio	g726-16	On	□
□	audio	g726-24	On	□
□	audio	g726-32	On	□
□	audio	g726-40	On	□
□	audio	g729	On	□
□	audio	g729a	On	□
□	audio	gsm	On	□
□	audio	pcma	On	□
□	audio	pcmu	On	□
□	audio	*	Off	□
□	video	*	Off	□

Select if all codecs should be allowed, or just the codecs that are listed as allowed in the **Codecs** table.

Codecs

If you selected to only allow some codecs, enter the allowed codecs in the table.

Codecs that are not allowed can also be listed here, as long as you select "Off" under This Codec Is Allowed.

Type

Select the codec type. The "-" option will make this row match all media types where the codec name is defined.

Name

Enter the name of the codec to be allowed. The codec name should be entered as it appears in the SDP (like *PCMA* or *G723*).

This Codec Is Allowed

Select **On** to allow the codec and **Off** to block it.

Delete Row

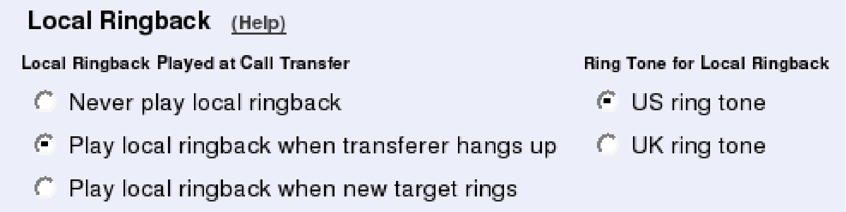
If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Local Ringback

When a call is transfered by the Telecommuting Module, the calling person normally does not hear any new ring tone. For various purposes, you might want the Telecommuting Module itself to play a ring tone for call transfers.



Local Ringback (Help)

Local Ringback Played at Call Transfer	Ring Tone for Local Ringback
○ Never play local ringback	● US ring tone
● Play local ringback when transferer hangs up	○ UK ring tone
○ Play local ringback when new target rings	

Local Ringback Played at Call Transfer

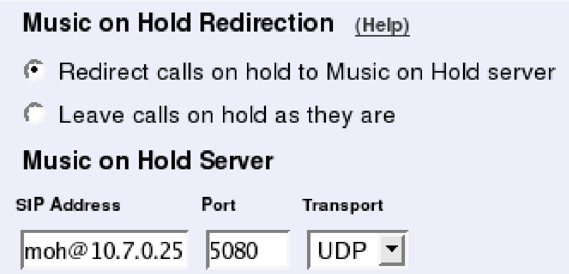
Select to never play local ringback, to play it when the new target phone rings, or to play it when the transferer hangs up.

Ring Tone for Local Ringback

Select the ring tone to be used when the Telecommuting Module plays ringback at call transfers.

Music on Hold Redirection

When a call is put on hold, the phone is sometimes not redirected to a Music on Hold server by the phone putting it on hold. When this happens, the Telecommuting Module can redirect the phone on hold to an external Music on Hold server instead.



Music on Hold Redirection (Help)

● Redirect calls on hold to Music on Hold server

○ Leave calls on hold as they are

Music on Hold Server

SIP Address	Port	Transport
moh@10.7.0.25	5080	UDP

Select if the Telecommuting Module should redirect calls on Hold to a Music on Hold server, or if the calls should be left as they are.

Music on Hold Server

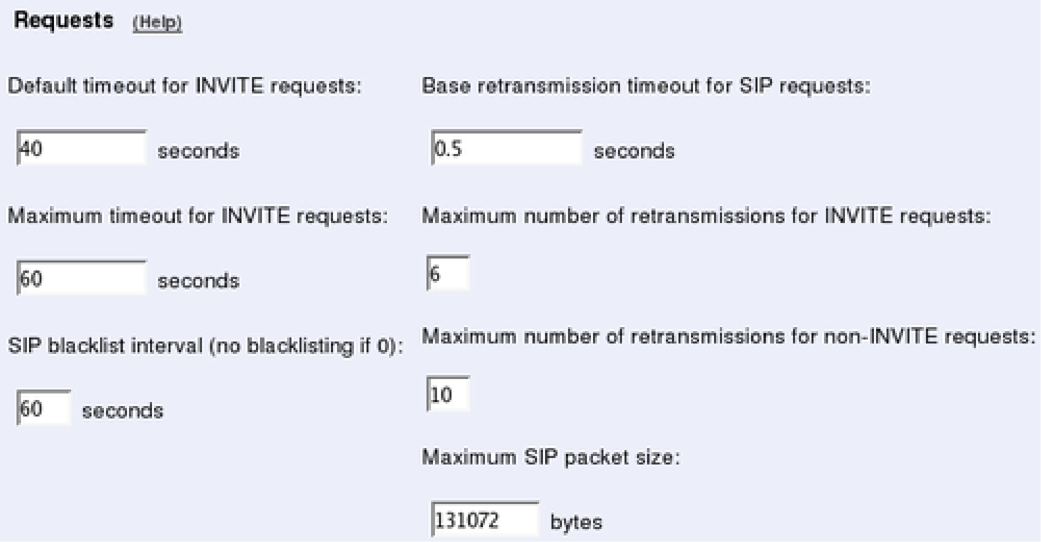
Enter the address and port of the Music on Hold server.

In the **SIP Address** field, enter the SIP domain/IP address of the Music on Hold server, and possibly also a username/extension for Music on Hold. This could look like `moh@10.47.10.17`.

You can also select to direct the request to a specific port, and select which transport should be used for the Music on Hold request. If no port is given, the Telecommuting Module will use the port from the DNS lookup (if a domain is given) or the standard SIP ports (5060 for UDP/TCP, 5061 for TLS).

Requests

You can configure timeouts for the different functions of the Telecommuting Module SIP module here. It is not recommended to change from the default values unless you really know what you're doing.



Requests (Help)

Default timeout for INVITE requests: 40 seconds

Maximum timeout for INVITE requests: 60 seconds

SIP blacklist interval (no blacklisting if 0): 60 seconds

Base retransmission timeout for SIP requests: 0.5 seconds

Maximum number of retransmissions for INVITE requests: 6

Maximum number of retransmissions for non-INVITE requests: 10

Maximum SIP packet size: 131072 bytes

Default timeout for INVITE requests

When sending an INVITE request you can specify a timeout, telling how long you can wait before getting an answer.

If no timeout is given when an INVITE request is sent, the Telecommuting Module sends the default timeout entered here.

Maximum timeout for INVITE requests

Here, enter the maximum timeout to allow for an INVITE request. If a higher timeout is given, the Telecommuting Module changes it to the value entered here.

SIP blacklist interval

When the Telecommuting Module sends out a SIP request and no reply is received, the SIP peer (say, a SIP server or an IP phone) will be blacklisten for the given time interval. This blacklisting means that no new SIP requests will be sent to the unit, even if requests that should be routed to this unit is received by the Telecommuting Module.

If the SIP request which caused the blacklisting, or a subsequent SIP request for that unit, can be routed to another device instead, the Telecommuting Module will keep on sending those requests to the next known IP address for the domain/user in question. When the blacklist ends, the Telecommuting Module will go back to sending requests to the previously blacklisted unit again.

If a 0 is entered into this field, the SIP blacklisting will not be used by the Telecommuting Module.

Base retransmission timeout for SIP requests

When the Telecommuting Module sends out a SIP request, it will expect a reply within a certain time. If no reply has been received within the **Base retransmission timeout**, the Telecommuting Module will start resending the request.

Maximum number of retransmissions for INVITE requests

When the Telecommuting Module sends out an INVITE request, it will wait for a reply until the **Base retransmission timeout** and then start to retransmit the request. The time intervals between retransmissions will double for each new retransmission.

Example: If the **Base retransmission timeout** is 0.5 seconds and the **Maximum number of retransmissions** is 6, the INVITE requests will be sent with intervals of 0.5 s, 1 s, 2 s, 4 s, 8 s, and 16 s.

Maximum number of retransmissions for non-INVITE requests

When the Telecommuting Module sends out a request which is not an INVITE request, it will wait for a reply until the **Base retransmission timeout** and then start to retransmit the request. The time intervals between retransmissions will double for each new retransmission until the interval reaches 4 seconds. After that, retransmissions will be made with a 4-second interval.

Example: If the **Base retransmission timeout** is 0.5 seconds and the **Maximum number of retransmissions** is 7, the requests will be sent with intervals of 0.5 s, 1 s, 2 s, 4 s, 4 s, 4 s, and 4 s.

Maximum SIP packet size

This setting allows you to set a limit to the size of SIP packets. A high value will increase performance, but use more memory. A low value will decrease performance, but use less memory.

Save

Saves the Sessions and Media configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Remote SIP Connectivity

If you are at a hotel or somewhere else where you find yourself behind a NAT-ing device that does not understand SIP, you will have use of the SIP Remote Connectivity of 3Com VCX IP Telecommuting Module. This will help your client to traverse the NAT, even if the device doing the NAT does not understand SIP. The SIP Remote Connectivity is only available if you have installed the Remote Connectivity module.

If you have a STUN-capable SIP client, you need just turn on the STUN server of the Telecommuting Module to make the client work behind NAT. If you have a SIP client that does not do STUN (or if the STUN-capable client is located behind a Symmetric NAT device), you have to use the Remote NAT Traversal feature. This is easier for the client, but generates more network traffic for the Telecommuting Module.

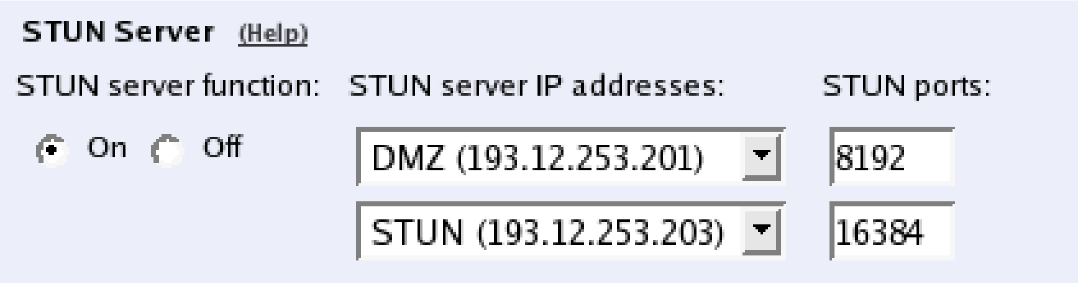
The settings on this page are only available when the Remote SIP Connectivity module has been installed.

STUN Server

Use the STUN server if you have STUN-aware SIP clients. You will need at least two public IP addresses to make it work with all client implementations of STUN.

STUN will not work properly if the NAT device uses Symmetric NAT (where the client's private IP/port pair translates to different public IP/port pairs depending on destination, and where computers other than the destination host are not allowed to reply on that IP/port pair).

The client also needs extra configuring for this; it must know which IP addresses and ports the STUN server has.



STUN Server (Help)

STUN server function: ● On ○ Off

STUN server IP addresses: DMZ (193.12.253.201), STUN (193.12.253.203)

STUN ports: 8192, 16384

STUN server

Select if the STUN server should be switched **On** or **Off**.

STUN server IP addresses

When activated, the STUN server requires two IP addresses, and a pair of ports on these two IP addresses, on the Telecommuting Module. STUN clients will then send test packets to these ports.

Select two IP addresses out of the ones assigned to the Telecommuting Module under **Directly Connected Networks** and **Alias** on the interface pages.

Note: for the STUN server to work properly, you need to select IP addresses which the clients can reach. In normal circumstances, this means that only public IP addresses can be used.

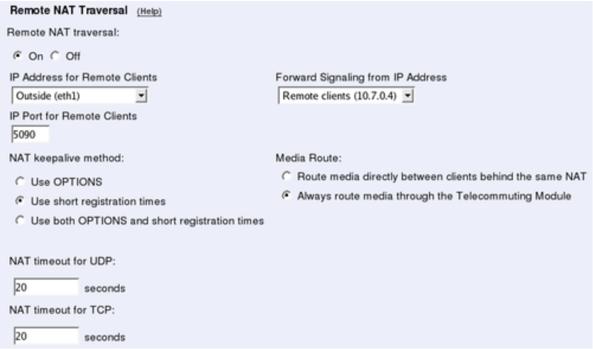
STUN ports

Enter the ports to use for the STUN server. These ports, on the IP addresses selected, will not be available for anything else.

Remote NAT Traversal

If your SIP client is not STUN-capable, you can use the built-in Remote NAT traversal feature of the Telecommuting Module. The client must register on the Telecommuting Module (or through it).

The SIP client needs to re-REGISTER, or respond to OPTIONS packets, rather often for this to work. The exact period for this depends on the NAT-ing device, but 20 seconds should be enough to get across most NAT boxes.



Remote NAT Traversal (Help)

Remote NAT traversal:

● On ○ Off

IP Address for Remote Clients: Outside (eth1)

Forward Signaling from IP Address: Remote clients (10.7.0.4)

IP Port for Remote Clients: 5090

NAT keepalive method:

○ Use OPTIONS
● Use short registration times
○ Use both OPTIONS and short registration times

Media Route:

○ Route media directly between clients behind the same NAT
● Always route media through the Telecommuting Module

NAT timeout for UDP: 20 seconds

NAT timeout for TCP: 20 seconds

Remote NAT traversal

Switch this function on or off.

Remote Clients Signaling Forwarding

Many SIP servers need to separate signaling to and from remote clients from signaling to and from the SIP Trunk. For this purpose, you can specify which IP address and port the remote clients will connect to. This can’t be the same IP address and port as what the SIP provider uses!

You also specify which IP address the Telecommuting Module will use when it forwards this SIP signaling to the server on the LAN. In this way, the trunk signaling and remote client signaling will be separated for the PBX.

IP Address for Remote Clients

Select which IP address remote clients connect to. This can be the same IP address as is used by the SIP provider, but then you need to select a different signaling port below.

IP Port for Remote Clients

Enter the signaling port to which remote SIP clients should connect. The Telecommuting Module will listen for SIP signaling on this port only for the IP address selected above.

If you select an alias IP address as the address to where remote clients should connect, you can’t enter a port, but must use port 5060 (5061 for TLS connections). If you select an IP address that was entered in the **Directly Connected Networks** table, you must specify a port.

You cannot select a port that is already in use for something else, or specified in the **Additional SIP Signaling Ports** table.

Forward Signaling from IP Address

Select which IP address the Telecommuting Module should use as the sender IP address when forwarding signaling from remote clients.

As all other SIP signaling will be forwarded using the IP address entered in the **Directly Connected Networks**, you must select an **Alias** IP address here.

NAT keepalive method

Clients using this function will have to send SIP packets very often, to keep the IP/port NAT binding. Select which method to use to force the clients to send packets frequently.

OPTIONS are sent from the Telecommuting Module to the client, and the client is required to respond to these OPTIONS packets to keep the NAT binding.

With **short registration times**, the Telecommuting Module tells the client to register with shorter intervals than it normally should have used, to keep the NAT binding. This will load the SIP registrar as well (if the Telecommuting Module is not the registrar), but is a method supported by all SIP clients.

NAT timeout for UDP

Enter the timeout the NAT box uses for UDP connections. The Telecommuting Module uses this information when deciding the intervals with which to send OPTIONS or tell the client to re-register.

NAT timeout for TCP

Enter the timeout the NAT box uses for TCP connections. The Telecommuting Module uses this information when deciding the intervals with which to send OPTIONS or tell the client to re-register.

Media Route

Usually, media is always sent via the Telecommuting Module when the Remote NAT Traversal feature is used. For clients behind the same NAT, media can be made to go directly between the clients, to lower the Telecommuting Module and network load.

Chapter 11. SIP Traffic

SIP (Session Initiation Protocol) is a protocol for creating and terminating various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP takes care of the initiation, modification and termination of a session with one or more participants. The protocol makes it possible for the participants to agree on what media types they should share. You can find more information about SIP in appendix A, More About SIP, and in RFC 3261.

The SIP module in the 3Com VCX IP Telecommuting Module handles SIP requests for users who have registered on the Telecommuting Module itself or a machine connected to the Telecommuting Module (see also Local Registrar). The Telecommuting Module receives the request via the firewall (or, for the Standalone type, directly from the clients) and processes it. When the SIP negotiation is finished, the Telecommuting Module lets the media streams of this SIP session through. All media streams pass through the Telecommuting Module if the clients are located on different firewall interfaces.

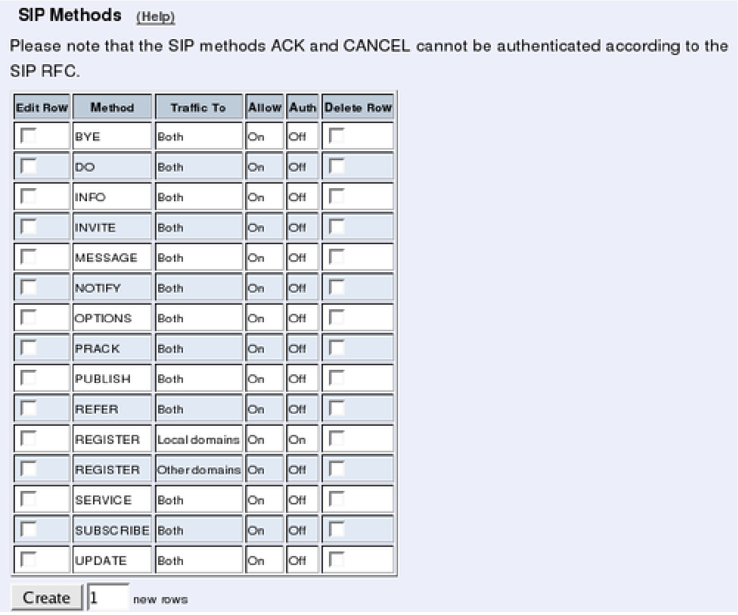
These SIP functions are configured in the **SIP Traffic** section:

- Allowed SIP methods
- Filtering of SIP signaling
- Local SIP domains
- SIP users
- SIP user authentication
- RADIUS accounting for SIP
- Routing of outgoing SIP requests
- Routing of incoming SIP requests

SIP Methods

Enter the SIP methods you want to allow and/or authenticate. Methods that are not listed here will be blocked by the Telecommuting Module.

Common methods are predefined (from RFC 3261). Note that the standard methods **ACK** and **CANCEL** cannot be authenticated.



SIP Methods (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
☐	BYE	Both	On	Off	☐
☐	DO	Both	On	Off	☐
☐	INFO	Both	On	Off	☐
☐	INVITE	Both	On	Off	☐
☐	MESSAGE	Both	On	Off	☐
☐	NOTIFY	Both	On	Off	☐
☐	OPTIONS	Both	On	Off	☐
☐	PRACK	Both	On	Off	☐
☐	PUBLISH	Both	On	Off	☐
☐	REFER	Both	On	Off	☐
☐	REGISTER	Local domains	On	On	☐
☐	REGISTER	Other domains	On	Off	☐
☐	SERVICE	Both	On	Off	☐
☐	SUBSCRIBE	Both	On	Off	☐
☐	UPDATE	Both	On	Off	☐

Method

Enter the name of the SIP method. This should be the name used in RFC 3261.

Traffic To

Here, you select the direction of the traffic. **Local domains** means that traffic to **Local SIP Domains** of this Telecommuting Module is affected by this row. **Other domains** means that traffic to all domains which are not **Local SIP Domains** of this Telecommuting Module is affected by this row. **Both** means that this row affects all traffic for the method, regardless of where the traffic is bound.

Allow

Select if the method in this direction should be allowed or not. For methods that are not allowed, the Telecommuting Module sends a 403 (Forbidden) response.

Auth

Select if the method in this direction should be authenticated or not. Note that SIP authentication must be turned on (on the **Authentication and Accounting** page), or authentication will not be performed.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the SIP Methods configuration to the preliminary configuration.

Cancel

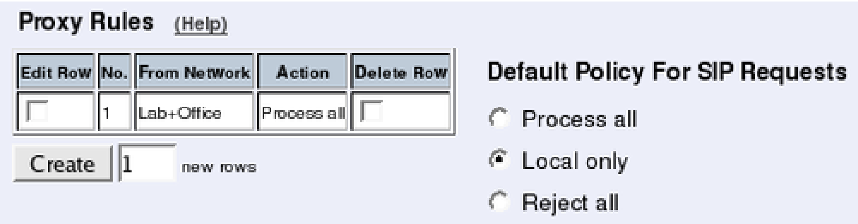
Clears and resets all fields in new rows and reset changes in old rows.

Filtering

Under Filtering, you can filter out SIP requests based on various criteria. Filter based on sender IP address (Sender IP Filter Rules), sending and receiving SIP user (Header Filter Rules), or content type (Content Types).

Sender IP Filter Rules

Here, you set all the rules for SIP requests from different networks. Requests that do not match any rule are handled according to the **Default Policy For SIP Requests**.



Proxy Rules (Help)

Edit Row	No.	From Network	Action	Delete Row
□	1	Lab+Office	Process all	□

Create [1] new rows

Default Policy For SIP Requests

○ Process all

● Local only

○ Reject all

No.

The **No.** field determines the order of the rules. Rules are used in the order in which they are displayed in the table; rule number 1 is first. The order is important if you used networks which partly contain the same IP addresses. To change order for a rule, enter the new number in the field and press **Save**.

From Network

The network name that the SIP request originates from. You can select between the networks defined on the **Networks and Computers** page under **Network Configuration**.

Action

Under **Action**, you select what to do with a SIP request from the selected network. The choices are **Process all**, which handles all requests regardless of destination, **Local only**, which only handles requests to **Local SIP Domains** (entered on the **Local Registrar** page), and **Reject all**, which doesn’t handle any requests at all.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

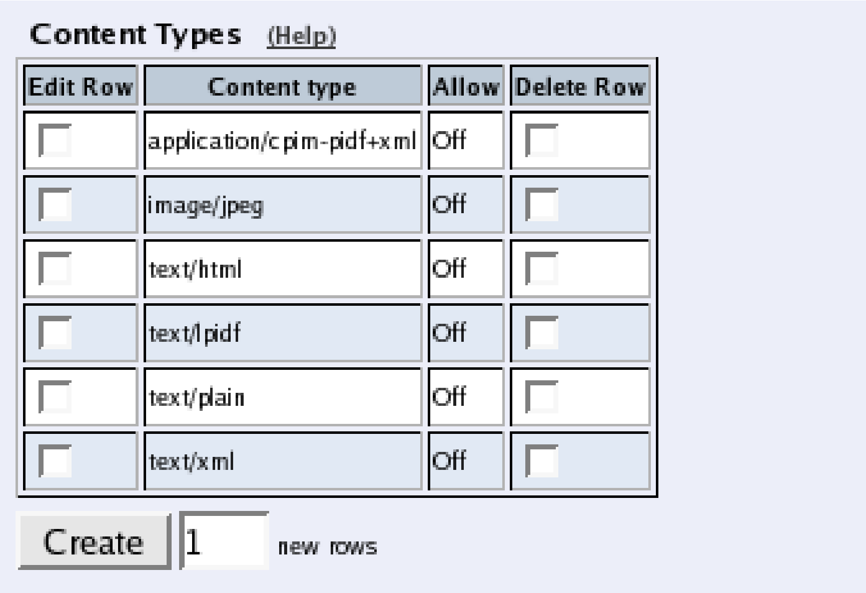
Default Policy For SIP Requests

Select what to do with SIP requests that do not match any of the **Proxy Rules**. The choices are **Process all**, which handles all requests regardless of destination, **Local only**, which only handles requests to **Local SIP Domains** (entered on the **Local Registrar** page), and **Reject all**, which doesn't handle any requests at all.

Content Types

The SIP packets present information in different ways, using content types (MIME types). Enter here which types the SIP proxy should accept. The most common MIME types are predefined and you only have to activate them.

The content types *application/sdp* (used for SIP requests), *application/xpidf+xml* (used for Presence) and *text/x-msmsgsinvite* (used by Messenger) are always accepted - you don't have to enter them into the table. You can find a complete list of MIME types at ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types/.



Edit Row	Content type	Allow	Delete Row
□	application/cpim-pidf+xml	Off	□
□	image/jpeg	Off	□
□	text/html	Off	□
□	text/lpidf	Off	□
□	text/plain	Off	□
□	text/xml	Off	□

Content Type

Enter the content type (only one in each row). The format is *category/type*, e.g. **`text/plain`**. You can also allow all content types by entering **`*/*`** in a row and allow it.

Allow

Select if the Telecommuting Module should allow (**On**) or reject (**Off**) this content type in SIP signaling.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

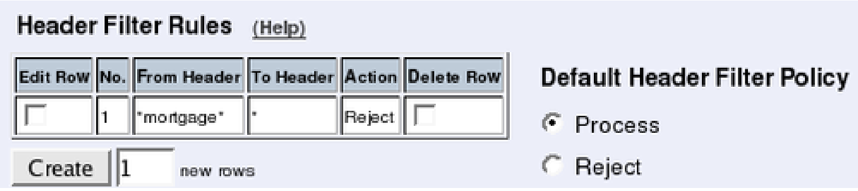
Enter the number of new rows you want to add to the table, and then click on **Create**.

Header Filter Rules

Header Filter Rules lets you filter out SIP requests based on the contents of the To and From headers. This could be useful if you want to prevent groups of users to make calls through the Telecommuting Module.

Wild cards can be used: * for any number (zero or more) characters, ? for exactly one character.

Requests that do not match any rule are handled according to the **Default header filter policy** set beside the table.



Header Filter Rules (Help)

Edit Row	No.	From Header	To Header	Action	Delete Row
□	1	*mortgage*	*	Reject	□

Create 1 new rows

Default Header Filter Policy

● Process

○ Reject

No.

The **No.** field determines the order of the rules. Rules are used in the order in which they are displayed in the table; rule number 1 is first. To change order for a rule, enter the new number in the field and press **Save**.

From Header

Enter an expression which the From header should match. If this rule should match all From headers, enter *.

To Header

Enter an expression which the To header should match. If this rule should match all To headers, enter *.

Action

Select if this rule should make the Telecommuting Module **Process** or **Reject** the matching requests. Rejected requests get a code 403 packet in reply.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Default Header Filter Policy

Select what to do with SIP requests that do not match any of the **Header Filter Rules**. The choices are **Process** and **Reject**. Rejected requests get a code 403 packet in reply.

Save

Saves the Filtering configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Local Registrar

The SIP registrar keeps track of where a user is right now. The registrar receives registrations from the SIP user clients and discards them when they become obsolete. A user can register from several computers.

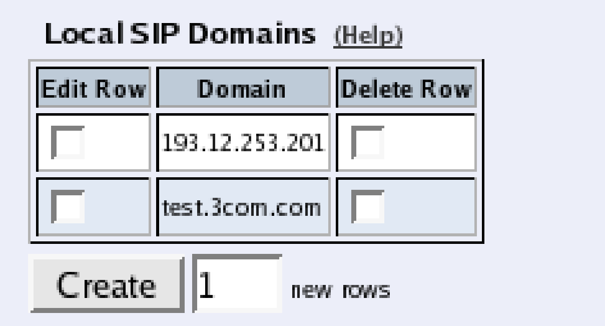
Here, you enter the SIP domains the Telecommuting Module should manage and set up the SIP user database. If authentication should be used, you also need to do some settings on the **Authentication and Accounting** page, and select which SIP methods should be authenticated on the **SIP Methods** page.

If you want to use a RADIUS server for SIP users instead of a local database, you select that on the **Authentication and Accounting** page.

Local SIP Domains

Here, you enter the domains that the SIP registrar should handle. Only users in these domains can register on the Telecommuting Module.

Note that you should only list domains for which the users are expected to register on the Telecommuting Module itself. SIP requests for other domains will be forwarded by the Telecommuting Module to the server managing the domain in question.



Local SIP Domains (Help)

Edit Row	Domain	Delete Row
□	193.12.253.201	□
□	test.3com.com	□

Domain

Enter the name of the domain, such as `3com.com`. Sometimes you have to use an IP address (of the Telecommuting Module) as the domain as well, when the SIP client substitutes the domain for the IP address noted in DNS.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

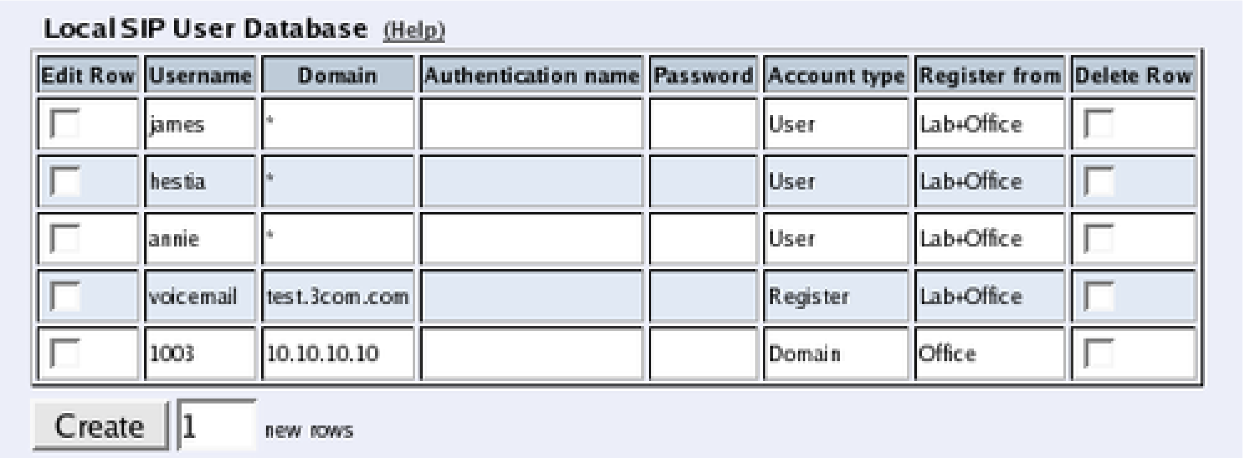
Enter the number of new rows you want to add to the table, and then click on **Create**.

Local SIP User Database

You can restrict which users are allowed to use SIP. Here, you enter the users allowed, select a network from where the SIP traffic is allowed and give the password they should use for authentication.

If the authentication is **Off**, this list should consist of the users allowed to register on the Telecommuting Module. SIP authentication is turned on and off on the **Authentication and Accounting** page.

If you want to use a RADIUS server for SIP users instead of a local database, you select that on the **Authentication and Accounting** page.



Local SIP User Database (Help)

Edit Row	Username	Domain	Authentication name	Password	Account type	Register from	Delete Row
□	james	*			User	Lab+Office	□
□	hestia	*			User	Lab+Office	□
□	annie	*			User	Lab+Office	□
□	voicemail	test.3com.com			Register	Lab+Office	□
□	1003	10.10.10.10			Domain	Office	□

Username

Enter the name of a user allowed to use SIP. Note that only the user name should be entered. Enter "*" to state that all SIP users in this domain should have the same limitations. The user name is used when contacting the user.

If **SIP authentication** is On, every user must be entered on a separate line.

Domain

Enter the domain that the user belongs to. An example of a domain is `3com.com`. Enter "*" to allow all SIP domains.

Authentication Name

If the user should use a different name than its user name for authentication purposes, please enter the authentication name here. It is only used for authentication.

Password

If authentication is required for some methods, press the button to enter the password.

Register From

Here, you can restrict from where this user's SIP traffic can come when he registers. Select a computer/group of computers. The available alternatives are the networks you defined on the **Networks and Computers** page under **Network Configuration**.

This restriction is only for the REGISTER method. Other SIP methods are not checked for originator according to this setting.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Save

Saves the Local Registrar configuration to the preliminary configuration

Cancel

Clears and resets all fields in new rows and resets changes in old rows.

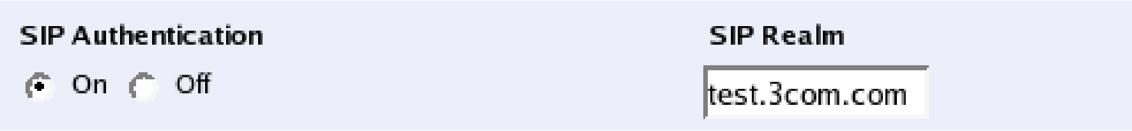
Authentication and Accounting

You can require authentication from SIP users when they perform various SIP functions (register a user, start a call, hang up a call, send a message etc). Here you configure if the Telecommuting Module should require authentication, and which database should be used to authenticate the user.

To require authentication for registration is a good way of ensuring that no one claims to be another user. However, you should not always use authentication; if you do, people from outside can't call you or send messages via SIP without knowing the password.

You also have the possibility to send Account ticks to a RADIUS server, to enable billing of SIP calls.

Authentication settings



SIP Authentication

● On ○ Off

SIP Realm

test.3com.com

SIP Authentication

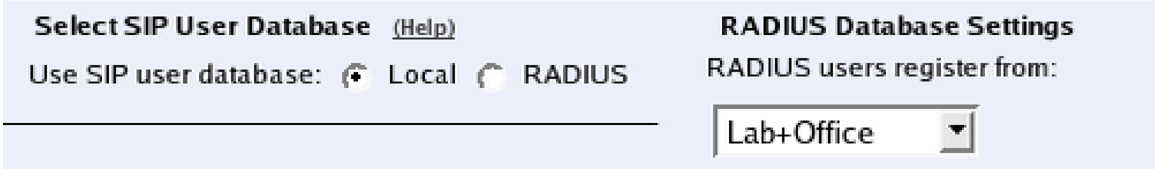
Decide whether SIP authentication should be **On** or **Off**. If **Off**, the Telecommuting Module will not ask clients for authentication for any SIP method, regardless of what settings are made in the **SIP Methods** table.

SIP Realm

When authentication is required for a method, the SIP client will ask for a password. The **Realm** is what the client will present on your screen when asking for a password. If you, for example, use **`sip.3com.com`** as your **Realm**, the client will ask for password with a text which looks like this:

> Enter the password for sip.3com.com

SIP User Database



Select SIP User Database (Help)

Use SIP user database: ● Local ○ RADIUS

RADIUS Database Settings

RADIUS users register from:

Lab+Office

Select SIP User Database

You can either enter SIP users on the **Local Registrar** page to allow them to use SIP, or use an external RADIUS database to which the Telecommuting Module connects to verify users. You can only use a RADIUS database if the SIP authentication is turned on.

Select if the Telecommuting Module should use a local SIP user database (entered on the **Local Registrar** page) or an external RADIUS database.

If a RADIUS database is used, at least one RADIUS server must be entered on the **RADIUS** page under **Basic Configuration**.

Note that when a RADIUS database is used, the RADIUS server has no means of distinguishing different SIP domains, but will authenticate only the username. As a consequence, you can't have users on different domains with the same username.

RADIUS Database Settings

If RADIUS is used for SIP user authentication, all SIP users get the same privileges. Select the network from which they can register. Select from the networks defined on the **Networks and Computers** page under **Network Configuration**.

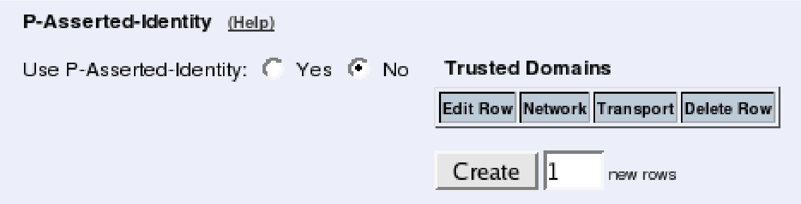
When RADIUS is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

More information about how to configure the RADIUS server to authenticate SIP users can be found in the RADIUS section.

P-Asserted-Identity

When the P-Asserted-Identity header is used, this header is added to all outgoing requests for which the Telecommuting Module has performed authentication. For incoming requests from untrusted domains, where this header is present, the header will be removed before the request is processed.

More information about the P-Asserted-Identity header can be found in RFC 3325.



P-Asserted-Identity (Help)

Use P-Asserted-Identity: ○ Yes ● No

Trusted Domains

Edit Row	Network	Transport	Delete Row

Create 1 new rows

Use P-Asserted-Identity

Select here if the Telecommuting Module should use the P-Asserted-Identity header or not. If it is not used, the **Trusted Domains** setting will have no effect.

Trusted Domains

You can also list the trusted domains for this function. Servers within the trusted domain can add a P-Asserted-Identity header, just as the Telecommuting Module itself can. When such a request is received by the Telecommuting Module, it will not perform authentication itself, but consider the user already authenticated.

Network

Select a network. All IP addresses in this domain will be regarded as trusted servers, which means that if any of them add a P-Asserted-Identity header, the Telecommuting Module will trust it. The available alternatives are the networks you defined on the **Networks and Computers** page under **Network Configuration**.

Transport

Select a transport for the request from a trusted server.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

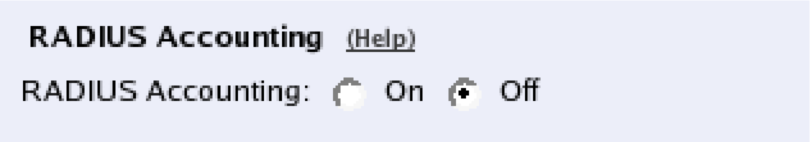
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Use From address in P-Asserted-Identity without authentication

Select if the SIP URI and any display name in the From header of incoming requests is to be added in a P-Asserted-Identity header without authenticating the request.

RADIUS Accounting



RADIUS Accounting (Help)

RADIUS Accounting: ○ On ● Off

RADIUS Accounting can be used to keep track of user calls. This enables billing users for SIP calls.

When RADIUS Accounting is turned on, the Telecommuting Module sends account ticks to notify the configured RADIUS server about when calls start and stop. RADIUS Accounting is defined in RFC 2866.

When RADIUS Accounting is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

Save

Saves the Authentication and Accounting configuration to the preliminary configuration.

Cancel

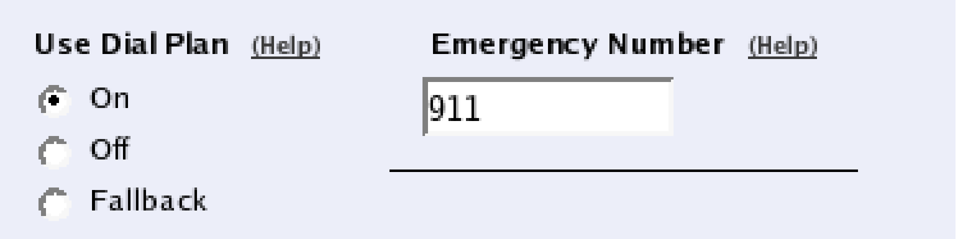
Reverts all of the above fields to their previous configuration.

Dial Plan

The Dial Plan lets you route incoming SIP calls based on the incoming From header and Request-URI.

When neither the Advanced SIP Routing nor the SIP Trunking module has been installed, this page presents only limited functionality.

General



Use Dial Plan (Help)

● On

○ Off

○ Fallback

Emergency Number (Help)

911

Use Dial Plan

The Dial Plan can be turned On, Off or used in Fallback mode. In fallback mode, the Dial Plan is inactive unless a particular SIP server to be routed to is out of order. As a backup, the Dial Plan then becomes active.

Emergency Number

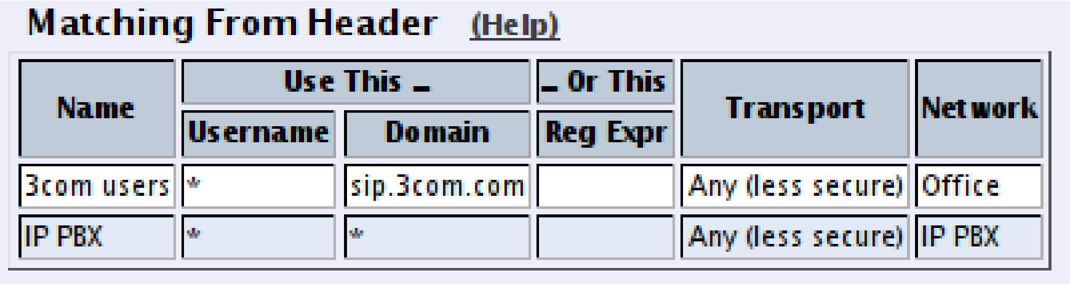
Enter the emergency phone number for your country (like 112 or 911). Calls to this number will be allowed even if all SIP traversal licenses are used up.

Matching From Header

Here you create criterias for the From header of the SIP messages. This is used when matching requests in the **Dial Plan** table. For a request to match, all criterias must be fulfilled.

You can enter a username and domain or create a regular expression (reg exp) to match the From header.

This table is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.



Matching From Header (Help)

Name	Use This –		– Or This	Transport	Network
	Username	Domain	Reg Expr		
3com users	*	sip.3com.com		Any (less secure)	Office
IP PBX	*	*		Any (less secure)	IP PBX

Name

Enter a **Name** for this From header pattern. The name is used in the **Dial Plan** table.

Username

Enter the username that the From header should contain. You can enter "*" to match all usernames.

Domain

Enter the domain that the From header should contain. You can enter "*" to match all domains.

Reg Expr

Instead of entering a username and domain, you can create regular expressions to match the From header.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Read about regular expressions at http://www.regular-expressions.info/. 3Com VCX IP Telecommuting Module supports *Extended Regular Expressions*.

Transport

Select which transport protocol or protocols this should match.

Network

Select from which network the SIP traffic should be sent. Select from the networks created on the **Networks and Computers** page under **Network Configuration**.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

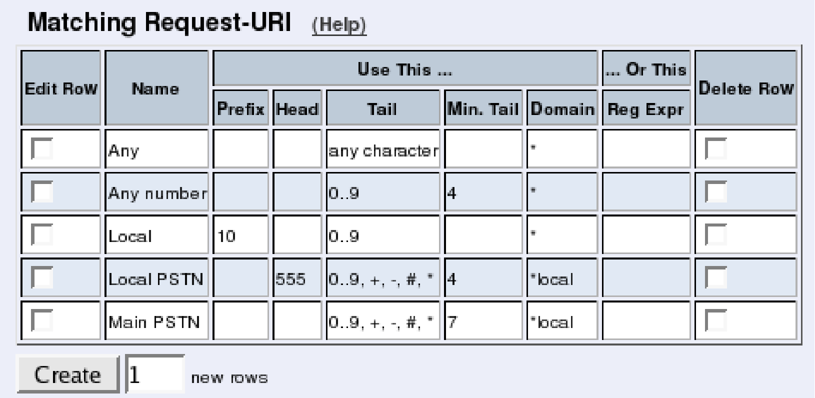
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Matching Request-URI

Here you create criterias for the Request-URI of the SIP messages. This is used when matching requests in the **Dial Plan** table. For a request to match, all criterias must be fulfilled.

You can either enter the username parts and the domain, or create a regular expression to match the Request-URI.



Matching Request-URI (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
□	Any			any character		*		□
□	Any number			0..9	4	*		□
□	Local	10		0..9		*		□
□	Local PSTN		555	0..9, +, -, #, *	4	*local		□
□	Main PSTN			0..9, +, -, #, *	7	*local		□

Create 1 new rows

Name

Enter a **Name** for this Request-URI pattern. The name is used in the **Dial Plan** table.

Prefix

The **Prefix** part of the username is the first part of the username. You enter zero or more characters, where there should be an exact match. The characters entered in this column are stripped before the request is forwarded.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Head

The **Head** part of the username is the first part of the username when the **Prefix** has been stripped. Here, too, there should be an exact match. The characters entered in this column are kept when the request is forwarded.

Tail

The **Tail** part of the username is what is left after the **Prefix** and **Head** parts have been removed. Select here allowed characters in the Tail. The Tail is kept when the request is forwarded.

The "anything" option means that any character and any number of characters are allowed in the Tail. The "nothing" option means that the Tail must not contain any character, which means that the username consists only of the Prefix and Head parts.

If you use a Reg Exp, select "-" as the Tail.

When neither the Advanced SIP Routing or the SIP Trunking module has been installed, this column only offers a limited number of options.

Min. Tail

Enter the minimum number of characters in the **Tail**.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Domain

Enter the domain that the From header should contain. You can enter "*" to match all domains, or "*local" to match all **Local SIP Domains**.

Reg Expr

Instead of entering a username and domain, you can create regular expressions to match the incoming Request-URI.

In this expression, you can also make subexpressions, which can be used in the **Forward To** table. Subexpressions are made by putting the expression inside parantheses. In the expression **(sip:(.+))@3com.com**, which matches any Request-URI like sip:user@3com.com, there are two referable subexpressions: *sip:user* and *user*. You can create up to 9 subexpressions per row.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Read about regular expressions at http://www.regular-expressions.info/. 3Com VCX IP Telecommuting Module supports *Extended Regular Expressions*.

Delete Row

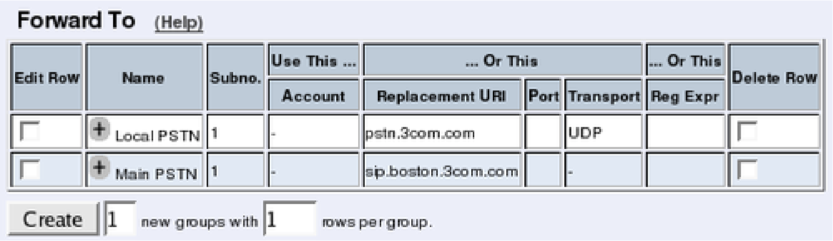
If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Forward To

Here you may enter expressions for the Dial Plan, used to define where and how the Telecommuting Module should forward the request using the Dial Plan. Expressions can be defined either by selecting a non-User-account from the **Local SIP User Database** table, or by defining a replacement URI, port and transport.



Forward To (Help)

Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement URI	Port	Transport	Reg Expr	
□	+ Local PSTN	1	-	pstn.3com.com		UDP		□
□	+ Main PSTN	1	-	sip.boston.3com.com		-		□

Create 1 new groups with 1 rows per group.

Name

This is the name for this destination. The name is used in the **Dial Plan** table.

Subno.

This field is used to sort rows within this destination group. The rows are used in the displayed order.

If the first receiver does not respond, or if the Telecommuting Module receives a 5xx or 6xx response, the request is sent to the receiver on the next row.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Account

Select an account from the **User Routing** table to where the request should be sent.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Replacement URI

Instead of routing the request to a defined user, you can enter a new Request-URI for the request. Enter the new URI here.

With this setting, you can only change the domain part of the Request-URI, not the user part.

Port

Enter the port to where the request should be sent.

Transport

Select which transport should be used to send the request.

Reg Expr

Instead of routing the request to a defined user, or entering a fixed Request-URI, you can create a regular expression which forms a new Request-URI. The regular expression is built from subexpressions from the **Matching Request-URI** table. To use this, regular expressions must be used on the corresponding row in the **Matching Request-URI** table.

Subexpressions are numbered in the order of their starting parenthesis and referred to as *$number*. In the expression **(sip:(.+))@3com.com**, which matches any Request-URI like sip:user@3com.com, there are two referable subexpressions: *sip:user*, which is referred to as *$1*, and *user*, which is referred to as *$2*. You can always refer to the entire Request-URI with *$0*.

By adding the parameter ";b2bua" at the end of the expression, you force the request to the Telecommuting Module back-to-back user agent, which will make it stateful for all requests. This can be useful if you want the Telecommuting Module to send RADIUS accounting tickets for all calls.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

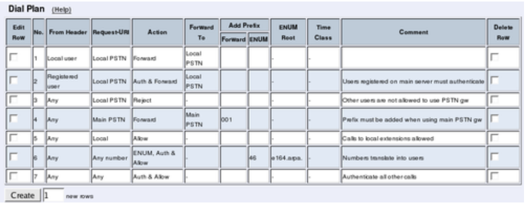
Create

Enter the number of new groups and rows you want to add to the table, and then click on **Create**.

Dial Plan

Here, you create the actual Dial Plan. For each line, select a From entry and Request-URI to match. Then select an Action and, optionally, a Forward to entry to define how the matching requests should be handled by the Telecommuting Module.

You may define lines without a Forward to definition. This is useful if you for example are forwarding by ENUM.



Dial Plan (Help)

Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
□	1	Local user	Local PSTN	Forward	Local PSTN			-	-		□
□	2	Registered user	Local PSTN	Auth & Forward	Local PSTN			-	-	Users registered on main server must authenticate	□
□	3	Any	Local PSTN	Reject	-			-	-	Other users are not allowed to use PSTN gw	□
□	4	Any	Main PSTN	Forward	Main PSTN	001		-	-	Prefix must be added when using main PSTN gw	□
□	5	Any	Local	Allow	-			-	-	Calls to local extensions allowed	□
□	6	Any	Any number	ENUM, Auth & Allow	-		46	e164.arpa.	-	Numbers translate into users	□
□	7	Any	Any	Auth & Allow	-			-	-	Authenticate all other calls	□

No.

This is a number that is used to identify each individual Dial Plan rule. Rules are sorted in numerical order. To move a rule to a certain row, enter the number on the row to which you want to move it. You need only renumber rules that you want to move; other rules are renumbered automatically. When you click on **Save** or add a new row, the rules are re-sorted. The order of the rules is important. *Rules are used in the order in which they are displayed in the table*; rule number 1 is first.

From Header

Select a matching From header pattern, created in the **Matching From Header** table;

Selecting "-" means that no restrictions are made on the From header or sending IP address.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Request-URI

Select a matching Request-URI pattern, created in the **Matching Request-URI** table;

Action

Select actions for this request. The Telecommuting Module can do the following:

Forward: The request is sent to the destination selected under Forward To.

Auth: The Telecommuting Module asks the requestor for authentication.

ENUM: The Telecommuting Module performs an ENUM lookup to get the new destination.

Allow: The Forward To column is ignored and the request is processed according to the Telecommuting Module settings outside the **Dial Plan** table.

Reject: The request is rejected. The Telecommuting Module sends a 403 (Forbidden) response.

A lot of combinations of the above actions are available in the drop-down menu.

When neither the Advanced SIP Routing or the SIP Trunking module has been installed, this column only offers a limited number of options.

Forward To

Select a Forward To pattern, created in the **Forward To** table;

Add Prefix

Sometimes, you might want to add something to a Request-URI when sending the request on to certain servers. Under **Forward**, you can enter a prefix which will be added to the Request-URI when the Forward action is performed. Under **ENUM**, you can enter a prefix which will be added to the Request-URI when the ENUM action is performed.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

ENUM Root

If ENUM should be performed for this request, you must select an ENUM Root. Select from the roots created in the **ENUM Root** table.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Time Class

For each rule you select a **Time class**, which regulate on what days and at what time of a day the rule will be active. Inactive rules are ignored when deciding what should be done with the incoming SIP signaling. You define the different time classes on the **Time Classes** page under **SIP Traffic**.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Comment

Enter a comment to remind yourself what this row is meant to do.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

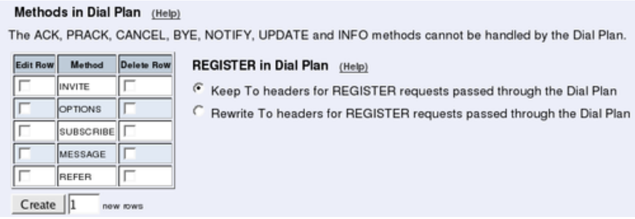
Enter the number of new rows you want to add to the table, and then click on **Create**.

Methods in Dial Plan

In this table, enumerate which SIP methods the **Dial Plan** should handle.

The ACK, PRACK, CANCEL, BYE, NOTIFY, UPDATE and INFO methods can't be handled by the **Dial Plan**. These methods are routed in other ways according to the session they belong to.

This table is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.



Methods in Dial Plan (Help)

The ACK, PRACK, CANCEL, BYE, NOTIFY, UPDATE and INFO methods cannot be handled by the Dial Plan.

Edit Row	Method	Delete Row
□	INVITE	□
□	OPTIONS	□
□	SUBSCRIBE	□
□	MESSAGE	□
□	REFER	□

Create 1 new rows

REGISTER in Dial Plan (Help)

● Keep To headers for REGISTER requests passed through the Dial Plan

○ Rewrite To headers for REGISTER requests passed through the Dial Plan

Method

Enter the method name. Standard SIP methods can be found in RFC 3261.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

REGISTER in Dial Plan

REGISTER requests can be handled by the Dial Plan, but require some special processing.

The REGISTER request is the standard method to connect a SIP username to an IP address. For this, the To header is used to convey the SIP username, and the Request-URI is used to tell the server to which the request should be sent. For this reason, To headers in REGISTER requests forwarded through the Dial Plan may no longer match the server to which they are sent.

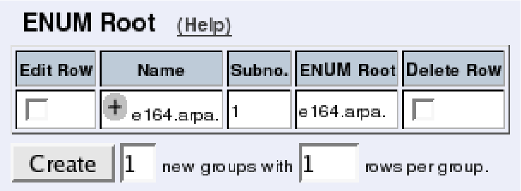
When **Rewrite To headers for REGISTER requests passed through the Dial Plan** is selected, the domain part of the To header is rewritten to match the new Request-URI.

ENUM Root

In this table, ENUM roots can be listed. The ENUM root is something like a DNS top domain.

Normally, only the standard ENUM root e164.arpa. is used, but other roots can be added, e.g. for test purposes. Read more on ENUM in RFC 3824

This table is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.



ENUM Root (Help)

Edit Row	Name	Subno.	ENUM Root	Delete Row
□	⊕ e164.arpa.	1	e164.arpa.	□

Create 1 new groups with 1 rows per group.

Name

Enter a name for this combination of ENUM roots.

Subno.

This field is used to sort rows within this ENUM root group The rows are used in the displayed order; if the first server does not respond, the request is sent to the next one.

ENUM Root

The ENUM root to use.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows** or **Save**.

Create

Enter the number of new groups and rows you want to add to the table, and then click on **Create**.

Save

Saves the Dial Plan configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Routing

Here, you configure routing of the SIP signaling received by the Telecommuting Module. The options are: to forward all SIP requests to a server, regardless of what they concern (**Outbound Proxy**), to forward requests to a specific user to other users as well (**Static**

Registrations), and to forward all requests addressed to a specific SIP domain to a SIP server (**DNS Override For SIP Requests**).

You can also configure how incoming calls for local SIP users should be processed. You can restrict allowed callers and send the calls on to a voice mail server.

You can also select to process class 3xx messages in the Telecommuting Module or pass them on to the client.

When the Advanced SIP Routing module is not installed, this page presents only limited functionality.

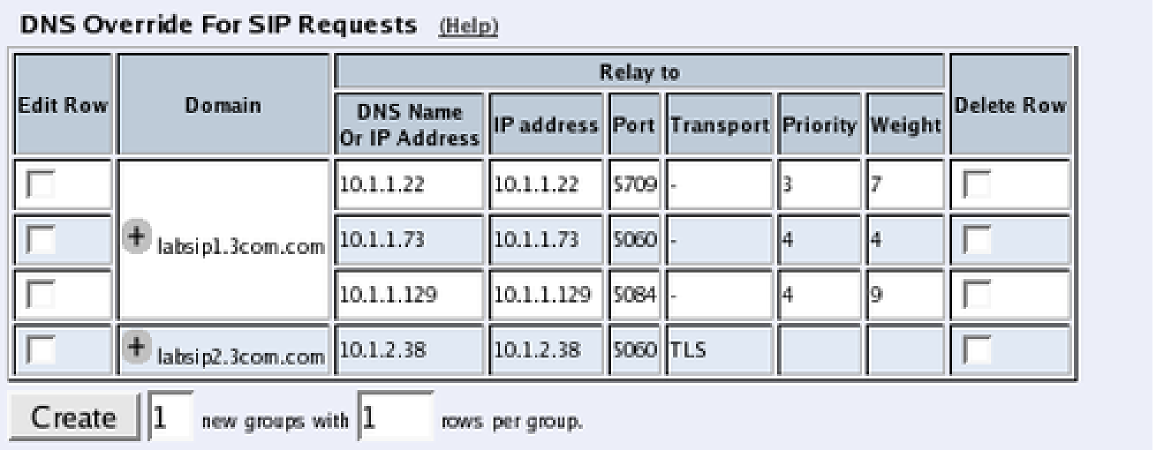
DNS Override For SIP Requests

Here, you can register SIP domains to which the Telecommuting Module should be able to forward requests, but which for some reason cannot be resolved in DNS. Enter an IP address and port to which the requests should be forwarded. You can also select to use a specific protocol.

The Telecommuting Module uses the Request-URI of the incoming SIP packet to match for the domains in this table. When it matches a domain, the packet will be forwarded to the IP address entered here. Note that the Request-URI will not be rewritten!

You can also enter subdomains to **Local SIP Domains**, if you want the subdomain to be handled by a separate SIP proxy. This table has a higher priority than **Local SIP Domains**, which means that if you register a subdomain to a domain registered under **Local SIP Domains**, the Telecommuting Module will forward SIP requests to the subdomain instead of processing them itself.

You can enter more than one IP address or host name for a domain, and set weights and priorities for these.



DNS Override For SIP Requests (Help)

Edit Row	Domain	Relay to						Delete Row
		DNS Name Or IP Address	IP address	Port	Transport	Priority	Weight	
□	+ labsip1.3com.com	10.1.1.22	10.1.1.22	5709	-	3	7	□
□		10.1.1.73	10.1.1.73	5060	-	4	4	□
□		10.1.1.129	10.1.1.129	5084	-	4	9	□
□	+ labsip2.3com.com	10.1.2.38	10.1.2.38	5060	TLS			□

Create 1 new groups with 1 rows per group.

Domain

Enter the domain name of the SIP domain. This domain is compared to the domain in the Request-URI of the incoming SIP packet.

You can't enter a domain that was entered in the **Local SIP Domains** table.

Relay To

DNS Name Or IP Address

Enter the IP address for the SIP server handling the domain. You can also enter a DNS name for the SIP server, if it has a DNS-resolvable host name, even if the SIP domain is not possible to look up in DNS.

IP address

Shows the IP address of the **DNS Name Or IP Address** you entered in the previous field.

Port

Here, enter the port on which the SIP server listens for SIP traffic. The standard port is 5060 (5061 for TLS).

Transport

You can select which transport protocol to use between the Telecommuting Module and the SIP server. Under **Transport**, select from UDP, TCP and TLS.

Priority

If you entered more than one IP address/host name for the same domain, you should also assign them **Priority** and **Weight**. A low **Priority** value means that the unit should have a high priority.

Weight

If more than one unit has the same **Priority**, the signaling sent to them is distributed between them according to their **Weight**. If two units have the same priority, and Unit 1 has weight 4, and Unit 2 has weight 9, 4/13 of the signaling will be sent to Unit 1, and 9/13 will be sent to Unit 2.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

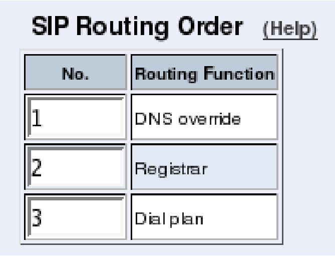
Create

Enter the number of new groups and rows you want to add to the table, and then click on **Create**.

SIP Routing Order

You can configure the order between some SIP routing functions.

For most standard setups this is not needed, but special complicated scenarios may require a change of order.



SIP Routing Order (Help)

No.	Routing Function
1	DNS override
2	Registrar
3	Dial plan

No.

The order of the function. You change order of the functions by giving them new order numbers.

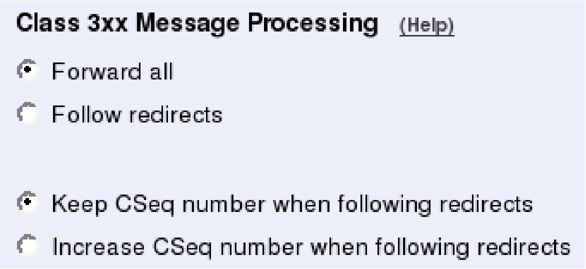
Routing Function

These are the functions to be ordered. **DNS Override** means the **DNS Override For SIP Requests** table. **Local Registrar** means all locally registered users (but not registration requests) and the **Static Registrations** table. **Dial Plan** means the **Dial Plan** table.

Class 3xx Message Processing

Sometimes during negotiation for a connection, status messages about this process will be sent. Here you select whether to forward these to the client or process them in the Telecommuting Module.

A class 3xx message from a server means that the connection attempt was terminated, but no connection was established, e.g. due to use of the wrong address or service. The Telecommuting Module as well as some clients can use this information to make new attempts which might have a better chance to succeed.



Class 3xx Message Processing (Help)

● Forward all

○ Follow redirects

● Keep CSeq number when following redirects

○ Increase CSeq number when following redirects

The choices are **Forward all**, which forwards all class 3xx messages to the client (which might be able to use this information), and **Follow redirects**, which means that the Telecommuting Module itself uses the information and might make new connection attempts. In this case, it will only inform the client when the connection finally is established or the attempt has failed totally.

Normally, the *CSeq* number of the request is kept when SIP devices follows redirects. In some situations, other SIP equipment might require the CSeq number to increase when the Telecommuting Module follows redirects. Select here if it should do so.

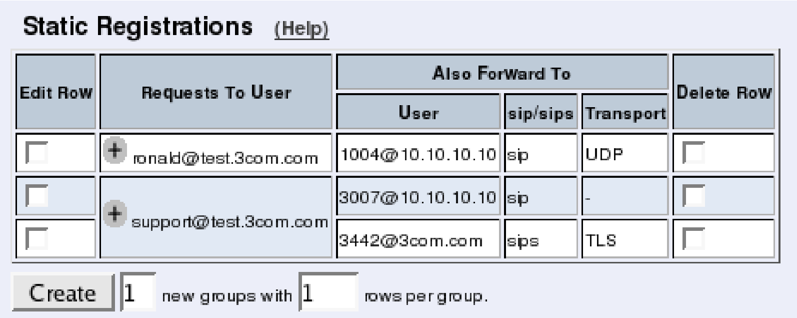
Static Registrations

You can specify that calls to a certain user address should also be redirected to another address, or that calls to a non-person user name (like support@company.com) should be redirected to one or more other addresses.

Static registrations only affect SIP requests addressed to **Local SIP Domains**.

Even if a call should be forwarded, the Telecommuting Module will try to put it through to the original addressee.

Note that this table should *not* be used for your own XF or XF/Register accounts. Use the **User Routing** table to forward calls for these accounts instead.



Static Registrations (Help)

Edit Row	Requests To User	Also Forward To			Delete Row
		User	sip/sips	Transport	
□	⊕ ronald@test.3com.com	1004@10.10.10.10	sip	UDP	□
□	⊕ support@test.3com.com	3007@10.10.10.10	sip	-	□
□		3442@3com.com	sips	TLS	□

Create 1 new groups with 1 rows per group.

Requests To User

Enter the user address. Calls to this user are sent to the user, but also forwarded to users listed under **Also forward to**. The address should be entered on the form *user@domain*.

Also Forward To

User

Enter the address to which the calls should be forwarded. The address should be entered on the form *user@domain*. You can forward to more than one address by creating several rows for the same **Request to user** name.

You can add parameters to the destination address to limit what is sent to that user. Parameters are added after the address, separated by semicolon. The following parameters exist:

methods=: Enumerate the SIP methods that should be sent on to this user. If this parameter is not used, all requests are forwarded regardless of which method is used.

audio: Audio calls are forwarded to the user. Audio calls are defined as requests with an SDP where a "m=audio" line is present.

video: Video calls are forwarded to the user. Video calls are defined as requests with an SDP where a "m=video" line is present.

+sip.message: Requests are forwarded to the user if the body contains a line with "m=message" in it.

Example: If audio calls should be forwarded to *adam@sip.ingate.com*, enter *adam@sip.ingate.com;audio*. If only the NOTIFY and SUBSCRIBE methods should be forwarded to *emmie@sip.ingate.com*, enter *emmie@sip.ingate.com;methods=NOTIFY,SUBSCRIBE*.

sip/sips

Select if the request to this address should be sent by SIP or SIPS (SIP Secure). With SIPS, you require that the request is sent over TLS all the way to the addressee.

Transport

Select the protocol to use when sending the request.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

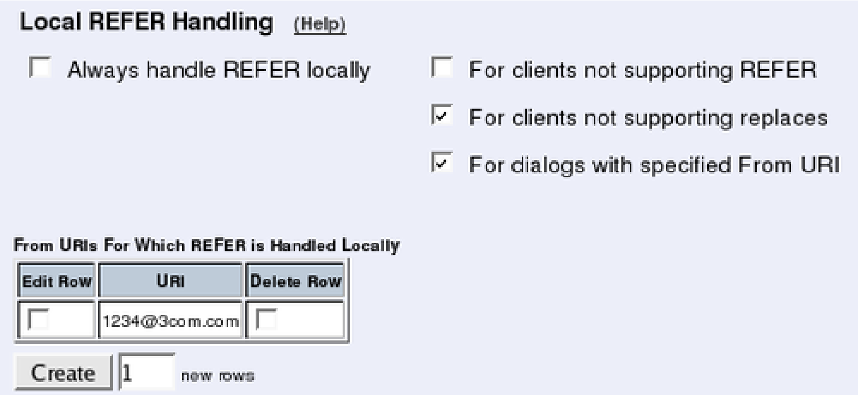
Create

Enter the number of new groups and rows you want to add to the table, and then click on **Create**.

Local REFER Handling

Some SIP clients and servers are unable to handle the REFER method, which is used when transferring calls between users. You can make the Telecommuting Module handle the REFERs locally instead of forwarding them to the inept client.

Check boxes for the REFER requests that the Telecommuting Module should handle locally. If no boxes are checked, all REFER requests are forwarded to the destination indicated in the request.



Local REFER Handling (Help)

□ Always handle REFER locally

□ For clients not supporting REFER

☑ For clients not supporting replaces

☑ For dialogs with specified From URI

From URIs For Which REFER is Handled Locally

Edit Row	URI	Delete Row
□	1234@3com.com	□

Create 1 new rows

Always handle REFER locally

With this option, all REFER requests through the Telecommuting Module will be intercepted and handled by the Telecommuting Module instead of the intended destination.

For clients not supporting REFER

When SIP clients start a dialog, they provide a list of supported SIP methods. With this option, the Telecommuting Module will intercept REFER requests bound to client that did not list REFER as a supported method.

For clients not supporting replaces

When SIP clients start a dialog, they provide a list of supported SIP methods and parameters. With this option, the Telecommuting Module will intercept REFER requests bound to client that did not list "replaces" as a supported parameter.

For dialogs with specified From URI

With this option, all REFER requests with a From header matching a URI listed in the **From URIs For Which REFER is Handled Locally** table will be handled locally by the Telecommuting Module.

For dialogs with specified User-Agent header

Some clients or servers may have a limited or erroneous handling of REFER requests. With this option, all REFER requests bound to a client with a User-Agent header matching one listed in the **User-Agent headers for which REFER is handled locally** table will be handled locally by the Telecommuting Module.

From URIs For Which REFER is Handled Locally

Here, URIs are listed that should match From headers for which the Telecommuting Module should handle REFER requests locally.

If the **For dialogs with specified From URI** check box is not checked, this table will be ignored.

URI

Enter the SIP URI here. The "*" wildcard can be used for the entire or part of the URI, like **@ingate.com*.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

User-Agent headers for which REFER is handled locally

Here, User-Agent names are listed for which the Telecommuting Module should handle REFER requests locally.

If the **For dialogs with specified User-Agent header** check box is not checked, this table will be ignored.

User-Agent

Enter the User-Agent name here. The "*" wildcard can be used for the entire or part of the name, like *snom**.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

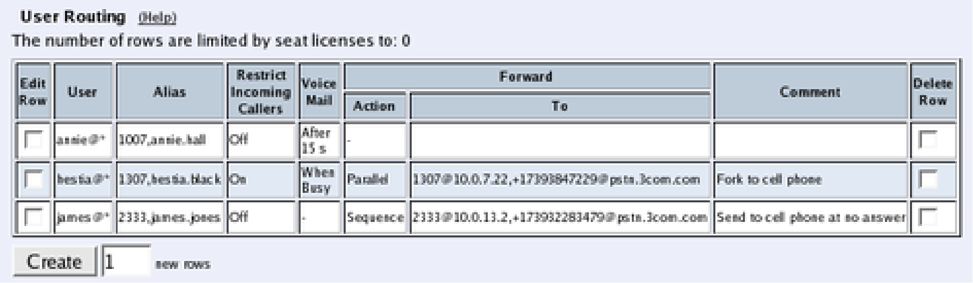
Enter the number of new rows you want to add to the table, and then click on **Create**.

User Routing

This table makes it possible to allow advanced routing options to be enabled per user. You may enter aliases that are used to match incoming request to a specific user. Additionally you may define that the request should be forwarded to other users, and also set up connections to voice mail.

This table is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

When the Advanced SIP Routing module has not been installed, this table only offers a limited number of options.



User Routing (Help)

The number of rows are limited by seat licenses to: 0

Edit Row	User	Alias	Restrict Incoming Callers	Voice Mail	Forward		Comment	Delete Row
					Action	To		
□	annie@*	1007,annie.hall	Off	After 15 s	-			□
□	hestia@*	1307,hestia.black	On	When Busy	Parallel	1307@10.0.7.22,+17393847229@pstn.3com.com	Fork to cell phone	□
□	james@*	2333,james.jones	Off	-	Sequence	2333@10.0.13.2,+173932283479@pstn.3com.com	Send to cell phone at no answer	□

User

Select a user here from the users defined in the **Local SIP User Database** table.

When you have selected to use a RADIUS database for authentication purposes, there will be a special option here called "*local domain users". This selection goes for all users on the domain, even when they are not registered. This means that all usernames, even those not configured in the RADIUS database, will be included in this selection, as the Telecommuting Module has no access to the entire user list.

Alias

Enter aliases for the user, such as short extensions or optional SIP call names.

Restrict Incoming Callers

You can select to restrict which external users are allowed to make calls. If you turn Restrict Incoming Callers **On**, only locally defined users (in the **Local SIP User Database** table) and users in the **Allow Calls From Unauthenticated Users** table are allowed to call this user.

Forward

You can send the request to other users. Select here how and whom it should be sent.

Action

One of the following actions can be selected:

Reject: The call is rejected. Nothing is forwarded.

Forward: The call will only be forwarded to the users under **To**; if there are any registrations for the user selected under **User**, they will not receive the call.

Parallel: The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. Requests for all these users are sent in parallel.

Sequence: The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. First, the request is sent to all local registrations. If there is no final response after 25 seconds, the request is sent on to the first user in the To list. After another 25 seconds, the request is sent to the second user in the To list.

Random: The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. First, the request is sent to a randomly chosen user in the list. If there is no final response after 25 seconds, the request is sent on to another user in the list.

This can be useful for support centres.

To

Enter a comma-separated list of the users to forward the request to.

Send To Voice Mail

Select when to send the SIP request on to a Voice Mail server.

Time Class

For each rule you select a **Time class**, which regulate on what days and at what time of a day the rule will be active. Inactive rules are ignored when deciding what should be done with the incoming SIP signaling. You define the different time classes on the **Time Classes** page under **SIP Traffic**.

This column is only available when the Advanced SIP Routing module has been installed.

Comment

Enter a comment to remind yourself what this row is meant to do.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

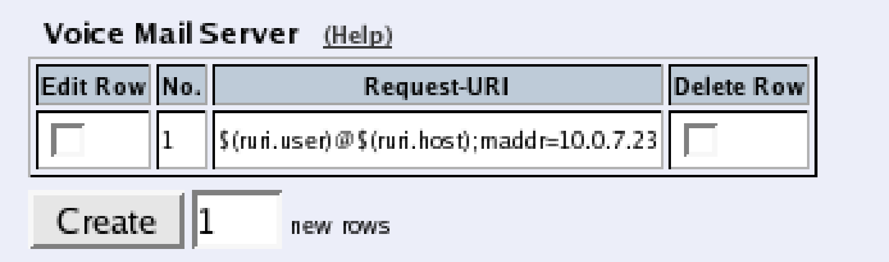
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

Voice Mail Server

Here you configure which voice mail server to use for the users in the **User Routing** table. You can also enter the Request-URI to use when connecting to the voice mail server. The Request-URI must start with a sip: or sips:, and can contain references to various usernames and domains.

This table is only available when the Advanced SIP Routing module has been installed.



Voice Mail Server (Help)

Edit Row	No.	Request-URI	Delete Row
□	1	$(ruri.user)@$(ruri.host);maddr=10.0.7.23	□

No.

The Voice Mail servers are used in the order they are presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other servers are renumbered automatically. When you click on **Save**, the servers are re-sorted.

Request-URI

Enter a fixed Request-URI or one containing references to the current call. The following references are available:

cfg.user: The username from the current line in the **User Routing** table.

cfg.host: The domain from the current line in the **User Routing** table.

ruri.user: The username in the incoming Request-URI.

ruri.host: The domain in the incoming Request-URI.

to.user: The username in the incoming To header.

to.host: The domain in the incoming To header.

from.user: The username in the incoming From header.

from.host: The domain in the incoming From header.

When you want to reference one of the above entities, you put them in $().

If you want to use the username from the current line in the **User Routing** table, and send it to this user at vmserver.com, it should look like this: **sip:$(cfg.user)@vmserver.com**.

If you want to user the username and domain from the incoming Request-URI and just send the request on to vmserver.com, it should look like this: **sip:$(ruri.user)@$(ruri.host);maddr=vmserver.com**.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

Create

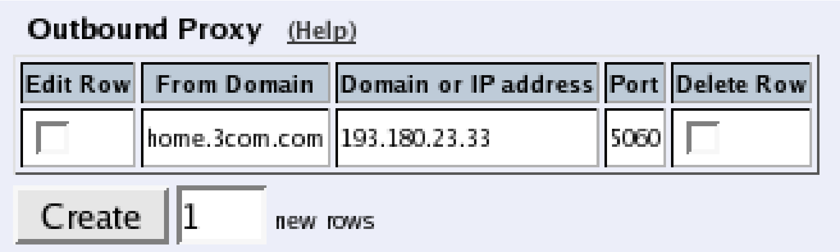
Enter the number of new rows you want to add to the table, and then click on **Create**.

Outbound Proxy

Here, you can enter one or more external SIP proxies to which all or part of the SIP requests should be sent. This could be useful e.g. if the Telecommuting Module separates two local departments of a company, and all SIP requests should be processed by the main firewall connected to the Internet.

This setting should only be used when the Telecommuting Module should not try to re-route requests, as it will only be able to send to the outbound proxy entered here.

You can direct requests to different SIP proxies based on the sender and receiver domain of the request.



Edit Row	From Domain	Domain or IP address	Port	Delete Row
□	home.3com.com	193.180.23.33	5060	□

Create: 1 new rows

From Domain

Enter a SIP domain here. When an incoming SIP request originates from a user in this domain (the domain is in the From field), the Telecommuting Module will send it on to the SIP proxy entered on this row.

You can send all requests to the same external SIP proxy. Enter "*" here to match all SIP domains.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Request-URI Domain

Enter a SIP domain here. When an incoming SIP request is bound to a user in this domain (the domain is in the Request-URI), the Telecommuting Module will send it on to the SIP proxy entered on this row.

You can send all requests to the same external SIP proxy. Enter "*" here to match all SIP domains.

This column is only available when the Advanced SIP Routing or the SIP Trunking module has been installed.

Domain or IP Address

Enter the domain name or IP address of the external SIP proxy.

Port

Enter the port number of the external SIP proxy.

If no port number is entered, the Telecommuting Module will make a DNS query for an SRV record. If a port number is entered, it will query for an A record.

Gateway

Enter the gateway for the external SIP proxy.

You can select which default gateway should be used for requests sent to this SIP proxy. If you select "-", the requests will be sent to the SIP Default Gateway.

Delete Row

If you select this box, the row is deleted when you click on **Create new rows**, **Save**, or **Look up all IP addresses again**.

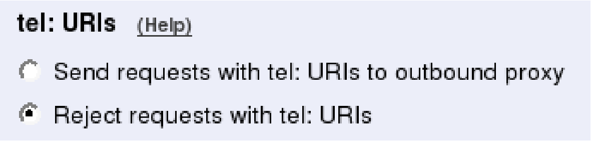
Create

Enter the number of new rows you want to add to the table, and then click on **Create**.

tel: URIs

tel: URIs is a different URI scheme than the *user@domain* scheme, where the URIs contain only the phone number itself, and the SIP server is expected to know what to do with them.

The Telecommuting Module has no built-in support for tel: URIs itself, but if your outbound proxy can resolve them, you can have the Telecommuting Module send them there.



tel: URIs (Help)

○ Send requests with tel: URIs to outbound proxy

● Reject requests with tel: URIs

You can select to **Send requests with tel: URIs to outbound proxy**. If you entered a SIP server to receive requests from all domains in the **Outbound Proxy** table, this is also where all tel: URI requests will be sent. You must ensure that this SIP server will know how to handle these requests.

If you have no access to a SIP server which handles tel: URIs, you can instead select to **Reject requests with tel: URIs**. In this case, when the Telecommuting Module receives a request with a tel: URI, it will respond with the code 416.

Save

Saves the Routing configuration to the preliminary configuration.

Cancel

Reverts all of the above fields to their previous configuration.

Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

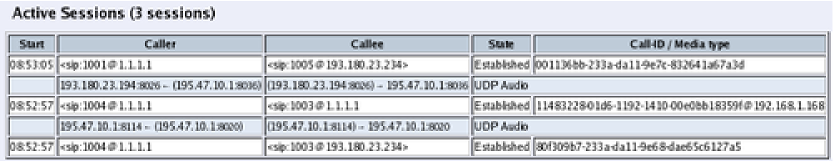
This button will only be visible if a DNS server has been configured.

Registrar and Session Status

You can monitor the current SIP activity. The tables are updated when you select the page or reload it.

Active Sessions

Here the currently active sessions are listed.



Active Sessions (3 sessions)

Start	Caller	Callee	State	Call-ID / Media type
08:53:05	<sip:1001@1.1.1.1	<sip:1005@193.180.23.234>	Established	001136bb-233a-da11-9e7c-832641a67a3d
	193.180.23.194:8026 – (195.47.10.1:8036)	(193.180.23.194:8026) – 195.47.10.1:8036	UDP Audio	
08:52:57	<sip:1004@1.1.1.1	<sip:1003@1.1.1.1	Established	11483228-01d6-1192-1410-00e0bb18359f@192.168.1.168
	195.47.10.1:8114 – (195.47.10.1:8020)	(195.47.10.1:8114) – 195.47.10.1:8020	UDP Audio	
08:52:57	<sip:1004@1.1.1.1	<sip:1003@193.180.23.234>	Established	80f309b7-233a-da11-9e68-dae65c6127a5

Start

The time when the call started.

Caller

The SIP and IP addresses of the calling user.

Callee

The SIP and IP addresses of the called user.

State

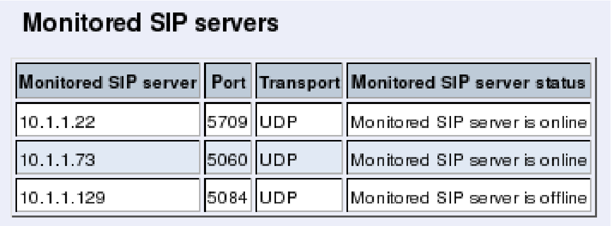
Shows if the call is established or under negotiation.

Call ID/Media Type

Each SIP session has a unique ID, which is shown here. You can also see what media type is used in the call.

Monitored SIP Servers

Here, status is shown for all domains monitored according to the **SIP Servers To Monitor** table.



Monitored SIP servers

Monitored SIP server	Port	Transport	Monitored SIP server status
10.1.1.22	5709	UDP	Monitored SIP server is online
10.1.1.73	5060	UDP	Monitored SIP server is online
10.1.1.129	5084	UDP	Monitored SIP server is offline

Monitored SIP server

The name of the SIP server being monitored by the Telecommuting Module.

Port

The port of the SIP server being monitored by the Telecommuting Module.

Transport

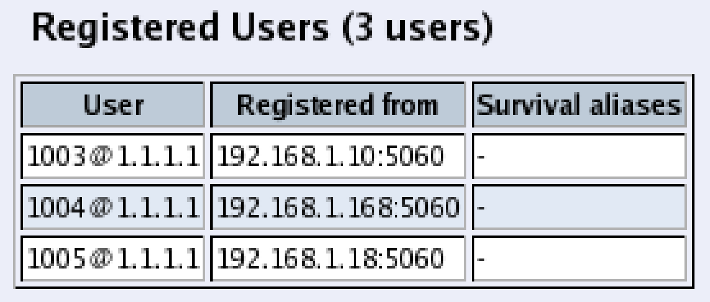
The transport being monitored by the Telecommuting Module for this SIP server.

Monitored SIP server status

The status for the monitored SIP server. **Monitored SIP server is online** means that the Telecommuting Module can contact the SIP server. **Monitored SIP server is offline** means that the Telecommuting Module can't contact the SIP server.

Registered Users

Here the currently registered users are listed.



Registered Users (3 users)

User	Registered from	Survival aliases
1003@1.1.1.1	192.168.1.10:5060	-
1004@1.1.1.1	192.168.1.168:5060	-
1005@1.1.1.1	192.168.1.18:5060	-

User

The SIP address of the registered user. The address looks like *name@domain*, where *name* is a user name or a telephone number, and *domain* is a domain name or the IP address of the SIP registrar (the Telecommuting Module).

Registered from

The IP address of the computer from which the user registered.

Survival aliases

If the VoIP Survival module is installed, aliases for this user is shown here. The aliases shown are the ones configured for the user on the main server.

Chapter 12. Tools

Under **Tools**, you find handy tools to troubleshoot the Telecommuting Module setup.

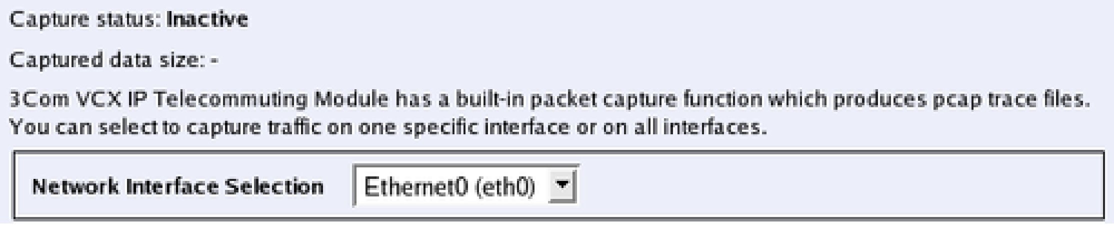
Packet Capture

3Com VCX IP Telecommuting Module has a built-in packet capturer which can produce pcap trace files. This sniffer will capture all IP packets according to your selections, even those you can't see in the log (like RTP packets).

The Telecommuting Module capturer needs to be manually activated and deactivated. As this produces a log which usually contains a lot more packets than the standard log, it is advisable only to run the capturer for short time periods.

The capture of the packets can be downloaded and analyzed in any tool that handles pcap traces, like Ethereal/Wireshark.

Network Interface Selection



Capture status: **Inactive**

Captured data size: -

3Com VCX IP Telecommuting Module has a built-in packet capture function which produces pcap trace files. You can select to capture traffic on one specific interface or on all interfaces.

Network Interface Selection: Ethernet0 (eth0)

Select on which interface or VLAN the sniffer should listen for packets. You can also select to listen on all interfaces.

Some network cards have VLAN hardware support. For this type of cards, incoming VLAN tagged traffic is not logged on the main interface, but only on the VLAN interface. Outgoing VLAN tagged traffic is logged on the main interface.

Other interfaces do not have VLAN hardware support. For this type of interface, VLAN traffic is logged on the main interface.

Currently, the only network cards in 3Com products to support VLAN are the Gigabit network cards.

IP Address Selection

You can limit the selection by specifying certain IP addresses.

In these fields, enter a single IP address (e. g., 10.3.27.3), a range of IP addresses (e. g., 10.3.27.1-10.3.28.254), an IP address followed by a netmask (e. g.,10.3.27.0/24), a combination of these, or nothing at all. If a field is empty, all IP addresses are selected.

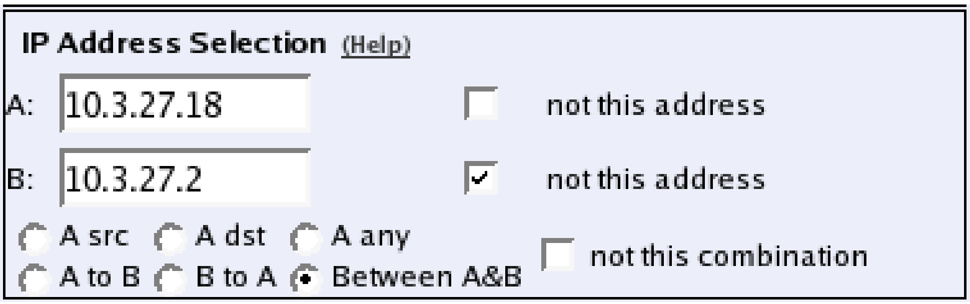
If you want to study all traffic except the one to or from a specific computer or group of computers, enter the IP address(es) here and mark the "not this address" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the IP address in field A matches. Field B is ignored.
A dst	Packets to the IP address in field A matches. Field B is ignored.

A any	Packets to or from the IP address in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to study all packets to or from 10.3.27.18, except those to the file server 10.3.27.2, you should fill in the form like this:



IP Address Selection (Help)

A: 10.3.27.18 □ not this address

B: 10.3.27.2 ☑ not this address

○ A src ○ A dst ○ A any

○ A to B ○ B to A ● Between A&B

□ not this combination

Protocol/Port Selection

You can limit the selection by specifying certain protocols.

All IP protocols

No restriction regarding protocols.

TCP/UDP

When selecting TCP or UDP, you can choose all packets or packets to certain ports only.

In these fields, you can enter a single port number (32), a range of port numbers (1-1023), a list of port numbers and ranges separated by commas (53, 1024-65535) or nothing at all. If the field is empty, any port will match. See appendix G, Lists of ports, ICMP and protocols, for more information on port numbers.

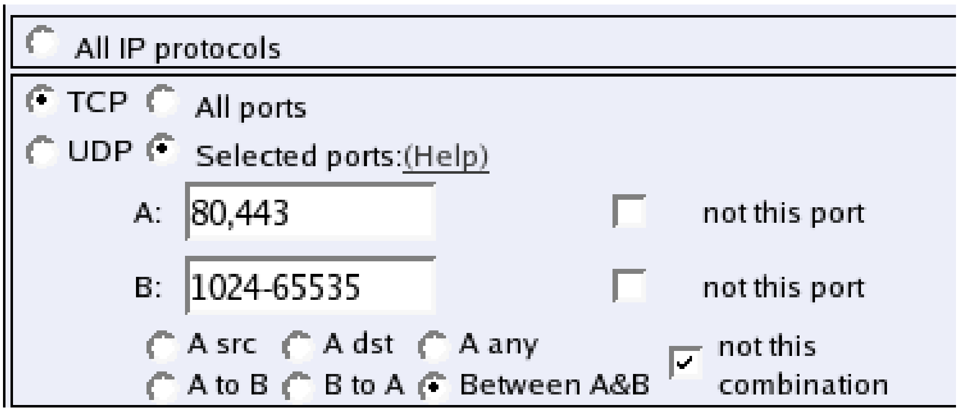
If you want to study all traffic except the one to or from a specific port or group of ports, enter the port number(s) here and mark the "not this port" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the port number in field A matches. Field B is ignored.
A dst	Packets to the port number in field A matches. Field B is ignored.
A any	Packets to or from the port number in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.

not this combination — Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to search for all packets to a web server, but not packets on the "normal" client and server ports in your environment, fill in the form like this:



○ All IP protocols

● TCP ○ All ports

○ UDP ● Selected ports:(Help)

A: 80,443 □ not this port

B: 1024-65535 □ not this port

○ A src ○ A dst ○ A any ☑ not this combination

○ A to B ○ B to A ● Between A&B

ICMP

ICMP packets contain a type field and a code field. When searching for ICMP packets, you can select all packets or only those matching certain criteria.

In the type and code fields, you can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e. g., 5, 10-20) or nothing at all. If the field is empty, any type or code will match. See appendix G, Lists of ports, ICMP and protocols, for more information on ICMP types and codes.

If you want to study all traffic except the one of a certain type/code, enter the type/code number(s) here and mark the "not" box.

ESP

ESP is an authentication/encryption protocol. Select this if you want to search for encrypted packets.

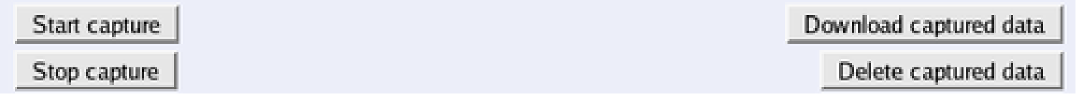
Note that you must have selected a log class which saves to local file, for encrypted packets, to be able to display them here.

Protocol number

Here, you enter the number(s) of the protocols you want to search for. You can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e. g., 5, 10-20) or nothing at all. If the field is empty, any protocol will match. See appendix C, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols, for more information on protocol numbers.

If you want to study all traffic except the one over a certain protocol or protocols, enter the protocol number(s) here and mark the "not" box.

Collect data



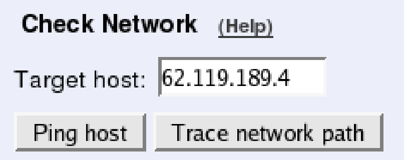
Below the selection boxes, you activate and deactivate the capture function by pressing the **Start capture** and **Stop capture** buttons.

When the capturer has been stopped, the captured log can be downloaded by pressing the **Download captured data** button. The captured data can be deleted by pressing the **Delete captured data** button.

Check Network

You can perform ping and trace a network path from the Telecommuting Module to another IP address to check that the network connection is working.

Check Network



Target host: 62.119.189.4

Target host

Enter the IP address of the computer for which you want to check the network connectivity.

Ping host

When you press this button, the Telecommuting Module will send ten ping packets to the target host and register the replies from that host.

Note that the target host must be configured to respond to ping packets for this test to succeed. Most common computers do that by default, but 3Com VCX IP Telecommuting Modules do not respond to ping request unless they have been configured to do so.

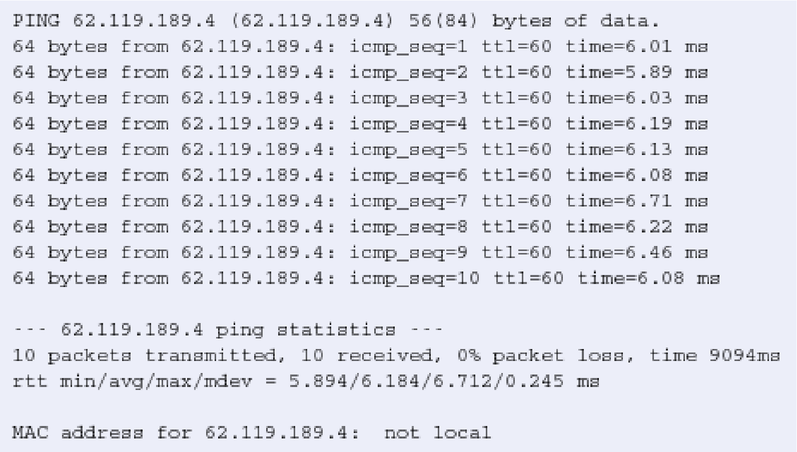
Trace network path

When you press this button, the Telecommuting Module will send packets to the target host and register which path is used by those packets.

For this test to succeed, there must not be more than 30 network elements between the Telecommuting Module and the target host.

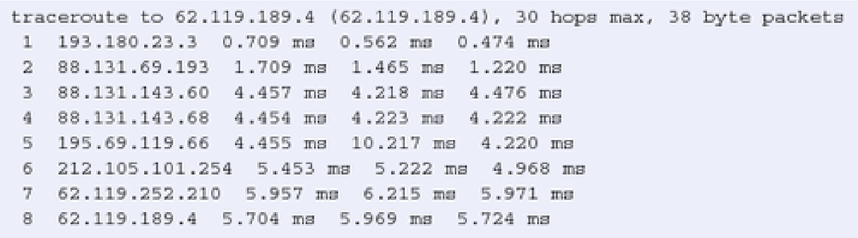
Test Results

Below the buttons, the result of the latest test run is shown. A ping test will result in the ten sent packets and their response times.



```
PING 62.119.189.4 (62.119.189.4) 56(84) bytes of data.
64 bytes from 62.119.189.4: icmp_seq=1 ttl=60 time=6.01 ms
64 bytes from 62.119.189.4: icmp_seq=2 ttl=60 time=5.89 ms
64 bytes from 62.119.189.4: icmp_seq=3 ttl=60 time=6.03 ms
64 bytes from 62.119.189.4: icmp_seq=4 ttl=60 time=6.19 ms
64 bytes from 62.119.189.4: icmp_seq=5 ttl=60 time=6.13 ms
64 bytes from 62.119.189.4: icmp_seq=6 ttl=60 time=6.08 ms
64 bytes from 62.119.189.4: icmp_seq=7 ttl=60 time=6.71 ms
64 bytes from 62.119.189.4: icmp_seq=8 ttl=60 time=6.22 ms
64 bytes from 62.119.189.4: icmp_seq=9 ttl=60 time=6.46 ms
64 bytes from 62.119.189.4: icmp_seq=10 ttl=60 time=6.08 ms

--- 62.119.189.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9094ms
rtt min/avg/max/mdev = 5.894/6.184/6.712/0.245 ms

MAC address for 62.119.189.4:  not local
```

A trace test will result in a list of all network elements the packets use to get to the target host.



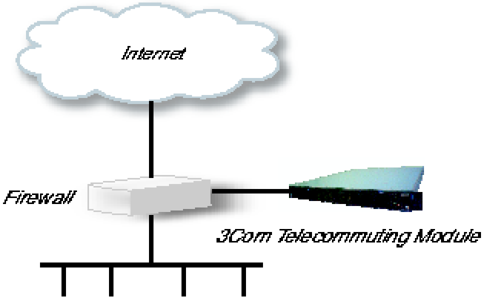
```
traceroute to 62.119.189.4 (62.119.189.4), 30 hops max, 38 byte packets
 1  193.180.23.3  0.709 ms  0.562 ms  0.474 ms
 2  88.131.69.193  1.709 ms  1.465 ms  1.220 ms
 3  88.131.143.60  4.457 ms  4.218 ms  4.476 ms
 4  88.131.143.68  4.454 ms  4.223 ms  4.222 ms
 5  195.69.119.66  4.455 ms  10.217 ms  4.220 ms
 6  212.105.101.254  5.453 ms  5.222 ms  4.968 ms
 7  62.119.252.210  5.957 ms  6.215 ms  5.971 ms
 8  62.119.189.4  5.704 ms  5.969 ms  5.724 ms
```

Chapter 13. Firewall and Client Configuration

Additional configuration for the firewall and the SIP clients is required to make the Telecommuting Module work properly. The amount and nature of the configuration depends on which **Telecommuting Module Type** was selected.

The DMZ type

Using the DMZ type, the network configuration should look like this:



The Firewall

The firewall to which the Telecommuting Module is connected should have the following configuration:

SIP over UDP

- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the Telecommuting Module (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the Telecommuting Module (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the Telecommuting Module to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the Telecommuting Module, you don't have to do this step.
- NAT between the Telecommuting Module and the Internet must not be used.
- NAT between the Telecommuting Module and the internal networks must not be used.

SIP over TCP/TLS

- Let through TCP traffic between the Internet (all high ports) and the Telecommuting Module (ports 1024-32767). You must allow traffic in both directions.
- Let through TCP traffic between the internal networks (all high ports) and the Telecommuting Module (ports 1024-32767). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the Telecommuting Module (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the Telecommuting Module to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the Telecommuting Module, you don't have to do this step.
- NAT between the Telecommuting Module and the Internet must not be used.
- NAT between the Telecommuting Module and the internal networks must not be used.

The SIP clients

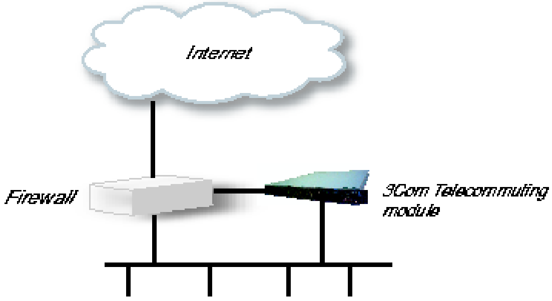
SIP clients will use the Telecommuting Module as their outgoing SIP proxy and as their registrar (if they can't be configured with the domain only). If you don't want to use the Telecommuting Module as the registrar, you should point the clients to the SIP registrar you want to use.

Other

The DNS server used must have a record for the SIP domain, which states that the Telecommuting Module handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

The DMZ/LAN type

Using the DMZ/LAN type, the network configuration should look like this:



The Firewall

The firewall to which the Telecommuting Module is connected should have the following configuration:

SIP over UDP

- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the Telecommuting Module (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the Telecommuting Module to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the Telecommuting Module, you don't have to do this step.
- NAT between the Telecommuting Module and the Internet must not be used.

SIP over TCP/TLS

- Let through TCP traffic between the Internet (all high ports) and the Telecommuting Module (ports 1024-32767). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the Telecommuting Module (the port interval for media streams which was set on the **Basic Settings** page). You must allow traffic in both directions.
- Let through UDP traffic between the Telecommuting Module (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the Telecommuting Module to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the Telecommuting Module, you don't have to do this step.
- NAT between the Telecommuting Module and the Internet must not be used.

SIP clients

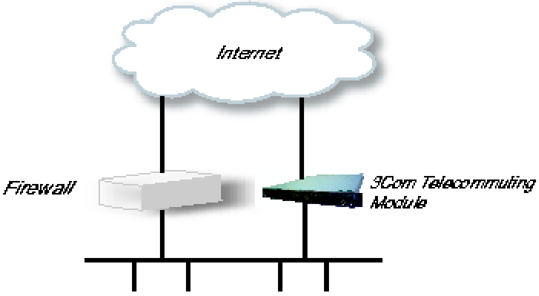
The SIP clients on the internal network should have the Telecommuting Module's IP address on that network as their outgoing SIP proxy and registrar.

Other

The DNS server used must have a record for the SIP domain, which states that the Telecommuting Module handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

The Standalone type

Using the Standalone type, the network configuration should look like this:



The SIP clients

SIP clients will use the Telecommuting Module as their outgoing SIP proxy and as their registrar (if they can't be configured with the domain only). If you don't want to use the Telecommuting Module as the registrar, you should point the clients to the SIP registrar you want to use.

Other

The DNS server used must have a record for the SIP domain, which states that the Telecommuting Module handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

Part IV. 3Com VCX IP Telecommuting Module Serial Console

This part contains complete descriptions of settings in the 3Com VCX IP Telecommuting Module terminal interface.

Chapter 14. Basic Administration

Some settings are available without having to log on the web interface, but instead connecting to the Telecommuting Module console via the serial cable. Here, the settings available from the console are listed.

The serial console is a text user interface which requires a terminal software on your workstation, such as Hyperterm in Windows.

Connecting to the serial console

Connect the Telecommuting Module to your workstation with the enclosed serial cable, plug in the power cord and turn the Telecommuting Module on. You will have to wait a few minutes while it boots up.

If you use a Windows workstation, connect like this: Start *Hyperterm*. A Location dialogue will show, asking for your telephone number and area. Click Cancel followed by Yes. Then you will be asked to make a new connection. Type a name for this connection, select an icon and click OK. The Location dialogue will show again, so click Cancel followed by Yes.

Now you can select Connect using COM1 and click OK. A Port settings dialogue will show, where you select 19200 as Bits per second. Use the default configuration for all other settings. Click OK and wait for a login prompt. (In some cases you have to press Return to get the login prompt.)

If you use a Linux workstation, connect like this: Make sure that there is a symbolic link named /dev/modem which points to the serial port you connected the Telecommuting Module to. Connect using *minicom* with the bit rate 19200 bits/s, and wait for a login prompt.

Log on as the user *admin*. The first time you log on, no password is required. You set the password when you run the installation script, which starts automatically when you have logged on.

Main Menu

The first thing you see after logging on as *admin* is the main menu. Here, you can change password, make a basic configuration of the Telecommuting Module, enter the Telecommuting Module into a failover team, save or load configuration, or remove all log messages from the e-mail queue.

```
3Com VCX IP Telecommuting Module Administration
  1. Basic configuration
  2. Save/Load configuration


  5. Wipe email logs
  6. Set password
  7. Command line interface
  a. About
  q. Exit admin
  ==>
```

1. Basic configuration

Basic settings for the Telecommuting Module, such as the IP address and the password.

This is one of two ways of giving the Telecommuting Module an IP address. The other way is to perform a *magic ping* (see chapter 2, Installing 3Com VCX IP Telecommuting Module).

2. Save/Load configuration

Save or upload the configuration using the Zmodem protocol.

5. Wipe email logs

Remove all log messages queued to be sent by e-mail.

6. Set password

Set a new password for the *admin* user.

7. Command line interface

Enter the Command Line Interface (CLI). See chapter 18, Command Line Reference, for more information about the CLI.

a. About

Under **About**, you get basic information about the Telecommuting Module's serial number, software version, installed licenses and patches, and links to more information.

q. Exit admin

Log out from the *admin* program.

Basic configuration

Use **Basic configuration** to give the Telecommuting Module a start configuration. You can assign an IP address to it (for the web GUI), enter the IP addresses of computers allowed to connect to the web GUI and change the administrator password.

Wherever you can enter a value, there will be a default one in brackets, which is the current value. Press Return to select the default value. This is an easy way to fast-forward if you only want to change one of the parameters.

IP address

Give the Telecommuting Module an IP address. The IP address will be added to any addresses already configured on the Telecommuting Module. The IP address entered here is the one that should be used to access the web GUI.

```
Basic unit installation program version 4.6.5

Press return to keep the default value

Network configuration inside:
 Physical device name[eth0]:
 IP address [0.0.0.0]: 10.47.2.242
 Netmask/bits [255.255.255.0]: 255.255.0.0
 Deactivate other interfaces? (y/n) [n]
```

Physical device name

Select which interface should get the IP address. The interfaces are named as on the exterior of the Telecommuting Module, such as eth0 and eth1.

IP address

Enter the IP address for the Telecommuting Module on the interface above. If the Telecommuting Module didn’t have an IP address before, the default address will be 0.0.0.0. Enter a different address, or the Telecommuting Module will be unreachable via the web GUI.

Netmask/bits

At **Netmask/bits**, enter the netmask for the network to which the IP address above belongs. The netmask can be written as an IP address or a number of bits (see also chapter 3, Configuring 3Com VCX IP Telecommuting Module).

Deactivate other interfaces

If the Telecommuting Module has been used one or more interfaces are active. Select here if all interfaces but the one selected above should be deactivated. You can activate them again via the web GUI.

Configuration computers

Enter here the computers from which it is allowed to configure the Telecommuting Module. The computers entered here are the only ones allowed to access the web GUI.

Select between allowing a single computer or an entire network.

```
Computers from which configuration is allowed:

You can select either a single computer or a network.

Configure from a single computer? (y/n) [y]
```

Configure from a single computer

If configuration of the Telecommuting Module should be allowed from a single computer only, answer **y** to the question above. Then enter the IP address of the configuration computer.

```
IP address [0.0.0.0]: 10.47.2.240
```

If the configuration computer is on the same network as the Telecommuting Module, these are all configuration settings needed. If the configuration computer is on a different network, the Telecommuting Module will ask for routing to that network.

```
Static routing:
The computer allowed to configure from is not on a network local to
this unit. You must configure a static route to it. Give
the IP address of the router on the network the unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

To let the Telecommuting Module know where traffic to the configuration computer should be sent to, you must enter the router it should use here. Enter the router which is on the same network as the Telecommuting Module and which is used to route traffic to the configuration computer.

You should also enter the network to which the configuration computer is connected.

Configure from multiple computers

If configuration of the Telecommuting Module should be allowed from more than one computer, answer **n** to the question above. Then enter the network address of the network to which the configuration computers are connected. This will allow all computers on this network to configure the Telecommuting Module.

```
Network number [0.0.0.0]: 10.47.2.0
Netmask/bits [255.255.255.0]: 255.255.255.0
```

Enter the network address and netmask for the configuration computer network. If they are on the same network as the Telecommuting Module, these are all configuration settings needed. If the configuration computers are on a different network, the Telecommuting Module will ask for routing to that network.

```
Static routing:
The network allowed to configure from is not on a network local to this
unit. You must configure a static route to it. Give the
IP address of the router on the network this unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

Enter the IP address of the router and the network to which the configuration computers are connected. This could be a bigger network than the one entered to distinguish the configuration computers.

Password

Set a password for the Telecommuting Module here.

```
Password []:
```

Note that the password will be printed on the screen when entered. It will also be shown when all settings are made.

Other

You can also select if all other configuration should be removed or not.

```
Other configuration
Do you want to reset the rest of the configuration? (y/n) [n]
```

If you answer `n`, nothing is removed. If you answer `y`, you have three alternatives to select from:

1. Clear as little as possible. This is the alternative that is used if you answer `n` to the question above. Both the preliminary and the permanent configurations will be updated with the configuration specified above.
2. Revert to the factory configuration and then apply the configuration specified above. This will affect the permanent but not the preliminary configuration.
3. Revert to the factory configuration and empty all logs and then apply the configuration specified above. Both the preliminary and the permanent configurations will be affected.

```
Update mode (1-3) [1]:
```

When all settings are entered, they are shown on the screen to be confirmed.

```
Is this configuration correct (yes/no/abort)?
```

`yes` will make the Telecommuting Module reboot using the new settings.

`no` will make the Telecommuting Module go through the Basic configuration questions again and allow you to change settings.

`abort` will make the Basic configuration script end without changing any settings.

Save/Load configuration

Here, you can save your configuration to a file or load a configuration from a file. The transfer is made using the Zmodem protocol, which can be found in terminal software such as Hyperterminal.

Load preliminary configuration

The configuration file selected here will be uploaded as a preliminary configuration. The permanent configuration will not be affected.

To load the configuration, select this alternative and then start the transfer in your terminal program.

Load both configurations and apply

The configuration file selected here will be uploaded as both the preliminary and the permanent configuration. When the upload is finished, the configuration will be applied.

To load the configuration, select this alternative and then start the transfer in your terminal program.

Save preliminary configuration

Save the preliminary configuration to a file. If your terminal program starts the transfer automatically, the file will be named `config.cfg`.

Save permanent configuration

Save the permanent configuration to a file. If your terminal program starts the transfer automatically, the file will be named `config.cfg`.

Main menu

Select this alternative to return to the main menu.

Wipe email logs

Here, you can erase all log messages queued for sending via email to one or more receivers. This could be useful if you by mistake made settings where lots of events are logged via email, which fill the queue rapidly.

```
This will remove all email logs that are waiting to be sent.

Do you want to proceed (yes/no)?
```

`yes` will remove all log messages from the email queue. These messages are not saved to file or similar before removed. If you log locally as well as via email, the local log will not be affected by this.

Note that this will only remove messages already queued up for sending. To prevent further queue jams, you must also change log classes for the events in question (see the chapter titled Logging).

`no` will make you return to the main menu without removing anything.

Set password

Here, you can change password for the *admin* user.

```
Old password:
New password:
New password again:
```

As this option requires that you are logged on as *admin*, you need to know the current password in order to change into a new one. If you have forgotten the password, you must reset it using the **FD** button to set a new one.

Exit admin

Select **Exit admin** to log out.

Chapter 15. Command Line Reference

This is a reference for the Command Line Interface (CLI), which can be accessed via the serial console or SSH (see the chapter titled Basic Administration).

Command Reference

Here is a list of the commands available in the Command Line Interface (CLI).

Commands are presented like this: **command [--flag] `parameter1|parameter2` [parameter3 ...]**. An example is:

ping `ip-address`

`--flag` means that the flag can modify the command in some way.

`parameter1` means that the parameter1 (like "ip-address" in the example) should be replaced with a specified parameter of that type (like a real IP address, 193.180.23.23).

`parameter1|parameter2` means that either parameter1 or parameter2 can be used.

`[parameter3]` means that this parameter is optional.

`parameter3 ...` means that this type of parameter can be used multiple times.

Help and Troubleshooting

help

Usage: **help [command ...]**

When this command is given without parameters, you get a list of available commands and tips about how to exit and how to interrupt a command.

If you enter a command, you will get information about how to use that command.

list-errors

Usage: **list-errors [--verbose] [table ...]**

List errors in a table. If no table name is entered, all errors in tables in the preliminary configuration are listed.

With the **--verbose** flag, a longer description of each error is displayed.

ping

Usage: **ping `ip-address|dns-name`**

Check if a host is reachable using ICMP Echo Request (ping). To use DNS names, a DNS server must be configured for the Telecommuting Module.

terminal-coding

Usage: **terminal-coding `encoding`**

Sets the character encoding used by the terminal. Supported encodings are ascii, iso-8859-1 and utf-8.

traceroute

Usage: **traceroute** `ip-address|dns-name`

Check the route for a packet to a remote host. To use DNS names, a DNS server must be configured for the Telecommuting Module.

Modifying Tables

add-row

Usage: **add-row** `table` **[**`field=value` **...]**

With this command, you add a row to a table and enter values into the listed fields for that row.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

clear-table

Usage: **clear-table** `table`

Remove all rows from a table.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

delete-row

Usage: **delete-row** `table rowid` **[**`rowid` **...]**

With this command, you delete one or more rows from a table. You get row IDs with the **dump-table** command.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

describe-table

Usage: **describe-table [--all] [**`table` **...]**

Describe a table (or all tables) with its fields and field types.

dump-table

Usage: **dump-table [--all] [--single-line] [**`table` **...]**

With this command, you show the contents of one or more tables. This is done as a number of commands that will re-create the data.

For tables with a fixed number of rows, a number of **modify-row** commands will be shown. For tables with a dynamic number of rows, there will be a **clear-table** command followed by a number of **add-row** commands.

The **--all** flag will make the Telecommuting Module show all tables. When this flag is used, you must not enter a table name.

The **--single-line** flag formats the output to make each command a single line. Otherwise, long commands will be split over multiple lines to make them easier to read and edit manually.

list-tables

Usage: **list-tables** `pattern`

List all tables matching the given pattern. The wildcard character "*" can be used in the pattern.

If you would like to find all tables with the string "forward" somewhere in the name, enter this:

list-tables *forward*

load-factory

Usage: **load-factory [--all]**

With this command, you reset the preliminary configuration to the factory default.

The **--all** flag resets all tables to their default values. Currently this flag is mandatory.

modify-row

Usage: **modify-row** `table` **[**`rowid`**]** `field=value` **[**`field=value` **...]**

With this command, you modify the listed fields of an existing row in a table. You get row IDs with the **dump-table** command.

If the table has a single fixed row ("Single row"), no row ID is required.

revert-edits

Usage: **revert-edits [--all]**

With this command, you reset the preliminary configuration to the permanent configuration.

The **--all** flag resets all tables to their permanent configuration. Currently this flag is mandatory.

Test Preliminary Configuration

abort-testrun

Usage: **abort-testrun**

With this command, you abort the ongoing test run.

acknowledge-event

Usage: **acknowledge-event**

Some events need to be acknowledged before you can enter any new commands. These events include when the Telecommuting Module ends a time-limited test mode.

Whenever you need to acknowledge an event, you will be prompted to do so by the CLI.

confirm-testrun

Usage: **confirm-testrun**

With this command, you confirm the ongoing test run, making the preliminary configuration permanent.

continue-testrun

Usage: **continue-testrun**

With this command, you enter an unlimited test mode. This can only be done when a test run is in progress. When in the unlimited test mode, you can make the preliminary configuration permanent using the **confirm-testrun** command, or abort the test run using the **abort-testrun** command.

start-testrun

Usage: **start-testrun** `[timelimit]`

With this command, you enter a limited test run of the Telecommuting Module's preliminary configuration. The test run will be automatically aborted when the time limit has expired, unless you enter the unlimited test mode using the **continue-testrun** command, or make the configuration permanent using the **confirm-testrun** command.

The test run can also be manually aborted using the **abort-testrun** command.

The time limit is specified in seconds. If no time limit is entered, the limit set in the **webgui.testmode** table is used.

Table Definitions

Here, the tables used in the Command Line Interface (CLI) are defined. For each table, the fields in the table are defined. Types and selections are defined in subsequent sections.

cert.cas

Corresponding setting in web GUI: CA Certificates on page Certificates

Table type: Dynamic

A list of CA certificates for use in the Ingate.

Field Name	Field Type	Explanation
cert	OptCertificate	The CA certificate.
crl	OptCertCrl	A certificate revocation list.
name	Name	The reference name for this certificate.

cert.own_certs

Corresponding setting in web GUI: Private Certificates on page Certificates

Table type: Dynamic

A list of own X.509 certificates.

Field Name	Field Type	Explanation
cert	OptPrivCert	An X.509 certificate.
name	Name	The reference name for this certificate.

config.allow_config

Corresponding setting in web GUI: Configuration Computers on page Access Control

Table type: Dynamic

A list of networks allowed to connect to the Ingate via HTTP or HTTPs for administration purposes.

Field Name	Field Type	Explanation
client_network	DnsIpNetwork_Filter	The network allowed to connect to the Ingate for administration purposes.
from_tunnel	OptIpsecPeerReference	Select if configuration traffic must be sent via an IPsec peer.
http	OnOffButton	Select if this row should apply to HTTP.
https	OnOffButton	Select if this row should apply to HTTPS.
logclass	LogclassReference	The logclass for this configuration traffic.
number	Integer	The rule number.
ssh	OnOffButton	Select if this row should apply to SSH.

config.allow_via_interface

Corresponding setting in web GUI: Configuration Allowed Via Interface on page Access Control

Table type: Fixed

Select to allow configuration traffic (HTTP, HTTPs, and SSH) via the different interfaces of the Ingate.

Field Name	Field Type	Explanation
config_on	OnOffToggle	Allow configuration via this interface.
interface	InterfaceSel	An interface on the Ingate.

config.auth_logclass

Corresponding setting in web GUI: Log class for configuration server logins on page Logging Configuration

Table type: Single row

The log class for configuration server logins.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

config.authentication

Corresponding setting in web GUI: User Authentication For Web Interface Access on page Access Control

Table type: Single row

Select how administrator logins via HTTP and HTTPs should be authenticated.

Field Name	Field Type	Explanation
auth_type	config_auth_sel	The authentication method to use for administrators.

config.http_servers

Corresponding setting in web GUI: Configuration via HTTP on page Access Control

Table type: Single row

The IP address and port which should allow HTTP connections to the administrator interface.

Field Name	Field Type	Explanation
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.

config.https_servers

Corresponding setting in web GUI: Configuration via HTTPS on page Access Control

Table type: Single row

The IP address and port which should allow HTTPS connections to the administrator interface, and the certificate to use by the Ingate to authenticate.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use for this IP/port combination.
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.

config.mgmt_logclass

Corresponding setting in web GUI: Log class for administration and configuration on page Logging Configuration

Table type: Single row

The log class for administration and configuration.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

config.ssh_servers

Corresponding setting in web GUI: Configuration via SSH on page Access Control

Table type: Single row

The IP address and port which should allow SSH connections to the administrator interface.

Field Name	Field Type	Explanation
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.

failover.iface_ref_hosts

Corresponding setting in web GUI: Reference Hosts on page Reference Hosts

Table type: Dynamic

A list of reference hosts for the failover team.

Field Name	Field Type	Explanation
address	DnsDynIpOtherHost	The IP address of the reference host.
interface	InterfaceSel	The interface to which the reference host is connected.

fent.always_fent

Corresponding setting in web GUI: Always use NAT traversal on page Remote SIP Connectivity

Table type: Single row

Field Name	Field Type	Explanation

fent_always_fent_exceptions

Corresponding setting in web GUI: Unconditioned NAT Exceptions on page Remote SIP Connectivity

Table type: Dynamic

Field Name	Field Type	Explanation

fent_always_fent_interfaces

Corresponding setting in web GUI: Unconditioned NAT Interfaces on page Remote SIP Connectivity

Table type: Dynamic

Field Name	Field Type	Explanation

fent.fent

Corresponding setting in web GUI: Remote NAT traversal on page Remote SIP Connectivity

Table type: Single row

Turn the SIP NAT Traversal on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

fent.fent_keepalive

Corresponding setting in web GUI: NAT keepalive method, NAT timeout for UDP, NAT timeout for TCP on page Remote SIP Connectivity

Table type: Single row

Type of keepalive to use for fented clients.

Field Name	Field Type	Explanation
tcp_timeout	PositiveSysInteger	Timeout for TCP - adapt to the NAT used (seconds).
type	fent_keepalive_sel	Use which method to keep fented clients alive.
udp_timeout	PositiveSysInteger	Timeout for UDP - adapt to the NAT used (seconds).

fent.map_signal_address

Corresponding setting in web GUI: Remote Clients Signaling Forwarding on page Remote SIP Connectivity

Table type: Single row

Map signaling address for remote users.

Field Name	Field Type	Explanation
listen_ip	OptOwnIpReference	Incoming destination IP address.
listen_port	OptPortNumber	Incoming destination port.
send_ip	OptAliasIpReference	Outgoing source IP address.

fent.media_release

Corresponding setting in web GUI: Media Route on page Remote SIP Connectivity

Table type: Single row

Route media directly between clients behind the same NAT.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

fent.stun

Corresponding setting in web GUI: STUN Server on page Remote SIP Connectivity

Table type: Single row

Settings for the builtin STUN server.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turn the STUN server on or off.
port1	OptPortNumber	One port of the STUN server, used by both IP addresses.
port2	OptPortNumber	Another port of the STUN server, used by both IP addresses.
server1	OptOwnIpReference	One IP address of the STUN server.
server2	OptOwnIpReference	Another IP address of the STUN server.

firewall.blind_route_policy

Corresponding setting in web GUI: Policy For Packets From Unused Gateways on page Default Gateway

Table type: Single row

This policy controls how packets from currently unused gateways should be treated.

Field Name	Field Type	Explanation
action	blind_sel	The policy to use for packets from unused gateways.

firewall.broadcast_logclass

Corresponding setting in web GUI: Log class for broadcast packets on page Logging Configuration

Table type: Single row

The log class for broadcast packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

firewall.default_policy

Corresponding setting in web GUI: IP Policy on page Basic Configuration

Table type: Single row

This setting specifies how the Ingate should treat packets that do not match any other configured rule.

Field Name	Field Type	Explanation
action	policy_sel	The policy to use for packets that don't match any

firewall.dhcp_logclass

Corresponding setting in web GUI: Log class for DHCP requests on page Logging Configuration

Table type: Single row

The log class for DHCP packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

firewall.network_groups

Corresponding setting in web GUI: Networks and Computers on page Networks and Computers

Table type: Dynamic

In this table all groups of computers/IP addresses are defined, to be used when configuring the rest of the Ingate.

Field Name	Field Type	Explanation
interface	OptVlanIfReference	The interface or VLAN of the Ingate on which this IP range is located.
lower_ip	OptDnsIpAddress	The first IP address in the range for this group.
name	GroupName	A name of the network group. It is used when referring to it from this or other tables.
subgroup	SubGroup	A reference to the 'name' field. Used when building a network group from multiple other groups.
upper_ip	OptDnsIpAddress	The last IP address in the range for this group. This field can be left empty if the group is a single IP address.

firewall.own_logclass

Corresponding setting in web GUI: Log class for packets to the Telecommuting Module on page Logging Configuration

Table type: Single row

The log class for packets addressed to the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

firewall.ping_policy

Corresponding setting in web GUI: Policy For Ping To Your 3Com VCX IP Telecommuting Module on page Basic Configuration

Table type: Single row

This setting specifies how the Ingate should reply to ping packets to its own IP addresses.

Field Name	Field Type	Explanation
policy	ping_policy_sel	Select the policy.

firewall.policy_logclass

Corresponding setting in web GUI: Log class for non-SIP packets on page Logging Configuration

Table type: Single row

The log class for packets that are processed according to the default policy of the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

firewall.services

Corresponding setting in web GUI: Services on page Services

Table type: Dynamic

Defines services used when building up firewall rules.

Field Name	Field Type	Explanation
client_ports	OptPortRangeList	Ports from which the traffic originates.
fwtype	fwtype_sel	The firewall type to use for this service.
ixmptype	OptIcmpRangeList	Type for ICMP packets.
name	GroupName	A name of the service. It is used to refer to this service.
protocol	OptProtocolReference	A reference to the 'name' field of the 'db.firewall.protocols' table.
server_ports	OptPortRangeList	Ports to which the traffic is destined.
subgroup	SubGroup	A reference to the 'name' field. Used when building a service from multiple other services.

firewall.spoofing_logclass

Corresponding setting in web GUI: Log class for spoofed packets on page Logging Configuration

Table type: Single row

The log class for spoofed packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

firewall.timeclasses

Corresponding setting in web GUI: Time Classes on page Time Classes

Table type: Dynamic

Time classes are defined to make time-limited firewall rules and relays possible.

Field Name	Field Type	Explanation
from_day	weekday_sel	The day when the time class starts.
from_time	Time_HH_MM	The time when the time class starts.
name	GroupName	A name of the time class. It is used when referring to it from other tables.
to_day	weekday_sel	The day when the time class ends.
to_time	Time_HH_MM	The time when the time class end.

idsips.active

Corresponding setting in web GUI: SIP IDS/IPS on page SIP IDS/IPS

Table type: Single row

Switches the IDS/IPS module on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

idsips.predefined_ips_rules

Corresponding setting in web GUI: Packet Filtering IDS/IPS Rules from 3Com on page SIP IDS/IPS

Table type: Dynamic

Table for imported predefined IDS/IPS rules from Ingate.

Field Name	Field Type	Explanation
action	function_sel	The policy for how this type of traffic should be treated.
description	NonemptyString	Short description. Cannot be changed by the user.
enabled	OnOffToggleOn	Turns this rule on or off.
id	NonemptyString	Unique ID number for the rule. Should even be unique from the rate limited number. Cannot be changed by the user.
logclass	IDSIPSLogclassReference	How traffic matching this rule should be logged.
name	Name	Name of the rule. Cannot be changed by the user.
protocol	NonemptyString	Protocol - udp, tcp or ip where ip means both tcp and udp. Cannot be changed by the user.
rulestub	NonemptyString	Active part of the rule. Cannot be changed by the user.

idsips.rate_limited_ips

Corresponding setting in web GUI: Rate Limiting on page SIP IDS/IPS

Table type: Dynamic

Table for user specified IDS/IPS rate limit rules.

Field Name	Field Type	Explanation
blacklist_duration	OptNonNegativeInteger	The blacklist interval (in seconds).
enabled	OnOffToggleOn	Turns this rule on or off.
hits	hits_number	The number of hits inside the given window.
logclass	IDSIPSLogclassReference	How traffic matching this rule should be logged.
method	SipMethodsReference	The SIP method to match on.
name	IpsRuleName	User-defined name.
number	Integer	The rule number.
request_uri	OptString	The Request-URI to match on. Written as a regular expression.
response	OptString	The SIP response to match on. Written as a regular expression.
source_netgroup	OptNetgroupReference	The source network for the traffic.
window	window_number	Time interval (in seconds) for hits.

ipsec.crypto_def

Corresponding setting in web GUI: Crypto Definitions on page IPsec Cryptos

Table type: Dynamic

Field Name	Field Type	Explanation

ipsec.esp_proposals

Corresponding setting in web GUI: ESP/IPsec (Phase 2) Encryption Proposals on page IPsec Cryptos

Table type: Dynamic

Field Name	Field Type	Explanation

ipsec.espah_logclass

Corresponding setting in web GUI: Log class for ESP packets on pages IPsec Settings and Logging Configuration

Table type: Single row

The log class for ESP packets.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

ipsec.ike_logclass

Corresponding setting in web GUI: Log class for IKE and NAT-T packets on pages IPsec Settings and Logging Configuration

Table type: Single row

The log class for IKE and NAT-T packets.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

ipsec.ike_proposals

Corresponding setting in web GUI: IKE/ISAKMP (Phase 1) Encryption Proposals on page IPsec Cryptos

Table type: Dynamic

Field Name	Field Type	Explanation

ipsec.ipsec_nets

Corresponding setting in web GUI: IPsec Networks on page IPsec Tunnels

Table type: Dynamic

A list of networks which will use IPsec connections.

Field Name	Field Type	Explanation
name	Name	A name of the network. It is used to refer to this network.
network	DnsIpNetwork_Filter	The network to be tunneled through an IPsec tunnel.

ipsec.nat_t_keepalive

Corresponding setting in web GUI: NAT Traversal (NAT-T) on page IPsec Settings

Table type: Single row

NAT-T keepalive settings.

Field Name	Field Type	Explanation
force	OnOffToggle	Force the Ingate to send keepalive packets.
interval	Integer	The interval between two keepalive packets (seconds).

ipsec.peers

Corresponding setting in web GUI: IPsec Peers on page IPsec Peers

Table type: Dynamic

A list of IPsec peers for the Ingate.

Field Name	Field Type	Explanation
auth_type	AuthtypeSel	The authentication type for this peer.
enabled	OptOnOffToggleOn	Activate this peer.
isakmp_sa_life	IsakmpSALife	ISAKMP key lifetime.
local_addr	OptOwnIpReference	The Ingate's IP address to which this peer must connect.
name	GroupName	A name of the peer. It is used to refer to this peer.
radius	OptOnOffToggle	Activate RADIUS authentication for a road warrior peer.
remote_addr	IpsecPeerAddr	The peer's IP address.
secret	AuthData	Authentication data for this peer.
subgroup	SubGroup	A reference to the 'name' field. Used when building a peer from multiple other peers.

ipsec.pluto_logclass

Corresponding setting in web GUI: Log class for IPsec key negotiations on pages IPsec Settings and Logging Configuration

Table type: Single row

The log class for IPsec key negotiations.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

ipsec.plutoverbose_logclass

Corresponding setting in web GUI: Log class for IPsec key negotiation debug messages on pages IPsec Settings and Logging Configuration

Table type: Single row

The log class for verbose messages from IPsec key negotiations.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

ipsec.radiusauth_server

Corresponding setting in web GUI: Authentication Server on page Authentication Server

Table type: Single row

The Ingate IP address and port to use for road warrior RADIUS authentication. A certificate must also be selected.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use for this IP/port combination.
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.

ipsec.tunneled_nets

Corresponding setting in web GUI: IPsec Tunnels on page IPsec Tunnels

Table type: Dynamic

Definitions of which networks can use each IPsec connection.

Field Name	Field Type	Explanation
ipsec_sa_life	IpsecSALife	IPsec key lifetime.
local_net	OptIpsecNetReference	The local network which can use the connection.
local_type	IpsecNetLocalSel	The type of IP for which the IPsec connection is negotiated and which can use the connection.
nat_as_address	OptOwnIpReference	What address traffic through this tunnel should be NAT:ed as, if set. The IPsec SA will be negotiated for this address too, instead of the specified local network.
peer	IpsecPeer_Group	The peer for which network definitions are made.
remote_net	OptIpsecNetReference	The remote network which can use the connection.
remote_type	IpsecNetRemoteSel	The type of IP for which the IPsec connection is negotiated and which can use the connection.

ipsec.userauth_logclass

Corresponding setting in web GUI: Log class for IPsec user authentications on pages IPsec Settings and Logging Configuration

Table type: Single row

The log class for IPsec user authentications.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

ipsec.x509_cacerts

Corresponding setting in web GUI: CA Certificates on page IPsec Certificates

Table type: Dynamic

Certificates for CAs which have signed IPsec peer certificates.

Field Name	Field Type	Explanation
ca	CaReference	A CA certificate.

ipsec.x509_cert

Corresponding setting in web GUI: Local X.509 Certificate on page IPsec Certificates

Table type: Single row

The X.509 certificate to use for IPsec connections.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate of this unit.

misc.conntrack_timeouts

Corresponding setting in web GUI: Advanced on page Advanced

Table type: Single row

Timeouts for connections through the Ingate.

Field Name	Field Type	Explanation
icmp	PositiveSysInteger	Timeout for ICMP connections.
tcp_established	PositiveSysInteger	Timeout for established TCP connections.
udp	PositiveSysInteger	Timeout for one-way UDP connections.
udp_stream	PositiveSysInteger	Timeout for two-way UDP connections.

misc.default_domain

Corresponding setting in web GUI: Default domain on page Basic Configuration

Table type: Single row

The default domain when entering configuration.

Field Name	Field Type	Explanation
domain	OptDomainName	A domain name to use in the settings.

misc.dns_servers

Corresponding setting in web GUI: DNS Servers on page Basic Configuration

Table type: Dynamic

A list of DNS servers which the Ingate can use.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
server	DnsDynIpReachableHost	A DNS server.

misc.dyndns

Corresponding setting in web GUI: DynDNS General Configuration, User, SMTP Server on page Dynamic DNS update

Table type: Single row

Settings for the DynDNS service.

Field Name	Field Type	Explanation
backup	OnOffToggle	The SMTP server entered here is a backup server.
enabled	OnOffToggle	Activate update via DynDNS.
ip	OptDepOwnIpReference	The local IP address to be referred to for the host names listed here.
mx	OptDomainName	The SMTP server for the domain(s).
offline	OnOffToggle	Use offline URL redirection.
password	DyndnsPassword	The DynDNS password.
service	DyndnsServiceSel	The DynDNS service to use.
user	OptName	The DynDNS user name.
wildcard	OnOffToggle	Use wildcard host names.

misc.dyndns_name

Corresponding setting in web GUI: DNS Names to Update at DynDNS on page Dynamic DNS update

Table type: Dynamic

A list of host and domain names to be updated at DynDNS.

Field Name	Field Type	Explanation
name	DomainName	A host or domain name.

misc.fversion

Corresponding setting in web GUI: Check for new versions of 3Com VCX IP Telecommuting Module on page Basic Configuration

Table type: Single row

Activate version control on the Ingate.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

misc.ntp_servers

Corresponding setting in web GUI: NTP Servers To Use If NTP Is Enabled on page Date and Time

Table type: Dynamic

A list of NTP servers to use.

Field Name	Field Type	Explanation
server	DnsDynIpReachableHost	A server name or IP address.

misc.unitname

Corresponding setting in web GUI: Name of this Telecommuting Module on page Basic Configuration

Table type: Single row

The name of this Ingate unit.

Field Name	Field Type	Explanation
unitname	OptString	The user-defined name.

misc.use_ntp

Corresponding setting in web GUI: Change Date and Time With NTP on page Date and Time

Table type: Single row

Activate NTP for the Ingate system clock.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

monitor.cpuload_level_alarm

Corresponding setting in web GUI: CPU Load Trap Levels on page SNMP

Table type: Single row

When to create alarm messages for high CPU load.

Field Name	Field Type	Explanation
max_cpuload	OptPercent	The load level when an alarm message should be created and the alarm state set.
ok_cpuload	OptPercent	The load level when the alarm state is reset.

monitor.email_alert_logclass

Corresponding setting in web GUI: Log class for email errors on page Logging Configuration

Table type: Single row

The log class for email errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

monitor.email_server

Corresponding setting in web GUI: SMTP Server on page Log Sending

Table type: Single row

The SMTP server to use when log messages are sent to an email address.

Field Name	Field Type	Explanation
server	OptDnsReachableHost	A server name or IP address.

monitor.hardware_logclass

Corresponding setting in web GUI: Log class for hardware errors on page Logging Configuration

Table type: Single row

The log class for hardware errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

monitor.logclasses

Corresponding setting in web GUI: Log Classes on page Log Classes

Table type: Dynamic

A list of log classes used in the Ingate.

Field Name	Field Type	Explanation
email	OptString	Enter email address(es) which the log message should be sent to.
facility	syslogfacility_sel	Select the syslog facility to use.
level	sysloglevel_sel	Select the syslog level to use.
local	OnOffToggle	Turn on or off logging to local disk/memory.
name	Name	The name of the log class. The name is used when referring to this log class.

monitor.memory_level_alarm

Corresponding setting in web GUI: Memory Usage Trap Levels on page SNMP

Table type: Single row

When to create alarm messages for high memory usage.

Field Name	Field Type	Explanation
max_memory	OptPercent	The memory usage level when an alarm message should be created and the alarm state set.
ok_memory	OptPercent	The memory usage level when the alarm state is reset.

monitor.radius_errors_logclass

Corresponding setting in web GUI: Log class for RADIUS errors on page Logging Configuration

Table type: Single row

The log class for RADIUS errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

monitor.sip_level_alarms

Corresponding setting in web GUI: SIP Sessions Trap Levels, SIP User Registrations Trap Levels on page SNMP

Table type: Single row

When to create alarm messages for used SIP User Registration and Traversal licenses.

Field Name	Field Type	Explanation
max_registered_users	OptNonNegativeInteger	The number of registered users when an alarm message should be created and the alarm state set.
max_sessions	OptNonNegativeInteger	The number of sessions when an alarm message should be created and the alarm state set.
ok_registered_users	OptNonNegativeInteger	The number of registered users when the alarm state is reset.
ok_sessions	OptNonNegativeInteger	The number of sessions when the alarm state is reset.

monitor.snmp_agent_address

Corresponding setting in web GUI: The Telecommuting Module IP address to respond to SNMP requests on page SNMP

Table type: Single row

The IP address of the Ingate which responds to SNMP requests.

Field Name	Field Type	Explanation
snmpagentip	OptDepOwnIpReference	The IP address to respond to SNMP requests.

monitor.snmp_agent_logclass

Corresponding setting in web GUI: Log class for SNMP errors on page Logging Configuration

Table type: Single row

The log class for SNMP errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

monitor.snmp_contact_person

Corresponding setting in web GUI: Contact person on page SNMP

Table type: Single row

The contact person for this Ingate.

Field Name	Field Type	Explanation
snmp_contact_person	OptDepString	The name of the contact.

monitor.snmp_management_stations

Corresponding setting in web GUI: Servers allowed to contact the Telecommuting Module via SNMP on page SNMP

Table type: Single row

The servers allowed to send SNMP requests to the Ingate.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The server network.

monitor.snmp_node_location

Corresponding setting in web GUI: Node location on page SNMP

Table type: Single row

The location of this Ingate.

Field Name	Field Type	Explanation
snmp_node_location	OptDepString	The location.

monitor.snmp_packet_logclass

Corresponding setting in web GUI: Log class for SNMP requests to the Telecommuting Module on page Logging Configuration

Table type: Single row

The log class for SNMP requests received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

monitor.snmp_trap_receivers

Corresponding setting in web GUI: SNMP Traps on page SNMP

Table type: Dynamic

A list of SNMP trap receivers.

Field Name	Field Type	Explanation
community	NonWhiteName	The SNMP community to use when sending traps.
server	DnsReachableHost	The server to receive traps.
version	snmptrapversion_sel	The SNMP version to use when sending traps.

monitor.snmp_trap_sending

Corresponding setting in web GUI: Trap sending function on page SNMP

Table type: Single row

Turn SNMP trap sending on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

monitor.snmp_v1v2c_access

Corresponding setting in web GUI: Access via SNMPv1 and SNMPv2c on page SNMP

Table type: Single row

Turn SNMP access using version 1 or version 2c on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

monitor.snmp_v1v2c_auth

Corresponding setting in web GUI: SNMP v1 and v2c on page SNMP

Table type: Dynamic

Authentication for SNMP requests v1 and v2c.

Field Name	Field Type	Explanation
community	NonWhiteName	A community.

monitor.snmp_v3_access

Corresponding setting in web GUI: Access via SNMPv3 on page SNMP

Table type: Single row

Turn SNMP access using version 3 on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

monitor.snmp_v3_auth

Corresponding setting in web GUI: SNMP v3 on page SNMP

Table type: Dynamic

Authentication for SNMP requests v3.

Field Name	Field Type	Explanation
authentication	snmpv3_auth_sel	Authentication algorithm used for this user.
password	SnmpPassword	The password for this user.
privacy	snmpv3_privacy_sel	Encryption algorithm used for this user.
user	NonWhiteName	A user allowed to make SNMP requests.

monitor.syslog_servers

Corresponding setting in web GUI: Syslog Servers on page Log Sending

Table type: Dynamic

A list of syslog servers where log messages should be sent.

Field Name	Field Type	Explanation
server	DnsDynIpReachableHost	A server name or IP address.

monitor.watchdogs

Corresponding setting in web GUI: Automatic Restart of the SIP Module on page Restart

Table type: Single row

Watchdog settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns this watchdog on or off.
service	NonWhiteName	The service monitored.

network.alias_addresses

Corresponding setting in web GUI: Alias on pages Interface (Network Interface 1 and 2)

Table type: Dynamic

A list of extra Ingate IP addresses on the networks defined in the ’db.network.local_nets’ table.

Field Name	Field Type	Explanation
address	DnsIpAddress	The IP address to use.
interface	InterfaceSel	The interface to which the network is connected.
name	Name	A name for this IP address. It is used to refer to the IP address.

network.extra_default_gateways

Corresponding setting in web GUI: Additional Default Gateways on page Default Gateway

Table type: Dynamic

A list of extra Ingate IP addresses on the networks defined in the ’db.network.local_nets’ table.

Field Name	Field Type	Explanation
address	DnsIpAddress	The IP address to use.
interface	InterfaceSel	The interface to which the network is connected.
name	Name	A name for this IP address. It is used to refer to the IP address.

network.interfaces

Corresponding setting in web GUI: General, Obtain IP Address Dynamically, Speed and Duplex on pages Interface (Network Interface 1 and 2)

Table type: Fixed

Interface settings.

Field Name	Field Type	Explanation
autoneg	autoneg_sel	Set speed and duplex for the interface.
dynip	dynip_client_sel	Select how the IP address is acquired.
enabled	OnOffToggle	Enable the interface.
interface	InterfaceSel	The physical interface.
name	Name	A name for this interface.

network.local_nets

Corresponding setting in web GUI: Directly Connected Networks on pages Interface (Network Interface 1 and 2)

Table type: Dynamic

A list of IP networks directly connected to the Ingate, and the Ingate's IP addresses on these networks.

Field Name	Field Type	Explanation
address	DnsIpNetwork_Interface	The IP address of the interface, and the netmask of the network.
interface	InterfaceSel	The interface to which the network is connected.
name	Name	A name for this IP address. It is used to refer to the IP address.
vlanid	OptVlanId	The VLAN associated with the network.

network.pppoe

Corresponding setting in web GUI: PPPoE on page PPPoE

Table type: Single row

PPPoE settings.

Field Name	Field Type	Explanation
lcp_echo_interval	OptPositiveSysInteger	Keep alive packet interval (seconds).
logclass	FirewallLogclassReference	The log class to use for PPPoE negotiations.
password	OptPassword	The PPPoE password.
service	OptNonWhiteString	The PPPoE service.
user	OptNonWhiteString	The name of the PPPoE user.

network.route_test_servers

Corresponding setting in web GUI: Gateway Reference Hosts on page Default Gateway

Table type: Dynamic

A list of reference servers to use when determining if a default gateway is alive.

Field Name	Field Type	Explanation
server	DnsIpAddress	The reference server to use.

network.routes

Corresponding setting in web GUI: Main Default Gateways, Static Routing on pages Default Gateway and Interface (Network Interface 1 and 2)

Table type: Dynamic

A list of static routes for networks not directly connected to the Ingate.

Field Name	Field Type	Explanation
destination	RouteDestination	The routed network.
gateway	DnsDynIpAddress	The router to use for this network.
interface	InterfaceSel	The interface where the router is located.
priority	RoutePriority	The priority of the gateway.

network.vlans

Corresponding setting in web GUI: Named VLANs on page VLAN

Table type: Dynamic

A list of VLANs used on the different interfaces.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface on which the VLAN is defined.
name	Name	A name of the VLAN. It is used to refer to this VLAN.
vlanid	VlanId	The id of this VLAN.

password.admin_users

Corresponding setting in web GUI: Other Accounts on page User Administration

Table type: Dynamic

A list of the users allowed to access the Ingate web administrator interface.

Field Name	Field Type	Explanation
password	AdminPassword	The password for this administrator user.
type	AdminTypeSel	The administrator type.
user	AdminUser	The name of this administrator user.

pptp.gre_logclass

Corresponding setting in web GUI: Log class for GRE packets on pages Logging Configuration and PPTP

Table type: Single row

The log class for GRE packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

pptp.pptp_enable

Corresponding setting in web GUI: PPTP server on page PPTP

Table type: Single row

Turn the PPTP function on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

pptp.pptp_logclass

Corresponding setting in web GUI: Log class for PPTP packets on pages Logging Configuration and PPTP

Table type: Single row

The log class for PPTP packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

pptp.pptp_nets

Corresponding setting in web GUI: Client Network, Keep Alive, DNS Servers, WINS Servers on page PPTP

Table type: Single row

Settings for the built-in PPTP server.

Field Name	Field Type	Explanation
client_netgroup	PPTPNetgroupReference	The range of IP addresses for PPTP clients.
dns1	OptDnsIpAddress	The DNS server which PPTP clients should use.
dns2	OptDnsIpAddress	A second DNS server which PPTP clients should use.
lcp_echo_interval	OptPositiveSysInteger	Keep alive packet interval (seconds).
local_addr	PPTPOwnIpReference	The local gateway for PPTP clients.
wins1	OptDnsIpAddress	The WINS server which PPTP clients should use.
wins2	OptDnsIpAddress	A second WINS server which PPTP clients should use.

pptp.pptp_serverip

Corresponding setting in web GUI: PPTP Connection IP Address on page PPTP

Table type: Single row

The IP address for the PPTP server in the Ingate.

Field Name	Field Type	Explanation
ip	PPTPOwnIpReference	The server IP address.

pptp.pptp_users

Corresponding setting in web GUI: PPTP Users on page PPTP

Table type: Dynamic

A list of PPTP users in the system.

Field Name	Field Type	Explanation
enabled	OnOffToggleOn	Activate the user.
password	PptpPassword	PPTP password for this user.
user	Name	The name of the PPTP user.

pptp.pptpneg_logclass

Corresponding setting in web GUI: Log class for PPTP negotiations on pages Logging Configuration and PPTP

Table type: Single row

The log class for PPTP negotiations to the Ingate PPTP server.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

qos.bandwidths

Corresponding setting in web GUI: General, Bandwidths For SIP Media, Bandwidths on pages QoS Interfaces and QoS and SIP

Table type: Fixed

QoS bandwidth settings per interface.

Field Name	Field Type	Explanation
egress_bandwidth	OptBandWidth	Egress bandwidth limit for the interface (kbit/s).
egress_enabled	OnOffToggle	Use egress QoS for this interface.
egress_reserve_sip_media	OptBandWidth	Bandwidth reservation for outgoing SIP media (kbit/s). Currently only applies to UDP.
egress_reserve_sip_media_emergency	OptBandWidth	Bandwidth reservation for outgoing emergency SIP media (kbit/s). Currently only applies to UDP.
ingress_bandwidth	OptBandWidth	Ingress bandwidth limit for the interface (kbit/s).
ingress_enabled	OnOffToggle	Use ingress QoS for this interface.
ingress_reserve_sip_media	OptBandWidth	Bandwidth reservation for incoming SIP media (kbit/s). Currently only applies to UDP.
ingress_reserve_sip_media_emergency	OptBandWidth	Bandwidth reservation for incoming emergency SIP media (kbit/s). Currently only applies to UDP.
interface	InterfaceSel	The interface for which QoS settings are made.

qos.classes

Corresponding setting in web GUI: QoS Classes on page QoS Classes

Table type: Dynamic

A list of QoS classes used for matching incoming traffic.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The source network for the traffic.
dscp	OptDSCPInteger	The DSCP field of the packets.
max_packet_size	OptPacketSize	The maximum packet size for the traffic.
min_packet_size	OptPacketSize	The minimum packet size for the traffic.
name	Name	The name of this class. This name is used to refer to the class in other tables.
number	Integer	The priority of this row.

Field Name	Field Type	Explanation
server_netgroup	OptNetgroupReference	The destination network for the traffic.
service	OptServicesReference	The service matching the traffic.
sip	sip_sel	The traffic type.
tos	opttos_sel	The TOS field of the packets.

qos.egress_default_queueing

Corresponding setting in web GUI: Unclassified Traffic on page QoS Interfaces

Table type: Fixed

Assign priority and bandwidth for traffic not listen in the 'db.qos.egress_queueing' table.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	pqueue_sel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

qos.egress_queueing

Corresponding setting in web GUI: Classification on page QoS Interfaces

Table type: Dynamic

Assign priority and bandwidth for different types of traffic.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic for which bandwidth is assigned or limited.
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	pqueue_sel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

qos.ingress_default_queueing

Corresponding setting in web GUI: Unclassified Traffic on page QoS Interfaces

Table type: Fixed

Assign priority and bandwidth for traffic not listen in the 'db.qos.ingress_queueing' table.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	pqueue_sel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

qos.ingress_queueing

Corresponding setting in web GUI: Classification on page QoS Interfaces

Table type: Dynamic

Assign priority and bandwidth for different types of traffic.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic for which bandwidth is assigned or limited.
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	pqueue_sel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

qos.sip_cac

Corresponding setting in web GUI: Call Admission Control, Codec Bandwidths on page QoS and SIP

Table type: Single row

Call Admission Control settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Use Call Admission control.

qos.status

Corresponding setting in web GUI: Type of QoS on page QoS Interfaces

Table type: Fixed

Global QoS settings.

Field Name	Field Type	Explanation
prio_save	Percent	Save this amount of bandwidth for lower priority traffic.
type	qostype_sel	Type of QoS to use.

qos.tagging

Corresponding setting in web GUI: TOS/DSCP Modification on page TOS Modification

Table type: Dynamic

A list of traffic to mark up by setting the TOS or DSCP field.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic to mark up.
dscp	OptDSCPInteger	Set the DSCP field.
tos	opttos_sel	Set the TOS field.

sip.accelerated_tls

Corresponding setting in web GUI: Accept TCP Marked As TLS on page Interoperability

Table type: Single row

Accept TCP marked as TLS.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.active

Corresponding setting in web GUI: SIP Module on page Basic Settings

Table type: Single row

Turns the SIP module on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.add_expire_header

Corresponding setting in web GUI: Expires Header on page Interoperability

Table type: Single row

Select if an Expires header should be added to the response to a SIP REGISTER request.

Field Name	Field Type	Explanation
action	add_expire_header_sel	Select which action to perform.

sip.allowed_codecs

Corresponding setting in web GUI: Codecs on page Sessions and Media

Table type: Dynamic

Field Name	Field Type	Explanation
allow	OnOffToggle	Allow this codec.
bandwidth	OptPositiveSysInteger	Bandwidth needed by this codec.
name	WildcardIdentifier	Name of codec.
type	OptCodecTypeSel	Type of codec.

sip.asserted_identity

Corresponding setting in web GUI: Use P-Asserted-Identity on page Authentication and Accounting

Table type: Single row

Turn use of P-Asserted-Identity on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.auth_methods

Corresponding setting in web GUI: SIP Methods on page SIP Methods

Table type: Dynamic

Allow and authenticate SIP requests based on which SIP method is used.

Field Name	Field Type	Explanation
allow	OnOffToggle	Allow this type of SIP request.
auth	OnOffToggle	Require authentication for this type of SIP request.
method	SipMethod	The SIP method for which the settings are made.
traffic_to	sip_auth_dir_sel	The direction of the SIP request.

sip.b2bua_offer_from_template

Corresponding setting in web GUI: on page Interoperability

Table type: Single row

Field Name	Field Type	Explanation

sip.codec_filtering

Corresponding setting in web GUI: Limitation of RTP Codecs on page Sessions and Media

Table type: Single row

Turn codec filtering on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.data_interfaces

Corresponding setting in web GUI: Data Interfaces on page Surroundings

Table type: Dynamic

Field Name	Field Type	Explanation

sip.default_gateway

Corresponding setting in web GUI: SIP Default Gateway on page Routing

Table type: Single row

Field Name	Field Type	Explanation

sip.dialing_domains

Corresponding setting in web GUI: Translation Exceptions on page Interoperability

Table type: Dynamic

List domain names/IP addresses that should not be rewritten when forwarded by the Ingate.

Field Name	Field Type	Explanation
ip	DnsIpAddress	The domain name.

sip.emergency

Corresponding setting in web GUI: Emergency Number on page Dial Plan

Table type: Single row

PSTN emergency number.

Field Name	Field Type	Explanation
emergency	NoCommaString	The emergency number.

sip.extern_radius_db

Corresponding setting in web GUI: Select SIP User Database, RADIUS Database Settings on page Authentication and Accounting

Table type: Single row

Settings for SIP authorization and authentication.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The network from which RADIUS database SIP users are allowed to register.
db_type	SIPRadiusSel	Which database to use for SIP authorization and authentication.

sip.external_relay

Corresponding setting in web GUI: DNS Override For SIP Requests on page Routing

Table type: Dynamic

Match on the domain in the Request-URI, and send the request on to a different server.

Field Name	Field Type	Explanation
domain	DomainGroup	Matches the domain in the Request-URI.
port	OptPortNumber	Port to forward the request to.
priority	rfc2782priority	Priority of this IP address. A lower number is a higher priority.
relay_to	DnsReachableHost	SIP domain or IP address to forward the request to.
transport	SipTransportSel	Transport to use when forwarding the request.
weight	rfc2782weight	Weight of this IP address. For IP addresses of the same priority, requests are forwarded according to their weight. A higher number means more requests.

sip.fix_file_transfer_port

Corresponding setting in web GUI: Open Port 6891 For File Transfer on page Interoperability

Table type: Single row

Always open port 6891 for file transfer.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.force_modify

Corresponding setting in web GUI: Force Translation on page Interoperability

Table type: Dynamic

List domain names/IP addresses that should always be rewritten when forwarded by the Ingate.

Field Name	Field Type	Explanation
domain	UnresolvedReachableHost	The domain name.

sip.forward_cancel_body

Corresponding setting in web GUI: Forward CANCEL Body on page Interoperability

Table type: Single row

Forward packet body from incoming CANCEL to outgoing CANCEL.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.forward_to_header

Corresponding setting in web GUI: on page Interoperability

Table type: Single row

Field Name	Field Type	Explanation

sip.forward_user_agent

Corresponding setting in web GUI: Keep User-Agent Header When Acting as B2BUA on page Interoperability

Table type: Single row

Field Name	Field Type	Explanation

sip.global_policies

Corresponding setting in web GUI: URI Encoding, Default Policy For SIP Requests , Allow RFC 2069 Authentication, SIP Authentication, SIP Realm, SIP URL Encryption on pages

Interoperability, Filtering and Authentication and Accounting

Table type: Single row

Miscellaneous SIP settings.

Field Name	Field Type	Explanation
sip_policy	sip_function_sel	The default policy for SIP requests. Exceptions are made in the 'db.sip.relay_rules' table.
sipauth_allow_rfc2069	OnOffToggle	Turn on or off support for authentication according to RFC 2069.
sipauth_enabled	OnOffToggle	Turn SIP Authentication on or off.
sipauth_realm	OptString	The SIP realm to use for authentication.

sip.header_filter_default

Corresponding setting in web GUI: Default Header Filter Policy on page Filtering

Table type: Single row

Default rule for processing SIP requests based on the From and To headers.

Field Name	Field Type	Explanation
action	sip_filter_action_sel	The action to take for requests.

sip.header_filter_rules

Corresponding setting in web GUI: Header Filter Rules on page Filtering

Table type: Dynamic

Rules for processing SIP requests based on the From and To headers.

Field Name	Field Type	Explanation
action	sip_filter_action_sel	The action to take for this request.
from_header	HeaderPattern	A pattern to match the From header of the request.
number	Integer	Priority of this rule. A lower number is a higher priority.
to_header	HeaderPattern	A pattern to match the To header of the request.

sip.ignore_uri_port_when_maddr

Corresponding setting in web GUI: Ports and the maddr Attribute on page Interoperability

Table type: Single row

Ignore port in URI when an maddr parameter is present.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.large_udp

Corresponding setting in web GUI: Allow Large UDP Packets on page Interoperability

Table type: Single row

Select to allow larger UDP packets than the standard allows, instead of switching to TCP signaling.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.lcs_companion

Corresponding setting in web GUI: MEDIAtor on page MEDIAtor

Table type: Single row

Settings for the MEDIAtor.

Field Name	Field Type	Explanation
enabled	OnOffToggle	MEDIAtor function.
inside_ip	OptOwnIpReference	The MEDIAtor’s IP address on the LAN.
listen_ip	OptOwnIpReference	The IP address on which the MEDIAtor should listen for connections from the Access Proxy.
listen_port	OptPortNumber	The port on which the MEDIAtor should listen for connections from the Access Proxy.
outside_ip	OptOwnIpReference	The MEDIAtor’s IP address on the WAN.

sip.listen

Corresponding setting in web GUI: Additional SIP Signaling Ports on page Basic Settings

Table type: Dynamic

A list of additional ports for incoming SIP signaling to the Ingate.

Field Name	Field Type	Explanation
comment	OptComment	A comment field for the administrator.
port	PortNumber	The port on which to listen.
transport	sip_transport_listen_sel	The accepted SIP transports on this port.

sip.local_domains

Corresponding setting in web GUI: Local SIP Domains on page Local Registrar

Table type: Dynamic

The SIP domains that this Ingate should be registrar for.

Field Name	Field Type	Explanation
domain	DomainName	A SIP domain.

sip.loose_refer_to

Corresponding setting in web GUI: Relaxed Refer-To on page Interoperability

Table type: Single row

Accept Refer-To headers with '?' but no angle brackets.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.loose_user_name_check

Corresponding setting in web GUI: Loose Username Check on page Interoperability

Table type: Single row

Only use the username, not the domain, when authenticating.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.lr_true

Corresponding setting in web GUI: Loose Routing on page Interoperability

Table type: Single row

Select to use 'lr=true' in routing headers.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.media_encryption_policy

Corresponding setting in web GUI: Default Encryption Policy on page Media Encryption

Table type: Single row

Standard encryption settings. Exceptions are made in the 'db.sip.media_encryption_rules' table.

Field Name	Field Type	Explanation
allow_transcoding	OnOffToggle	Allow transcoding of signaling.
allowed_suites	OptMediaEncryptionSuiteReference	The crypto group allowed.

sip.media_encryption_rules

Corresponding setting in web GUI: SIP Media Encryption Policy on page Media Encryption

Table type: Dynamic

Encryption settings per interface/VLAN. Exceptions from the standard policy set in 'db.sip.media_encryption_policy'.

Field Name	Field Type	Explanation
allow_transcoding	OnOffToggle	Allow transcoding of signaling for this interface/VLAN.
allowed_suites	OptMediaEncryptionSuiteReference	The crypto group allowed via this interface/VLAN.
interface	SipMcryptoSurroundingReference	The interface/VLAN for which encryption settings are made.

sip.media_encryption_settings

Corresponding setting in web GUI: Accept RTP/AVP With sdescriptions, Media Encryption, RTP Profile, Transmit RTP/AVP With sdescriptions, Windows Messenger Encryption Offers on pages Interoperability and Media Encryption

Table type: Single row

SIP media encryption settings.

Field Name	Field Type	Explanation
accept_avp_sdescriptions	OnOffToggle	Accept RTP/AVP sdescriptions.
enabled	OnOffToggle	Turn media encryption on or off.
prefer_rtp_savp	OnOffToggle	Use RTP/SAVP descriptions.
transmit_avp_sdescriptions	OnOffToggle	Transmit RTP/AVP sdescriptions.
wm5require	OnOffToggle	Always use ’required’ for Windows Messenger signaling.

sip.media_encryption_suite

Corresponding setting in web GUI: Crypto Suite Groups on page Media Encryption

Table type: Dynamic

Grouping crypto methods.

Field Name	Field Type	Explanation
name	GroupName	A name of the crypto methods group.
suite	media_encryption_suite_sel	An encryption method.

sip.media_ports

Corresponding setting in web GUI: SIP Media Port Range on page Basic Settings

Table type: Single row

The port range the Ingate should use for SIP media.

Field Name	Field Type	Explanation
ports_lower	PortNumber	The lowest port number in the range.

Field Name	Field Type	Explanation
ports_upper	PortNumber	The highest port number in the range.

sip.media_restriction

Corresponding setting in web GUI: Limitation of sender of media streams on page Sessions and Media

Table type: Single row

Limit where SIP media can be sent from.

Field Name	Field Type	Explanation
medialock	medialock_sel	Media sender limitation.

sip.media_timeouts

Corresponding setting in web GUI: Timeout for one-way media streams, Tear down media streams at RTP/RTCP timeout, Timeout for RTP streams, Timeout for RTCP streams on page Sessions and Media

Table type: Single row

SIP media timeouts.

Field Name	Field Type	Explanation
oneway	OptPositiveSysInteger	One-way media stream timeout (seconds).
rtcp	OptPositiveSysInteger	RTCP stream timeout (seconds).
rtp	OptPositiveSysInteger	RTP stream timeout (seconds).
tear_down	OnOffToggle	Select to tear down media streams at RTP/RTCP timeout.

sip.message

Corresponding setting in web GUI: Maximum SIP packet size on page Sessions and Media

Table type: Single row

Set the maximum SIP message size that the Ingate should accept.

Field Name	Field Type	Explanation
max_message_size	MaxMessageSizeInteger	The maximum size of SIP messages.

sip.mfull

Corresponding setting in web GUI: User Matching on page Interoperability

Table type: Single row

Select to match incoming SIP requests on username and domain instead of only on username.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.mimetypes

Corresponding setting in web GUI: Content Types on page Filtering

Table type: Dynamic

A list of content types to allow or reject in SIP packets.

Field Name	Field Type	Explanation
allowed	OnOffToggle	Allow or reject packets with this content type.
mimetype	MimeType	A content type in a SIP packet.

sip.monitor_server

Corresponding setting in web GUI: SIP Servers To Monitor on page Basic Settings

Table type: Dynamic

Monitored SIP servers.

Field Name	Field Type	Explanation
port	OptPortNumber	The port to be monitored on the server.
server	UnresolvedReachableHost	The server to be monitored.
transport	OptSipTransportSel	The transport to be monitored on the server.

sip.music_on_hold

Corresponding setting in web GUI: Music on Hold Redirection on page Sessions and Media

Table type: Single row

Play music on hold.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.music_on_hold_servers

Corresponding setting in web GUI: Music on Hold Server on page Sessions and Media

Table type: Single row

The music on hold servers to use (currently no more than one).

Field Name	Field Type	Explanation
port	OptPortNumber	The port of the MOH server.
transport	OptSipTransportSel	The transport used by the MOH server.
userdomain	OptName	The IP address or SIP domain of the MOH server, optionally including user.

sip.option_timeout

Corresponding setting in web GUI: SIP blacklist interval on page Sessions and Media

Table type: Single row

SIP blacklist interval. If no value is entered, blacklisting is not used.

Field Name	Field Type	Explanation
timeout	OptionTimeout	Blacklist interval (seconds).

sip.outbound_proxy

Corresponding setting in web GUI: Outbound Proxy on page Routing

Table type: Dynamic

Where to send SIP requests. Multiple outbound proxies can be used based on the domain in the From header of the request.

Field Name	Field Type	Explanation
from_domain	SipUserDomainDefaultAll	Matches the domain part of the From header.
to_domain	UnresolvedReachableHost	IP address or SIP domain to forward the request to.
to_port	OptPortNumber	Port to forward the request to.

sip.percent20_to_whitespace

Corresponding setting in web GUI: Convert Escaped Whitespaces in URIs on page Interoperability

Table type: Single row

Turns the conversion of %20 to a real whitespace on and off in sipfw.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.preserve_2543_hold

Corresponding setting in web GUI: Preserve RFC 2543 Hold on page Interoperability

Table type: Single row

Perform Hold according to the old RFC2543.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.public_ip

Corresponding setting in web GUI: Public IP address for NATed Telecommuting Module on page Basic Settings

Table type: Single row

The public IP for a NATed Ingate box. Used in SIP signaling.

Field Name	Field Type	Explanation
ip	OptDnsReachableHost	An IP address.

sip.radius_acct

Corresponding setting in web GUI: RADIUS Accounting on page Authentication and Accounting

Table type: Single row

RADIUS accounting in the Telecommuting Module.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.recurse_on_3xx_in_b2bua

Corresponding setting in web GUI: Class 3xx Message Processing on page Routing

Table type: Single row

Enables recursion on 3xx in the B2BUA, instead of the proxy, if recursion is enabled in reply_config.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.registrar_limits

Corresponding setting in web GUI: Registrar Limits on page Local Registrar

Table type: Single row

Limitations for the built-in SIP registrar.

Field Name	Field Type	Explanation
max_registrations	MaxReg	The allowed number of registrations per user.
max_users	OptNonNegativeInteger	The allowed number of registered users.
registration_timeout	RegTimeout	Registration timeout (seconds).

sip.relay_rules

Corresponding setting in web GUI: Sender IP Filter Rules on page Filtering

Table type: Dynamic

Rules for processing SIP requests based on the source network.

Field Name	Field Type	Explanation
action	sip_function_sel	The action to take for this request.
client_netgroup	NetgroupReference	The source network of the request.

Field Name	Field Type	Explanation
number	Integer	Priority of this rule. A lower number is a higher priority.

sip.remove_via

Corresponding setting in web GUI: Remove Via Headers on page Interoperability

Table type: Dynamic

Remove Via headers from requests send to the listed servers.

Field Name	Field Type	Explanation
ip	DnsReachableHost	The server for which to remove Via headers.

sip.reply_config

Corresponding setting in web GUI: Class 3xx Message Processing on page Routing

Table type: Single row

Select if 3xx messages (redirection messages) should be forwarded to the endpoint or used in the Ingate box.

Field Name	Field Type	Explanation
class3	class3_sel	Select how to use 3xx messages.

sip.rewrite_to_for_register_in_dp

Corresponding setting in web GUI: REGISTER in Dial Plan on page Dial Plan

Table type: Single row

Rewrite To headers for REGISTER requests passed through the Dial Plan.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.ringback

Corresponding setting in web GUI: Local Ringback on page Sessions and Media

Table type: Single row

Ringback settings.

Field Name	Field Type	Explanation
action	ringback_sel	Select when ringback should be played.
tone_type	ring_tone_type_sel	Type of ring tone to play (US or UK).

sip.route180

Corresponding setting in web GUI: Remove Headers in 180 Responses on page Interoperability

Table type: Single row

Make the unit remove the Record-Route and Contact headers in 180 responses to SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.route_use_sport

Corresponding setting in web GUI: Force Remote TLS Connection Reuse on page Interoperability

Table type: Dynamic

A list of SIP servers for which the actual source port of previous TLS connections will be reused when connecting with TLS, instead of port 5061.

Field Name	Field Type	Explanation
ip	DnsReachableHost	The IP address of the server.

sip.routing_order

Corresponding setting in web GUI: SIP Routing Order on page Routing

Table type: Fixed

Prioritization of routing methods in the Ingate.

Field Name	Field Type	Explanation
function	routing_priority_sel	The routing method to be prioritized.
number	Integer	Priority number of the row. Must be unique.

sip.rroute_always

Corresponding setting in web GUI: Force Record-Route for All Requests on page Interoperability

Table type: Single row

Make the unit add a Record-Route header for all SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.rroute_outbound

Corresponding setting in web GUI: Force Record-Route for Outbound Requests on page Interoperability

Table type: Single row

Make the unit add a Record-Route header for all non-local SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.session_limits

Corresponding setting in web GUI: Allowed number of concurrent sessions, Session timer, Allowed number of media streams per SIP session on page Sessions and Media

Table type: Single row

Limitations for SIP sessions.

Field Name	Field Type	Explanation
max_sipsessions	OptNonNegativeInteger	The allowed number of concurrent sessions. If left blank, no limit is set.
max_streams_per_leg	MaxStreamsPerSession	The allowed number of media streams per SIP session.
session_timeout	SessionTimeout	Session timeout (seconds).

sip.signal_address_for_destination

Corresponding setting in web GUI: Sender IP Address Per Destination on page Routing

Table type: Dynamic

Field Name	Field Type	Explanation

sip.sip_alias

Corresponding setting in web GUI: Static Registrations on page Routing

Table type: Dynamic

Set up forwarding of SIP requests to local SIP users.

Field Name	Field Type	Explanation
alias	AliasAlias	The user to which requests should be forwarded.
sips_sel	sips_sel	Select SIP/SIPS for the forwarded request.
transport	OptSipTransportSel	Select the transport to use for forwarded requests.
user	AliasUser	The user for which requests should be forwarded.

sip.sip_errors_logclass

Corresponding setting in web GUI: Log class for SIP errors on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP errors.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.sip_license_logclass

Corresponding setting in web GUI: Log class for SIP license messages on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP license messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.sip_media_logclass

Corresponding setting in web GUI: Log class for SIP media messages on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP media messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.sip_message_logclass

Corresponding setting in web GUI: Log class for SIP packets on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP packets.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.sip_signaling_logclass

Corresponding setting in web GUI: Log class for SIP signaling on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP signaling.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.sip_verbose_logclass

Corresponding setting in web GUI: Log class for SIP debug messages on pages Basic Settings and Logging Configuration

Table type: Single row

The log class for SIP debug messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

sip.st_type

Corresponding setting in web GUI: Telecommuting Module Type on page Telecommuting Module Type

Table type: Single row

Sets the SIParator type.

Field Name	Field Type	Explanation
st_type	st_type_sel	The SIParator type.

sip.strip_ice_attributes

Corresponding setting in web GUI: Strip ICE Attributes on page Interoperability

Table type: Single row

Remove ICE attributes from SDP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.surroundings

Corresponding setting in web GUI: Surroundings on page Surroundings

Table type: Dynamic

A list of Surroundings for a DMZ SIParator. Used to group networks which are on the same side of the connected firewall.

Field Name	Field Type	Explanation
surrounding_netgroup	NetgroupReference	A Surrounding network for a DMZ SIParator.

sip.tcp_timeout

Corresponding setting in web GUI: Timeout for SIP over TCP/TLS on page Sessions and Media

Table type: Single row

Timeout for SIP connections over TCP/TLS.

Field Name	Field Type	Explanation
tcp_timeout	PositiveSysInteger	Timeout for TCP (seconds).

sip.tel_to_outbound_proxy

Corresponding setting in web GUI: tel: URIs on page Routing

Table type: Single row

Select to send all TEL URI requests to the outbound proxy.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.tls_cacerts

Corresponding setting in web GUI: TLS CA Certificates on page Signaling Encryption

Table type: Dynamic

List of CA certificates for TLS connections.

Field Name	Field Type	Explanation
ca	CaReference	A CA certificate.

sip.tls_client_cfg

Corresponding setting in web GUI: Making TLS Connections on page Signaling Encryption

Table type: Single row

Default settings for making TLS connections. Exceptions for certain IP addresses listed in ’db.sip.tls_server_cfg’.

Field Name	Field Type	Explanation
client_methods	tls_client_methods	The method to use for TLS connections initiated by the Ingate.
default_cert	OptCertReference	The X.509 certificate to use for TLS connections initiated by the Ingate.

sip.tls_server_cfg

Corresponding setting in web GUI: TLS Connections On Different IP Addresses on page Signaling Encryption

Table type: Dynamic

List of IP addresses on which to accept TLS connections. For the listed IP addresses, the corresponding certificate is also used when making TLS connections from this IP address.

Field Name	Field Type	Explanation
cert	CertReference	The certificate to use for TLS connections on this IP address.
ip	OwnIpReference	An IP address for TLS connections.
require_client_cert	OnOffToggle	Require that the client present a certificate.
server_methods	tls_server_methods	The methods to accept for connections to this IP

sip.tls_settings

Corresponding setting in web GUI: Check server domain match on page Signaling Encryption

Table type: Single row

Check that the remote certificate matches the domain.

Field Name	Field Type	Explanation
check_x509_server_subject	OnOffToggle	Turn the setting on or off.

sip.transaction_config

Corresponding setting in web GUI: Requests on page Sessions and Media

Table type: Single row

Timeouts for SIP requests.

Field Name	Field Type	Explanation
default_timeout	PositiveSysInteger	Default timeout for INVITE requests (seconds).
inv_rt	InviteRetransmitCount	Maximum number of retransmissions for INVITE requests.
max_timeout	PositiveSysInteger	Maximum timeout for INVITE requests (seconds).
ninv_rt	NonInviteRetransmitCount	Maximum number of retransmissions for non-INVITE requests.
timer_a	TimerA_Float	Base retransmission timeout for SIP requests (seconds).

sip.trusted_domain

Corresponding setting in web GUI: Trusted Domains on page Authentication and Accounting

Table type: Dynamic

A list of trusted servers and networks for the P-Asserted-Identity header.

Field Name	Field Type	Explanation
transport	trusted_domain_transport_sel	The transport used by the trusted server(s).
trusted_netgroup	NetgroupReference	A trusted server or network.

sip.uri_encoding

Corresponding setting in web GUI: URI Encoding on page Interoperability

Table type: Single row

How to encode URIs.

Field Name	Field Type	Explanation
type	uri_encoding_sel	Type of URI encoding to do.

sip.ua_register

Corresponding setting in web GUI: Registration Parameters on page SIP Accounts

Table type: Single row

Field Name	Field Type	Explanation

sip.use_cancel_body_in_ack

Corresponding setting in web GUI: Use CANCEL Body In ACK on page Interoperability

Table type: Single row

Use packet body of CANCEL in corresponding ACK.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

sip.use_rtcp_attribute

Corresponding setting in web GUI: on page Interoperability

Table type: Single row

Field Name	Field Type	Explanation

sip.use_tls

Corresponding setting in web GUI: SIP Transport on page Signaling Encryption

Table type: Single row

Select which transports should be allowed for SIP signaling.

Field Name	Field Type	Explanation
tlsconf	tlsconf_sel	Select transport method.

sipswitch.accounts

Corresponding setting in web GUI: SIP Accounts on page SIP Accounts

Table type: Dynamic

Field Name	Field Type	Explanation

sipswitch.b2bua_transfer_enable

Corresponding setting in web GUI: Local REFER Handling on page Routing

Table type: Single row

A list of criteria of when to handle REFER locally.

Field Name	Field Type	Explanation
always	OnOffButton	Always

Field Name	Field Type	Explanation
clients_lack_refer	OnOffButton	For clients that cannot handle REFER.
clients_lack_replaces	OnOffButton	For clients that cannot handle Replaces.
use_from_uri	OnOffButton	For requests with listed From URIs.
use_user_agent	OnOffButton	For requests from listed User-Agents.

sipswitch.b2bua_transfer_from_user

Corresponding setting in web GUI: From URIs For Which REFER is Handled Locally on page Routing

Table type: Dynamic

A list of the From headers for which REFER requests should be handled locally.

Field Name	Field Type	Explanation
user	AliasAlias	The From header.

sipswitch.dial_plan

Corresponding setting in web GUI: Dial Plan on page Dial Plan

Table type: Dynamic

A list of request types and how to process them.

Field Name	Field Type	Explanation
action	dp_action_sel	The action to take for this type of SIP request.
comment	OptComment	A comment field for the administrator.
enum_prefix	OptString	A prefix to add to the Request-URI before looking it up in ENUM.
enum_root	EnumReference	The ENUM root to use when performing ENUM lookups.
forward_prefix	OptString	A prefix to add to the Request-URI before it is forwarded.
forward_to	OptForwardToReference	Where to forward the SIP request.
number	Integer	The priority of this row.
reqfrom	OptRequestFromReference	The sender of the SIP request.
ruri	OptRequestToReference	The Request-URI of the SIP request.
timeclass	OptTimeclassReference	When this row is active.

sipswitch.dial_plan_enable

Corresponding setting in web GUI: Use Dial Plan on page Dial Plan

Table type: Single row

Use the Dial Plan.

Field Name	Field Type	Explanation
enabled	fallback_sel	Use the Dial Plan.

sipswitch.dial_plan_methods

Corresponding setting in web GUI: Methods in Dial Plan on page Dial Plan

Table type: Dynamic

A list of methods which should be routed using the Dial Plan.

Field Name	Field Type	Explanation
method	NonemptyString	A SIP method. Cannot be any of ACK, CANCEL, PRACK, BYE NOTIFY, UPDATE, or INFO.

sipswitch.enum_root

Corresponding setting in web GUI: ENUM Root on page Dial Plan

Table type: Dynamic

A list of ENUM roots to use.

Field Name	Field Type	Explanation
name	GroupName	The name of this ENUM root. This name is used to refer to the root in other tables.
number	Integer	The priority of this row.
root	DomainName	The ENUM root.

sipswitch.forward_to

Corresponding setting in web GUI: Forward To on page Dial Plan

Table type: Dynamic

A list of SIP destinations for the Dial Plan.

Field Name	Field Type	Explanation
account	OptAccountReference	The SIP account to use when the request is forwarded.
domain	OptUnresolvedReachableHost	The replacement domain to use when the request is forwarded.
name	GroupName	The name of this destination. This name is used to refer to the destination in other tables.
number	Integer	The priority of this row.
port	OptPortNumber	The destination port to use when the request is forwarded.
regexp	regexp	A regular expression for the Request-URI to use when the request is forwarded.

Field Name	Field Type	Explanation
transport	OptSipTransportSel	The SIP transport to use when the request is forwarded.

sipswitch.incoming_unauth

Corresponding setting in web GUI: Allow Calls From Unauthenticated Users on page Routing

Table type: Dynamic

A list of SIP users allowed to call local users for which the ’restrict_incoming’ function in ’db.sipswitch.user_routing’ is enabled.

Field Name	Field Type	Explanation
url	SipWildcardUrl	A matching From header.

sipswitch.request_from

Corresponding setting in web GUI: Matching From Header on page Dial Plan

Table type: Dynamic

A list of matchings on the From header and sending computer.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	Computer or network from which the request was sent.
domain	OptSipUserDomain	The SIP domain name in the From header.
name	NonemptyString	The name of this sender match. This name is used to refer to the sender in other tables.
regexp	regexpwithAt	A regular expression to match the From header.
transport	bypass_transport_sel	The SIP transport of the incoming request.
username	OptString	The SIP user name in the From header.

sipswitch.request_to

Corresponding setting in web GUI: Matching Request-URI on page Dial Plan

Table type: Dynamic

A list of matchings on the Request-URI.

Field Name	Field Type	Explanation
domain	OptSipUserDomain	The Request-URI domain part.
head	HeadString	The start of the Request-URI username part (when the prefix has been stripped).
min_tail_length	OptPositiveSysInteger	The minimum number of characters in the tail.

Field Name	Field Type	Explanation
name	NonemptyString	The name of this Request-URI match. This name is used to refer to the Request-URI in other tables.
prefix	OptString	The start of the Request-URI username part. The prefix is stripped when the request is forwarded.
regexp	regexpwithAt	Regular expression to match the Request-URI.
tail	rest_func_sel	The rest of the Request-URI username part (after the prefix and head).

sipswitch.user_routing

Corresponding setting in web GUI: User Routing on page Routing

Table type: Dynamic

Routing settings for calls to local SIP users.

Field Name	Field Type	Explanation
action	account_fwd_action_sel	How to process the call.
aliases	OptAliasList	Other SIP names for this user (connections etc.).
comment	OptComment	A comment field for the administrator.
forward_to	FwdToList	Where to send the call.
restrict_incoming	OnOffToggle	Select to restrict incoming calls to only local users and users defined in the ’db.sipswitch.incoming_unauth’ table.
timeclass	OptTimeclassReference	When this row is active.
user	UserReference	The user for which routing settings are made.
voice_mail	account_voice_mail_sel	When to send calls to a voice mail server.

sipswitch.users

Corresponding setting in web GUI: Local SIP User Database on page Local Registrar

Table type: Dynamic

A list of SIP users and other accounts for this Ingate.

Field Name	Field Type	Explanation
auth_name	OptString	The authentication name for the user, if different from the username.
client_netgroup	NetgroupReference	The network from which the user can register.
domain	SipUserDomain	The SIP domain for the user.

Field Name	Field Type	Explanation
password	SipUserPassword	The password for the user.
type	account_type_sel	The account type for the user.
user	SipUserName	The name of this SIP user.

sipswitch.voicemail

Corresponding setting in web GUI: Voice Mail Server on page Routing

Table type: Dynamic

A list of Request-URIs to use for sending calls to voice mail servers.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
request_uri	NoCommaString	The Request-URI to use when the call is sent to the voice mail server. The Request-URI must in some way point to the voice mail server.

userdb.radius_local_endpoint

Corresponding setting in web GUI: Contact IP Address, Identifier on page RADIUS

Table type: Single row

IP address and identifier to use when connecting to a RADIUS server.

Field Name	Field Type	Explanation
nas_identifier	NasIdentifier	A NAS-Identifier.
radius_local_ip	OptOwnIpReference	The IP address to use when contacting the RADIUS
use_nas_ip_address	OnOffToggle	Use NAS-IP-Address as identifier.

userdb.radius_servers

Corresponding setting in web GUI: RADIUS Servers on page RADIUS

Table type: Dynamic

A list of RADIUS servers to use for authentication and accounting.

Field Name	Field Type	Explanation
port	RadiusServerPort	The port of the RADIUS server.
secret	RadiusSecret	The shared secret of the RADIUS server.
server	DnsReachableHost	The IP address of the RADIUS server.

voipsm.voipsm

Corresponding setting in web GUI: General, Registrations, PSTN Numbers on page VoIP Survival

Table type: Single row

Settings for VoIP Survival.

Field Name	Field Type	Explanation
areacode	OptDigitString	The local phone area code.
cachettl	OptPositiveSysInteger	Time to store subscriber data (days).
enabled	OnOffToggle	Turns the setting on and off.
maxnrlen	OptPositiveSysInteger	The maximum number of digits in local phone numbers (not including area code).
registration_time	OptPositiveSysInteger	Registration time for clients during survival mode (seconds).
timeout	OptPositiveSysInteger	How often the servers are checked (seconds).

voipsm.voipsm_domains

Corresponding setting in web GUI: Domains To Monitor on page VoIP Survival

Table type: Dynamic

A list of the domains monitored for VoIP Survival.

Field Name	Field Type	Explanation
domain	DomainName	The SIP domain to be monitored.
user_data_method	voipsm_method_sel	The method to use when requesting user information.

voipsm.voipsm_pstn_gateways

Corresponding setting in web GUI: PSTN Gateways on page VoIP Survival

Table type: Dynamic

A list of PSTN gateways to use when in Survival mode.

Field Name	Field Type	Explanation
gateway	UnresolvedReachableHost	A PSTN gateway.

Field Types

Here, all field types used in the tables are listed. For **selection** types, you can only use the listed keywords. Note that the CLI is case sensitive!

AdminPassword

A password for an admin user.

AdminTypeSel

A list of administrator account types.

Selection	Explanation
off	The user is disabled.
ro	The user can view any configuration and make log searches, but cannot change any configuration.
debug	The user can take packet captures, download support reports, and view internal dump pages.
bk	The user can download the configuration to file, and upload a configuration file to the Ingate. The user is also allowed to apply configurations.
rw	The user can make any changes to the configuration.
vpn	The user can make any changes in the VPN settings and apply configurations, but cannot change any other configuration.
sip	The user can make any changes in the SIP settings and apply configurations, but cannot change any other configuration.
vpnreneg	The user is allowed to press the ’Renegotiate IPsec tunnels’ button in the GUI to negotiate new IPsec tunnels, but cannot change any configuration.

AdminUser

adminuser&-d;

AliasAlias

A SIP URI/username (including domain).

AliasIpReference

AliasUser

A SIP URI/username (including domain).

AuthData

Authentication data for IPsec peers. The first character of the secret column determines the type of the secret: ’s’: Shared secret (aka PSK, pre-shared key). ’x’: X.509 certificate in PEM format. ’a’: The name of an X.509 CA certificate. ’c’: X.509 Distinguished Name.

AuthtypeSel

A selection of IPsec authentication methods.

Selection	Explanation
psk	A shared secret.
x509	An X.509 certificate.
x509ca	A trusted CA.
x509ca_dn	A trusted CA, with added Distinguished Name for the peer.

CaReference

A reference to the ’name’ field of ’db.cert.cas’. In other words, a CA certificate.

CertReference

A reference to one of the Ingate’s private certificates.

CryptoDefReference

DepUsableVlanInterface

DnsDynIpAddress

A datatype for DNS/ipaddr values. The address may be dynamically assigned.

DnsDynIpNetwork_Interface

DnsDynIpOtherHost

A DNS name or IP address that does not belong to this unit, but is on a directly connected network. A ’*’ wildcard can be used, meaning that the default gateway will be used when the unit gets a DHCP/PPPoE IP address.

DnsDynIpReachableHost

A DNS name or IP address that does not belong to this unit. A ’*’ wildcard can be used, meaning that this information will be provided when the unit gets a DHCP/PPPoE IP address.

DnsIpAddress

A datatype for DNS/ipaddr values.

DnsIpNetwork_Filter

A datatype for DNS/ipaddr and netmask values. DEMAND_FILTER: The host part must be all zeroes.

DnsReachableHost

A DNS name or IP address that does not belong to this unit.

DomainGroup

SIP domain group.

DomainName

Datatype used for domain names.

DyndnsPassword

A password for a DynDNS user.

DyndnsServiceSel

A selection of DynDNS services.

Selection	Explanation
dyndns	Dynamic DNS.
statdns	Static DNS.
custom	Custom DNS.

EnumReference

A reference to the ’name’ field of ’db.sipswitch.enum_root’. In other words, an ENUM root.

EspCryptoReference

FirewallLogclassReference

A reference to the ’name’ field of ’db.monitor.logclasses’. In other words, a log class.

FwdToList

A list of SIP addresses separated by comma.

GroupName

Datatype used as name of groups.

HeadString

A string to define the Head of the SIP URI. Without a SIP Trunk or Advanced SIP Routing module, the only allowed characters are ’1234567890+-#*’.

HeaderPattern

A SIP URI header. Can contain wildcards.

IDSIPSLogclassReference

A reference to the ’name’ field of ’db.monitor.logclasses’. In other words, a log class.

IkeCryptoReference

Integer

An integer, possibly within a specified interval. This class specifies no limits, so any integer is OK. Subclasses can specify the interval by setting either or both of _MIN and _MAX.

InterfaceSel

Select one of the installed physical interfaces. This behaves as if it were a reference to the ’interface’ column on ’db.network.interfaces’.

InviteRetransmitCount

An integer between 1 and 16.

IpsRuleName

Datatype used for rate limited IPS rule names.

IpsecAuthSel

Selection	Explanation

IpsecEncSel

Selection	Explanation

IpsecNetLocalSel

A selection of which local IP addresses can use the IPsec connection.

Selection	Explanation
exact	The exact network selected.
peerip	The IP address used for the negotiation.

IpsecNetRemoteSel

A selection of which remote IP addresses can use the IPsec connection.

Selection	Explanation
exact	The exact network selected.
subset	The network selected, or a subset of the network.
peerip	The IP address used for the negotiation.
private	One IP address from the private IP address ranges.
peerip/private	One IP address from the private IP address ranges, or the IP address used for the negotiation.

IpsecPeer_Group

A reference to the ’name’ field of ’db.ipsec.peers’. In other words, an IPsec peer.

IpsecSALife

An integer between 60 and 172800.

IsakmpGroupSel

Selection **Explanation**

IsakmpSALife

An integer between 60 and 172800.

LogclassReference

A reference to the 'name' field of 'db.monitor.logclasses'. In other words, a log class.

MaxMessageSizeInteger

An integer between 1024 and 67108864.

MaxReg

An integer between 1 and 100.

MaxStreamsPerSession

An integer between 1 and 10.

MimeType

A MIME type. The format is 'type/name'. The '*' wildcard is accepted to use as a type/name.

Name

Datatype used for names. Names must not be empty, and must not be a dash ('-').

NasIdentifier

A NAS-Identifier string, as defined in RFC 2138.

NetgroupReference

A reference to the 'name' field of 'db.firewall.network_groups'. In other words, the name of a group defined in the Networks and Computers table.

NoCommaString

A string. The comma character (',') is not allowed.

NonInviteRetransmitCount

An integer between 1 and 32.

NonWhiteName

Datatype used for names without whitespace. Names must not be empty, a dash ('-'), or contain whitespace.

NonemptyString

A string.

OnOffButton

An On-Off-toggle displayed as a check-box in the web server. The only reason this is a separate datatype, is to fool the web server into displaying it as a check-box, as there is currently no way to specify this in the OEM package.

OnOffToggle

Datatype with only allowed values being "on" and "off". Case is ignored, as is leading and trailing whitespace. The cooked value is a bool: True for "on" and False for "off". Default "off".

OnOffToggleOn

Identical to OnOffToggle, except default value is "on".

OptAccountReference

A reference to an account defined in ’db.sipswitch.users’. The reference is written on the form ’accountname@domain’.

OptAliasList

An optional list of SIP user names.

OptAliasIpReference

An optional reference to the ’name’ field of ’db.network.alias_addresses’. In other words, one of the machine’s own IP alias addresses.

OptBandWidth

An optional integer with a minimum value of 12.

OptCertCrl

An optional X.509 CRL.

OptCertReference

An optional reference to one of the Ingate’s private certificates.

OptCertificate

An optional X.509 certificate.

OptCodecTypeSel

Selection	Explanation
audio	An audio type codec.
video	A video type codec.
text	A text type codec.
application	An application type codec.

OptComment

An optional comment field for user consumption only.

OptDSCPInteger

An optional integer between 0 and 63.

OptDepOwnIpReference

An optional reference to the 'name' field of 'db.network.interfaces' or 'db.network.alias_addresses'. In other words, one of the machine's own IP addresses.

OptDepString

An optional string.

OptDigitString

Optional string that may only contain numeric data. This may be practical e. g. when storing telephone numbers that may start with 0.

OptDnsAutoRuntimeReachableHost

OptDnsIpAddress

A datatype for optional DNS/ipaddr values. Note: the DNS lookup is performed by the client of dbserver, such as the web server or CLI process. This ensures that the dbserver process is never blocked for long periods of time. Derived classes may define the following attributes: _OPTIONAL -- True if the network is optional. DYNAMIC -- True if the IP address may be DYNAMIC_IP_STR. Exactly what it means is not specified here.

OptDnsReachableHost

An optional DNS name or IP address that does not belong to this unit.

OptDomainName

Datatype used for optional domain names.

OptExtraGwReference

OptForwardToReference

A reference to the ’name’ field of ’db.sipswitch.forward_to’. In other words, a destination for the SIP request.

OptIcmpRangeList

An optional list of ICMP numbers.

OptIpsecNetReference

A reference to the ’name’ field of ’db.ipsec.ipsec_nets’. In other words, an IPsec network.

OptIpsecPeerReference

A reference to the ’name’ field of ’db.ipsec.peers’. In other words, an IPsec peer.

OptMediaEncryptionSuiteReference

Refers to the ’name’ field in ’db.sip.media_encryption_suite’.

OptName

Datatype used for optional names.

OptNetgroupReference

Optional reference to the ’name’ field of ’db.firewall.network_groups’. In other words, the name of a group defined in the Networks and Computers table.

OptNonNegativeInteger

A positive or zero integer.

OptNonWhiteString

An optional string with no whitespace allowed.

OptOnOffToggle

OptOnOffToggleOn

Identical to OnOffToggle, except default value is "on".

OptOwnIpReference

An optional reference to the ’name’ field of ’db.network.interfaces’ or ’db.network.alias_addresses’. In other words, one of the machine’s own IP addresses.

OptPacketSize

A optional packet size in the range 1-65535 bytes.

OptPassword

Datatype for optional passwords.

OptPercent

An optional integer from nothing to everything in percent (0-100).

OptPercentFloat

An optional float from nothing to everything in percent (0-100). Values are normalized to integers if possible.

OptPortNumber

A optional port number in the range 1-65535. Zero not normally allowed.

OptPortRangeList

An optional list of TCP or UDP ports.

OptPositiveSysInteger

An optional strictly positive integer that fits in an "int".

OptPrivCert

A datatype for optional private key/certificate pairs. The cooked value can be either of: - an fuegoutils.x509.privcert object, possibly with an extra "req" attribute that is an fuegoutils.x509.request object. - an fuegoutils.x509.privreq object. - FieldError - None (only if the datatype is optional)

OptProtocolRangeList

An optional list of protocol numbers.

OptRequestFromReference

A reference to the ’name’ field of ’db.sipswitch.request_from’. In other words, a matching From header.

OptRequestToReference

A reference to the ’name’ field of ’db.sipswitch.request_to’. In other words, a matching Request-URI.

OptServicesReference

An optional reference to the ’name’ field of ’db.firewall.services’. In other words, a defined service.

OptSipTransportSel

Selection	Explanation
tcp	Use TCP as transport.
udp	Use UDP as transport.
tls	Use TLS as transport.

OptSipUserDomain

An optional domain name or IP address. The '*' wildcard can be used, meaning any SIP domain. '*local' means any SIP domain for which this Ingate acts as registrar.

OptString

An optional string. Unlike most other optional types, the cooked value when no value is given isn't None. It is the empty string. Subclasses may override CHARSET to specify a character set the string must be able to be encoded as. (Note that the cooked value is always UTF-8, regardless of CHARSET).

OptTimeclassReference

A reference to the 'name' field of 'db.firewall.timeclasses'. In other words, the name of a time class.

OptUnresolvedReachableHost

An optional DNS name or IP address that does not belong to this unit.

OptVlanId

An integer between 1 and 4094.

OptVlanIfReference

An optional reference to a defined VLAN or interface, with an internal key. A VLAN will look like 'eth0.27' where eth0 is the physical interface for which this VLAN is defined, and 27 is the number assigned to this VLAN. An interface will look like 'eth2', where eth2 is the name of the physical interface.

OptionTimeout

An integer between 0 and 600.

OwnIpReference

A reference to the 'name' field of 'db.network.interfaces' or 'db.network.alias_addresses'. In other words, one of the machine's own IP addresses.

PPTPNetgroupReference

Optional reference to the 'name' field of 'db.firewall.network_groups'. In other words, the name of a group defined in the Networks and Computers table. The reference is not optional if 'db.pptp.pptp_enable' is on.

PPTPOwnIpReference

An optional reference to the ’name’ field of ’db.network.interfaces’ or ’db.network.alias_addresses’. In other words, one of the machine’s own IP addresses. The reference is not optional if ’db.pptp.pptp_enable’ is on.

Percent

An integer from nothing to everything in percent (0-100).

PfsGroupSel

Selection	Explanation

PortNumber

A port number in the range 1-65535. Zero not normally allowed.

PositiveSysInteger

A strictly positive integer that fits in an "int".

PptpPassword

A password for a PPTP user.

QoSClassReference

A reference to the ’name’ column of ’db.qos.classes’. In other words, a QoS class.

RadiusSecret

A RADIUS server secret.

RadiusServerPort

A port number. The default value is 1812.

RegTimeout

An integer between 1 and 36000.

RouteDestination

routedest&-d;

RoutePriority

An optional integer between 1 and 9.

SIPLogclassReference

A reference to the ’name’ field of ’db.monitor.logclasses’. In other words, a log class.

SIPRadiusSel

A selection of SIP user databases.

Selection	Explanation
local	A local database.
radius	A RADIUS database.

SessionTimeout

An integer between 90 and 86400.

SipLocalUserReference

SipMcryptoSurroundingReference

A reference to an interface or defined surrounding. For DMZ SIParators, the reference is made to a surrounding; the 'surrounding_netgroup' field in 'db.sip.surroundings'. For all other types, the reference is made to a defined VLAN or interface, as referred to in 'OptVlan-IfReference'.

SipMethod

A SIP method (uppercase).

SipMethodsReference

A reference to the 'method' field of 'db.sip.auth_methods'. In other words, a SIP method.

SipTransportSel

Selection	Explanation
tcp	Use TCP as transport.
udp	Use UDP as transport.
tls	Use TLS as transport.

SipUserDomain

A domain name or IP address. The '*' wildcard can be used, meaning any SIP domain. '*local' means any SIP domain for which this Ingate acts as registrar.

SipUserDomainDefaultAll

A domain name or IP address. The default value for this field is '*'.

SipUserName

A SIP user name.

SipUserPassword

A password for a SIP user.

SipWildcardUrl

SIP URL with wildcards. ? represents any single character while * represents a string of characters of any length. * is only allowed first, last and just before or after @.

SnmpPassword

A password for a SNMP v3 user.

SubGroup

A reference to another group in the same table. The default is to reference the column ’name’, but a subclass may set the class attribute REFERRED_COLUMN to specify another column. REFERRED_TABLE must not be touched. See class OptReference for additional attributes that may be set.

Time_HH_MM

A time of day (00:00 <= value <= 24:00). The cooked value is a tuple (h, m, s) where h, m and s are ints representing hour, minute and second. s will always be 0. Since 24:00 is acceptable, we cannot use the standard time class from the datetime module introduced in Python 2.3.

TimerA_Float

A number between 0.1 and 16.0.

UaRegisterInteger

UnresolvedReachableHost

A DNS name or IP address that does not belong to this unit.

VPNLogclassReference

A reference to the ’name’ field of ’db.monitor.logclasses’. In other words, a log class.

VlanId

An integer between 1 and 4094.

VlanIfReference

WildcardIdentifier

Identifier, or wildcard "*".

account_fwd_action_sel

A selection of actions to take for SIP requests.

Selection	Explanation
reject	Reject the request.
forward	Forward the request to listed users, not to the original user.
parallel	Forward the request to the original user and all listed users.
sequence	Forward the request to the original user, then to listed users in sequence.
random	Forward the request to a randomly selected user among the listed and original users. If there is no response a new user is selected to forward the request to.

account_type_sel

A selection of SIP user account types.

Selection	Explanation
user	A standard SIP user.
reg	A registration account. The Ingate registers the user with the server managing that domain.
xf	A forwarding account. The Ingate replaces the From header in the incoming request with the username and domain of this user. The request is then forwarded to the address entered in the ’db.sipswitch.dial_plan’ table.
xf+reg	A combination of the ’xf’ and ’reg’ accounts.
domain	An authentication account. When this account is used, the Ingate will respond with authentication details to authentication requests from the domain.
mr	A B2BUA account. The Ingate replaces the From header as for an ’xf’ account. The SDPs are rewritten to make SIP media always go via the Ingate.
mr+reg	A combination of the ’mr’ and ’reg’ accounts.

account_voice_mail_sel

A selection of when to forward calls.

Selection	Explanation
on	Always.
after5	After 5 seconds.
after10	After 10 seconds.
after15	After 15 seconds.
after25	After 25 seconds.
busy	When busy.
busy5	When busy or after 5 seconds.
busy10	When busy or after 10 seconds.
busy15	When busy or after 15 seconds.

Selection	Explanation
busy25	When busy or after 25 seconds.

add_expire_header_sel

A selection of when to perform certain actions based on the SIP request.

Selection	Explanation
always	Always perform this action.
never	Never perform this action.
if_in_request	Only perform this action when the request matched certain criteria.

autoneg_sel

Selection	Explanation
auto	Automatic negotiation.
100half	Use 100 Mbit/s, half duplex.
100full	Use 100 Mbit/s, full duplex.
10half	Use 10 Mbit/s, half duplex.
10full	Use 10 Mbit/s, full duplex.

blind_sel

A selection of policies for traffic to the Ingate.

Selection	Explanation
discard	Drop the packets silently.
reject	Drop the packets and send an ICMP message back.
policy	Drop packets according to the policy selected in the 'db.firewall.ping_policy' table.

bypass_transport_sel

A selection of SIP transports.

Selection	Explanation
tcp	TCP.
udp	UDP.
any	Any SIP transport.
tls	TLS.
tcp,tls	TCP or TLS.

class3_sel

Selection	Explanation
all	Send all messages on.

Selection	Explanation
recurse	Use the information in the messages locally.

config_auth_sel

A selection of authentication types for configuring the unit.

Selection	Explanation
local	A local database.
radius	A RADIUS database.
any	Use the local database as well as the RADIUS database.

dp_action_sel

A selection of forwarding actions.

Selection	Explanation
fwd	Forward the request to the selected destination.
a+fwd	Authenticate, then forward the request.
enum/a+allow	Look up destination in ENUM, then authenticate and allow the request.
deny	Reject the request.
enum/a+fwd	Look up destination in ENUM, then authenticate and forward the request.
enum/fwd	Look up destination in ENUM, then forward the request.
a+enum/a+allow	Authenticate and look up destination in ENUM, then authenticate again and allow the request.
enum/allow	Look up destination in ENUM, then allow the request.
allow	Allow the request.
a+enum/a+fwd	Authenticate and look up destination in ENUM, then authenticate again and forward the request.
a+allow	Authenticate, the allow the request.

fallback_sel

A selection of dial plan modes.

Selection	Explanation
off	Turned off.
on	Turned on.
fallback	Used if nothing else matches.

fent_keepalive_sel

A selection of how to keep bindings for fented clients alive.

Selection	Explanation
options	Send OPTIONS.

Selection	Explanation
registrations	Lower REGISTER expire.
both	Use both short registrations and OPTIONS.

function_sel

A selection of policies for traffic through the Ingate.

Selection	Explanation
discard	Drop the packets silently.
reject	Drop the packets and send an ICMP message back.
accept	Allow the packets.

fwtype_sel

A selection of the firewall types in the Ingate.

Selection	Explanation
dynamic	Dynamic session management.
static	Packet filtering.
ftp	Dynamic FTP management.
pptp	Dynamic PPTP management.
rtsp	Dynamic RTSP management.
tftp	Dynamic TFTP management.

hits_number

A positive integer with standard value 30.

media_encryption_suite_sel

A selection of the crypto algorithms which the Ingate can handle.

Selection	Explanation
cleartext	The media is unencrypted.

medialock_sel

Media stream limitation options.

Selection	Explanation
any	Allow multiple sender IP addresses and ports.
lock	Lock IP address and port to first sender.
any_restricted	Only allow receiving IP address, but multiple ports.

opttos_sel

A selection of TOS values. The field can also be set to ’-’.

Selection	Explanation
empty	The TOS field is not set.
md	The TOS field is set to Minimize Delay.
mt	The TOS field is set to Maximize Throughput.
mr	The TOS field is set to Maximize Reliability.

ping_policy_sel

A selection of the ping policies that can be used by the Ingate.

Selection	Explanation
local	Only reply to ping from units on the same interface.
never	Never reply to ping.
always	Reply to ping on all IP addresses.

policy_sel

A selection of policies for blocked traffic.

Selection	Explanation
discard	Drop the packets silently.
reject	Drop the packets and send an ICMP message back.

pqueue_sel

A selection of priority queues.

Selection	Explanation
prio1	Priority queue 1 (highest).
prio2	Priority queue 2.
prio3	Priority queue 3.
prio4	Priority queue 4.
prio5	Priority queue 5.
prio6	Priority queue 6.
prio7	Priority queue 7.
prio8	Priority queue 8 (lowest).

qostype_sel

Type of QoS to use.

Selection	Explanation
priority	Use strict priority queues.
dynamic	Use dynamic bandwidth allocation.

regexp

regexp&-d;

regexpwithAt

A regular expression, which requires exactly one @.

rest_func_sel

A selection of SIP URI tails.

Selection	Explanation
telchar	0-9, +, -, #, *
digit	0-9.
nothing	No tail.
alpha	a-z, A-Z.
alnum	a-z, A-Z, 0-9.
anychar	Any character.
xdigit	0-9, a-f, A-F (hexadecimal numbers).

rfc2782priority

An integer between 0 and 65535.

rfc2782weight

An integer between 0 and 65535.

ring_tone_type_sel

A selection of ring tone type.

Selection	Explanation
us	US ring tone.
uk	UK ring tone.

ringback_sel

A selection of when to play ringback RTP to transferee.

Selection	Explanation
never	Never play ringback RTP to transferee.
if_transfer_target_rings	Plays ringback RTP if transfer target rings.
if_transferer_hangs_up	Play ringback RTP if transferer hangs up.

routing_priority_sel

A list of different routing methods in the Ingate.

Selection	Explanation
dns_override	Use the 'db.sip.external_relay' table.

Selection	Explanation
registrar	Use the local registrar, including the ’db.sip.sip_alias’ table.
dialplan	Use the ’db.sipswitch.dial_plan’ table.

sip_auth_dir_sel

Selection	Explanation
in	Requests for local domains.
out	Requests for other domains.
both	All requests.

sip_filter_action_sel

Selection	Explanation
process	Allow the request.
reject	Reject the request.

sip_function_sel

A selection of which SIP requests to process, based on the Request-URI domain.

Selection	Explanation
proxy	Process all requests.
process	Only process requests to domains local to this unit.
reject	Process no requests.

sip_sel

A selection of traffic types.

Selection	Explanation
nonsip	Non-SIP traffic.
signaling	SIP signaling.
media	SIP media.

sip_transport_listen_sel

A selection of transports for SIP signaling.

Selection	Explanation
tcp	TCP.
udp	UDP.
udp,tcp	UDP and TCP.
tls	TLS.

sips_sel

Selection	Explanation
sip	Use ’SIP’ in the Request-URI.
sips	Use ’SIPS’ in the Request-URI.

snmptrapversion_sel

A selection of SNMP versions.

Selection	Explanation
v1	Version 1.
v2c	Version 2c.

snmpv3_auth_sel

A selection of authentication algorithms. - sha-1 -- SHA-1.

Selection	Explanation
md5	MD5.

snmpv3_privacy_sel

A selection of encryption algorithms.

Selection	Explanation
des	DES encryption.
none	No encryption.

st_type_sel

A selection of the SIParator types available.

Selection	Explanation
DMZ	DMZ type. Uses only one interface.
DMZ/LAN	DMZ/LAN type. Uses two or more interfaces.
standalone	Standalone type. Uses two or more interfaces.

syslogfacility_sel

A selection of syslog facilities.

Selection	Explanation
Kern	Kernel.
User	User.
Mail	Mail.
Daemon	Daemon.
Auth	Auth.
Lpr	Lpr.
News	News.
Uucp	Uucp.

Selection	Explanation
Cron	Cron.
Local0	Local0.
Local1	Local1.
Local2	Local2.
Local3	Local3.
Local4	Local4.
Local5	Local5.
Local6	Local6.
Local7	Local7.

sysloglevel_sel

A selection of syslog levels.

Selection	Explanation
Emerg	Emergency.
Alert	Alert.
Crit	Critical.
Err	Error.
Warning	Warning.
Notice	Notice.
Info	Informational.
Debug	Debug messages.

tls_client_methods

A selection of encrypted TCP methods, seen from the client end.

Selection	Explanation
SSLv2:SSLv2,SSLv3,TLSv1	Any method, use SSLv2 hello.
SSLv2:SSLv3,TLSv1	SSLv3 or TLSv1, use SSLv2 hello.
SSLv2:TLSv1	TLSv1, use SSLv2 hello.
SSLv3:SSLv3	SSLv3, use SSLv3 hello.
TLSv1:TLSv1	TLSv1, use TLSv1 hello.

tls_server_methods

A selection of encrypted TCP methods, seen from the server end.

Selection	Explanation
SSLv2,SSLv3,TLSv1:SSLv2,SSLv3,TLSv1	Any method.

Selection	Explanation
SSLv2,SSLv3,TLSv1:SSLv3,TLSv1	SSLv3 or TLSv1.
SSLv2,SSLv3,TLSv1:TLSv1	TLSv1, backwards-compatible.
SSLv3:SSLv3	SSLv3.
TLSv1:TLSv1	TLSv1.

tlsconf_sel

A selection of transport methods.

Selection	Explanation
no_tls	UDP or TCP.
allow_tls	UDP, TCP, or TLS.
only_tls	Only TLS.

trusted_domain_transport_sel

A selection of transports for SIP signaling.

Selection	Explanation
any	TCP or TLS.
tcp	TCP.
tls	TLS.

uri_encoding_sel

URI encoding options.

Selection	Explanation
encrypt	Always encrypt URIs.
db	Store URI and generate random username, only when needed.
escape	Escape URIs as usernames, only when needed.
preserve_db	Store URI and preserve username, only when needed.

voipsm_method_sel

A selection of codings to request extra user information with REGISTER messages.

Selection	Explanation
generic	A generic XML coding.
Broadsoft	A Broadsoft specific XML coding.

weekday_sel

The days of the week.

Selection	Explanation
monday	Monday
tuesday	Tuesday
wednesday	Wednesday
thursday	Thursday
friday	Friday
saturday	Saturday
sunday	Sunday

window_number

A positive integer with standard value 60.

CLI command examples

In this section, you can find some examples of how to use the CLI commands to create and change your configuration.

The CLI commands can be entered directly via the serial console or an ssh connection to the Telecommuting Module configuration interface. You can also enter all commands in a text file and upload it via the Telecommuting Module web GUI.

Add and change firewall rules

To add new firewall rules, you first need network definitions for the networks that will send and receive the traffic. These are made in the **firewall.netdefs** table.

If you just want to add rows to an existing configuration, use the **add-row**. If you want to remove old configuration in this table first, use the **clear-table** command before you start adding rows. This example will remove old networks and then add two new network rows:

```
clear-table firewall.netdefs

add-row firewall.netdefs interface=eth3 lower_ip=10.5.1.0 name=LAN subgroup=- upper_ip=10.5.1.255

add-row firewall.netdefs interface=eth0 lower_ip=0.0.0.0 name=internet subgroup=- upper_ip=255.255.255.255
```

After that, the firewall rule can be added to the **firewall.forwarding_rules** table. Here too, the **clear-table** command can be used to remove all old rules.

The commands below clears the table and adds two firewall rules for traffic from the LAN to the Internet.

```
clear-table firewall.forwarding_rules

add-row firewall.forwarding_rules (id 4) client=LAN comment="" enabled=on fromtunnel=- function=accept logclass=Local number=3 server=internet service=tcp timeclass=24/7 totunnel=-
```

```
add-row firewall.forwarding_rules (id 4) client=LAN comment="" enabled=on fromtunnel=- function=accept logclass=Local number=3 server=internet service=udp timeclass=24/7 totunnel=-
```

Apply a configuration

You can use CLI commands to apply the changed settings. Note that you need to perform approximately the same steps as when you apply in the web GUI; first start a test run (corresponds to pressing the **Apply configuration** button in the web GUI), and then confirm it (corresponds to pressing the **Save configuration** button on the test run page). If you need to test the new configuration for a longer period than you originally set as the test mode duration, you can enter a command to extend the test run (corresponds to pressing the **Continue test run** button on the test run page).

This command sequence will start a test run with a test mode duration of 200 seconds, then extend the test run and finally confirm it.

```
start-testrun 200
continue-testrun
confirm-testrun
```

Part V. Appendices

In the appendices, you find more thorough information about Internet and computer security, such as descriptions of Internet services and lists of Internet protocols.

Appendix A. More About SIP

The SIP Protocol

SIP (Session Initiation Protocol), defined in RFC 3261 (with various extensions), handles creation, modification and termination of various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP also supports user mobility by allowing registration of a user and proxying or redirecting requests to the user's current location. This is performed by the user registering his presence at a machine with the central registrar. The SIP registrar keeps track of the user, but doesn't hold any information about which media streams the computers or clients can manage. This is negotiated between the parts when initiating a SIP session.

Why use SIP?

Today, two protocols for transmitting IP telephony exist; SIP and H.323. The H.323 protocol was originally designed for video conferences over ISDN and is a mix of several protocols and standards for performing the various phases of a connection. The SIP protocol was designed for general session initialization over the Internet.

Both protocols have the disadvantage (from a firewall point of view) of needing dynamically allocated ports for the data transmission, but today no protocol supports tunneling random media streams.

When comparing the two protocols, there is one major drawback to the H.323 protocol: its lack of scalability. H.323 is mostly used in small LANs. When extending to world-wide IP networks, SIP has many advantages:

- Loop detection

  When trying to locate a user over several domains, loops can occur. H.323 has no support for loop detection, which can cause network overload.

  Loops are easily detected using SIP headers, as they specify all proxies that have handled the SIP packet.

- Distributed control

  H.323 uses gatekeepers, which are devices used for handling call states and redirecting calls to aliases. As every call is carried out statefully, the gatekeepers must keep a call state during the entire call. This of course makes the gatekeepers a major bottleneck in the system.

  There is also a need for a central point when performing multi-user calls, which means that someone must provide this central point, and that this machine must be dimensioned for the size of the call.

  SIP sessions are completely distributed, making the need of these central points disappear.

- Small connection overhead

  Establishing a connection using H.323 takes about three times the data and turnarounds compared to when using SIP.

Apart from this, there are some more disadvantages with H.323. As it uses many protocols, more ports need to be opened in a firewall to enable H.323 signaling through. SIP is a single protocol, which means that only one port has to be opened for SIP signaling. For both protocols, however, more ports must be opened for the data traffic.

SIP runs on both TCP and UDP (and, in fact, can be extended to run on almost any transport protocol), making it possible to use UDP for large servers, thereby enabling stateless sessions. H.323 only runs on TCP, which as already stated loads the servers by requiring state management.

SIP and Firewalls

When trying to use SIP through a firewall, there are some problems.

SIP initiates sessions of other protocols. This means that when a SIP session has been started, various other protocols are used as well, usually transmitted over TCP or UDP on some port. For a firewall, this is a problem, as it often opens up certain protocols and ports in advance, but now you don't know which ports to open. To handle SIP through a firewall which doesn't understand the SIP concept, all ports must be open all the time, which would make the firewall somewhat unnecessary. A firewall that understands SIP can open up the ports for the right protocols just when the SIP traffic needs it.

In the SIP headers there is a lot of information concerning what IP addresses the session participants use. This is a problem if a SIP session should be established through a firewall using NAT. The IP address on the hidden side (which appears in the SIP headers) won't be the same as the one that clients on the outside should use.

Managing Your Own SIP Domain

If you want to use your own SIP domain, there are some things you need to configure in order to make everything work nicely.

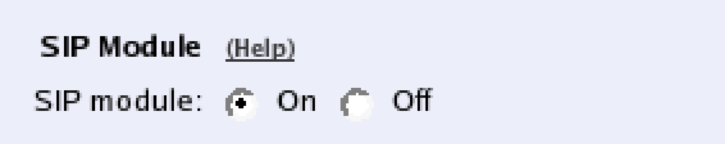
- The Telecommuting Module needs to be configured to handle the SIP domain.
- If you use a separate PBX/registrar, this must also be configured to handle the SIP domain.
- The DNS server managing your main domain should be updated with records for the SIP domain.
- The SIP clients used by users on this domain need to be configured.

Configuring the 3Com VCX IP Telecommuting Module

The Telecommuting Module only needs configuration to forward SIP requests to your registrar. This configuration guide assumes that the PBX is located on your LAN.

You can do this by using the Ingate *Startup Tool*, which can be downloaded from http://www.ingate.com/Startup_Tool.php. Below you find the configuration that should be made manually if you do not use the Tool.

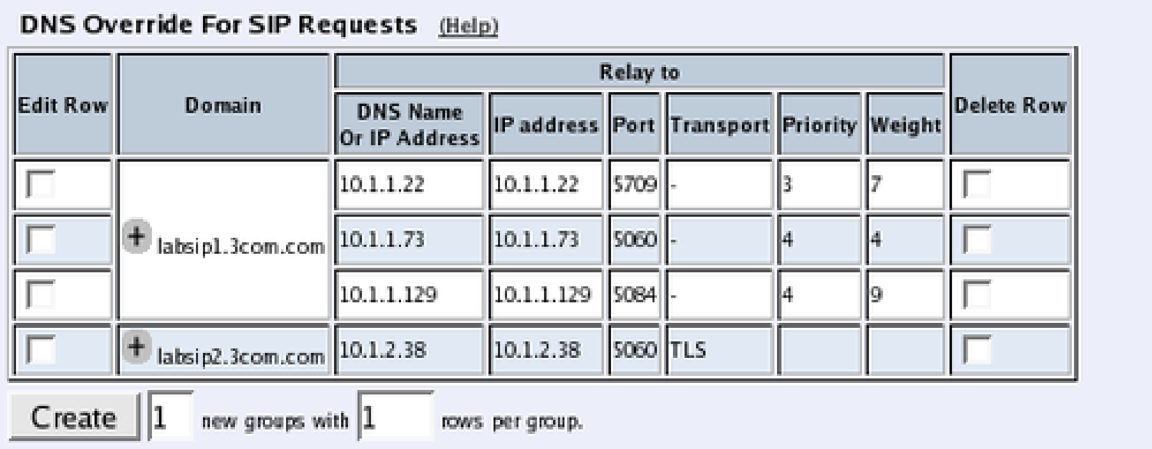
Go to the **Basic Settings** page under **SIP Services** and switch the SIP module on.



SIP Module (Help)

SIP module: ● On ○ Off

Go to the **Routing** page under **SIP Traffic**. In the **DNS Override For SIP Requests** table, add a row where you enter your SIP domain as the Domain, and enter your PBX/registrar IP address and port. You can also select which transport should be used when forwarding SIP requests to the PBX.

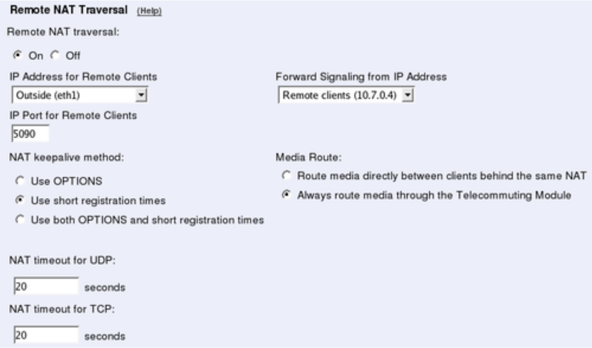


DNS Override For SIP Requests (Help)

Edit Row	Domain	Relay to						Delete Row
		DNS Name Or IP Address	IP address	Port	Transport	Priority	Weight	
□	+ labsip1.3com.com	10.1.1.22	10.1.1.22	5709	-	3	7	□
□		10.1.1.73	10.1.1.73	5060	-	4	4	□
□		10.1.1.129	10.1.1.129	5084	-	4	9	□
□	+ labsip2.3com.com	10.1.2.38	10.1.2.38	5060	TLS			□

Create 1 new groups with 1 rows per group.

If you have remote users behind NAT boxes, you also need to configure **Remote SIP Connectivity** under **SIP Services**. Use the built-in STUN server and/or the Remote NAT Traversal. It is recommended to use the Remote NAT Traversal, as it works for more clients and more NAT types.



Remote NAT Traversal (Help)

Remote NAT traversal:

● On ○ Off

IP Address for Remote Clients: Outside (eth1)

Forward Signaling from IP Address: Remote clients (10.7.0.4)

IP Port for Remote Clients: 5090

NAT keepalive method:

○ Use OPTIONS
● Use short registration times
○ Use both OPTIONS and short registration times

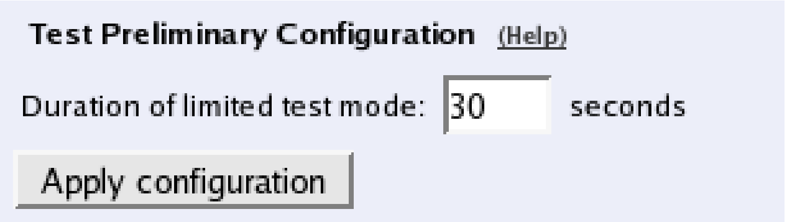
Media Route:

○ Route media directly between clients behind the same NAT
● Always route media through the Telecommuting Module

NAT timeout for UDP: 20 seconds

NAT timeout for TCP: 20 seconds

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.


Test Preliminary Configuration (Help)
Duration of limited test mode: 30 seconds
Apply configuration

Configuring the PBX

The PBX must be configured to accept registrations for your SIP domain. How you do this depends on the PBX you are using. Some PBX:s accept all domains.

Configuring the DNS Server

To make other SIP users find your SIP domain, you need to configure your DNS (or rather, the DNS managing the domain).

One way of doing this is to add an *A record* for the domain, and point it to the Telecommuting Module. With this solution, you need to have a SIP domain that is not used for anything else. An example of a SIP-specific domain would be **sip.3com.com**.

If you want to use the same domain for all your communication (like **3com.com**), you need to add an *SRV record* to the DNS server instead, and point it to the Telecommuting Module. The SRV record is used specifically by SIP devices.

This is an example of an SRV record:

```
_sip._udp    SRV   100   0    5060   tess
_sip._tcp    SRV   100   0    5060   tess
_sips._tcp   SRV   100   0    5061   tess
```

This SRV record is entered into the zone file for the SIP domain. It points to the host *tess*, which is supposed to be a computer under the same domain (tess.3com.com) - in this case the Telecommuting Module.

If you don't want to use all transports, you can enter just the lines for the transport you want to allow (like only the TCP line).

Configuring the SIP Clients

SIP clients that can be configured to use a domain name only need to use the DNS which handles the domain.

SIP clients that need to be configured with an (additional) IP address should use the IP address of the registrar when located on the LAN, and the outside IP address of the Telecommuting Module when located anywhere else.

SIP Sessions

Establishing a SIP session

You start a call (a session) by sending a request to the address of the person you want to communicate with. The format of the address is <sip:user@host>, where user can be a user name or a telephone number, and host can be a domain name (e.g. example.com) or a numerical IP address (e.g. 172.15.253.12). This means that it usually looks a lot like a standard email address. In this request information about which media streams the client wants to send/receive and what ports should be used is also included.

The SIP client sends this request to its default SIP proxy. This proxy resolves the SIP domain in DNS, and sends the request to the SIP registrar for that domain. The proxy also adds information stating that the request was routed through the proxy, thus ensuring that the reply will be routed the same way.

The registrar for the domain looks up the user to see where he is registered, and forwards the request to the machine in question. The SIP client on this machine alerts the user, indicating that someone wants to initiate a SIP session. The user confirms that he, too, wants the SIP session. The client sends a reply with necessary information about what ports should be used by this client for sending and receiving media streams.

The first client receives the reply and sends a confirmation packet. After this, the media streams can be sent.

SIP in 3Com VCX IP Telecommuting Module

SIP Routing Order

Here, the order for SIP routing decisions is listed. Sometimes you need to know this in order to configure the Telecommuting Module to make it work the way you want. The Telecommuting Module searches for the first matching setting in the list.

1. The Telecommuting Module checks that the SIP method in the packet is allowed according to the settings under **SIP Methods**.
2. The Telecommuting Module checks that the SIP packet is allowed according to the settings under **Sender IP Filter Rules**.
3. The Telecommuting Module checks that the SIP packet is allowed according to the settings under **Header Filter Rules**.
4. The Telecommuting Module checks if the SIP packet contains a Route header which determines the next destination.
5. If VoIP Survival is enabled and active, the Telecommuting Module checks if the SIP packet is addressed to a user under a monitored domain.
6. The Telecommuting Module checks for the SIP domain of the Request-URI in the **DNS Override For SIP Requests** table.
7. The Telecommuting Module checks for the SIP user from the Request-URI among locally registered users and users listed in the **Static Registrations** table.

8. The Telecommuting Module checks if there is a matching row in the **Dial Plan** table.
9. The Telecommuting Module checks if the SIP packet Request-URI contains one of its **Local SIP Domains**. If so, and no match was found in the above list, the Telecommuting Module returns a SIP packet with error code 404 (Not Found) to the sender.

After finding something to guide it in routing the packet, the Telecommuting Module proceeds to the next list, which tells it where to send the packet (if it hasn't already sent a 404 reply). This list is also searched until a match is found.

1. The Telecommuting Module sends the SIP packet to the **Outbound Proxy** if one has been entered.
2. The Telecommuting Module checks for the SIP domain of the Request-URI in the **DNS Override For SIP Requests** table.
3. If there are still unresolved domain names, the Telecommuting Module makes an ordinary DNS lookup.

SIP Packet Headers

This is a list of the more common SIP packet headers, and advice on how to modify them using different settings in the Telecommuting Module.

Request-URI

The Request-URI (RURI) of the SIP packet can be found in the first line, right after the name of the SIP method used. The RURI tells the destination of the packet.

When the Telecommuting Module acts as registrar for the domain of the RURI, it rewrites the RURI from *user@domain* into whatever the user gave as its *Contact* when it registered.

When the incoming RURI is one that the Telecommuting Module has previously substituted in a Contact header, the RURI is also rewritten.

When an XF account is used, the domain part of the incoming RURI will be changed into the domain of the XF account.

From

The From header contains the SIP user who sent the SIP request.

The Telecommuting Module only changes the From header when the built-in b2bua is used, like when an XF account is used.

To

The To header contains the SIP user who should receive the SIP request.

The Telecommuting Module only changes the To header when an XF account is used.

Contact

The Contact header tells on which address the SIP client wants to be contacted.

The Telecommuting Module always rewrites the Contact when a SIP request is forwarded through. To prevent this rewriting, the **URI Encoding** and **Preserve Username For All Requests** settings can be used.

Via

The Via header is used to keep track of which route the SIP request was sent. The response is sent back the same route.

The Via header is always rewritten by the Telecommuting Module when the SIP signaling crosses a NAT border (when the IP addresses change).

The Telecommuting Module can remove Via headers, when the server receiving the SIP request will not accept requests with more than one Via header. This is done using the **Remove Via Headers** setting.

Record-Route

The Record-Route header is used to make subsequent signaling for this request to be sent via the Telecommuting Module.

The Record-Route header is always rewritten by the Telecommuting Module when the SIP signaling crosses a NAT border (when the IP addresses change).

You can force the Telecommuting Module to add Record-Route headers using the **Force Record-Route for Outbound Requests** and **Force Record-Route for All Requests** settings.

Route

The Route header is used to send SIP signaling via a predefined route. All Record-Route headers added to the original SIP request will be converted into Route headers in later SIP requests within the same SIP session.

The Route header is always rewritten by the Telecommuting Module when the SIP signaling crosses a NAT border (when the IP addresses change).

Content-Type

The Content-Type header is used when the SIP packet has a body. A body is used to convey information about something, like call parameters when a voice call is set up. The Content-Type header defines the body type to help the client read the content correctly.

Some content types are automatically allowed through the Telecommuting Module, but most types must be allowed by configuration. For this, the **Content Types** table is used.

If a SIP packet is not allowed because of the content type, this error message is shown in the log: `SIP unaccepted content - deny`.

Appendix B. Troubleshooting

Troubleshooting the Telecommuting Module largely consists of checking the hardware (the Telecommuting Module, the network connectors, ...) and checking the Telecommuting Module log. The log is usually an excellent tool in finding out why the Telecommuting Module does not do what you wanted it to do.

Below is some general advice to help you troubleshoot, almost regardless of which problem you have.

- Check that the events you look for are really logged (on the **Logging Configuration** page).
- Check that the configuration has been applied properly, either by applying it (on the **Save/Load Configuration** page) or by checking the Permanent Configuration (on the **Show Configuration** page).
- Check that you display the log you want to look for. The correct date and time (or no date or time) should be filled in, the desired log entries should be checked on the righthand side of the page, and the three boxes concerning which IP packets to show should be filled in accordingly.

Network troubleshooting

No traffic shown in the log

- Check that the interface is turned on on the corresponding interface page.
- Check that the Telecommuting Module has a correct default gateway (on the **Basic Configuration** page).
- Check that the client computer has a correct default gateway.

Traffic discarded as spoofed

When traffic is blocked and the reason given is Spoofed, there is a mismatch between the network that the Telecommuting Module is configured for and the network that the client is configured for. The Telecommuting Module regards an IP address as spoofed if it detects traffic from that IP address on an interface where the IP address should not be.

An example of a situation where this occurs is when you move a computer from one Telecommuting Module interface to another without changing its IP address and netmask.

Another example is if the Telecommuting Module has been configured to use a network with a netmask of 255.255.255.128, but the network really is larger, like 255.255.254.0. The IP addresses outside the smaller IP interval will be regarded as spoofed by the Telecommuting Module.

SIP troubleshooting

Before going into the different error descriptions below, check that the SIP module is turned on and the configuration applied.

SIP users can't register on the Telecommuting Module

- Check that the SIP domain that the users try to register on is listed in the **Local SIP Domains** table.
- If you do not use RADIUS authentication, check that the SIP user which tries to register is listed in the **Local SIP User Database** table.
- If you do not use RADIUS authentication, check in the **Local SIP User Database** table that the SIP user which tries to register is allowed to register from the network where the SIP client is located. If you use RADIUS authentication, check on the **Authentication and Accounting** page that the SIP user which tries to registe ris allowed to register from teh network where the SIP client is located.
- If local SIP authentication is used, check that the SIP user uses the correct password.

SIP users can't register through the Telecommuting Module

- Check that the SIP domain that the users try to register on is not listed in the **Local SIP Domains** table.
- Check that SIP authentication is not used. If you want the Telecommuting Module to perform SIP authentication, make sure that the Telecommuting Module and the SIP registrar uses the same SIP realm.
- If the client sends the REGISTER request to the Telecommuting Module itself and the Telecommuting Module is supposed to redirect it to the registrar, check on the **Routing** page that this is configured correctly.
- Check that there are **Sender IP Filter Rules** to allow the registration through the Telecommuting Module. For the network from where the registration was sent (or as **Default Policy For SIP Requests**), you must select **Process all**.

SIP Trunking (calls via SIP operator)

- If your operator requires registration, check that the Telecommuting Module registered successfully. A successful registration is indicated in the **Registered Users** table on the **Registrar and Session Status** page. If you find the operator user listed in that table, the registration was successful.
- If you do not get a ring tone in the calling phone, there is probably something wrong in the SIP signaling. Check the log to see that the Telecommuting Module can connect to the operator. Also check that the Request-URI of the incoming INVITE request looks like you expected. For incoming calls, you might have to change your Dial Plan to match what the operator sends out, like a "+" first in the phone number. For outgoing calls, some

operators require the phone number to start with a "+". Contact your operator to find out the details about the dial scheme.

A call is established, but there is no voice

- If you use a DMZ Telecommuting Module Type, check on the **Surroundings** page that you have separated the clients into correct networks. Clients that can reach each other without using the Telecommuting Module should be in the same Surroundings network, and clients that must use the Telecommuting Module to reach each other should be in different Surroundings networks.
- If you use a DMZ or DMZ/LAN Telecommuting Module Type, check that the firewall connected to the Telecommuting Module does not block the media. See the chapter titled Firewall and Client Configuration, for more information about which ports should be opened in the firewall.

Administration troubleshooting

This section describes problems that can arise when administrating the Telecommuting Module.

The Telecommuting Module reverts to the old version when trying to upgrade

- Check the release note for new error checks, which will make some part of your configuration invalid with the new software version.

The Telecommuting Module is unaccessible for some time when trying to apply a configuration

There is something in the new configuration that does not allow you to access the web configuration interface.

- Check the log to see if your access attempts reached the Telecommuting Module.
- Check that the configuration IP address (**Configuration Transport** on the **Access Control** page) is the one you use when trying to access the Telecommuting Module. Note that if you apply a configuration which changes the configuration IP address, your web browser will not automatically be redirected to the new IP address.
- Check that configuration traffic is allowed via the interface your web browser is located behind (**Configuration Allowed Via Interface** on the **Access Control** page).
- Check that configuration traffic is allowed from the computer where you run your web browser (**Configuration Computers** on the **Access Control** page).

Log Messages

Here is a presentation of many common log messages that can be found in the Telecommuting Module log.

In many messages, information about IP addresses, usernames and other changing parameters will be displayed in the log messages. In the listing, such information will be presented contained in angle brackets. The listed log message "<Username> logged on" will mean that the real message in your log will look like "admin logged on" or "Charlie logged on", that is, the *<Username>* will be replaced by a username on your system.

SIP errors

These log messages can appear when the **SIP errors** box has been checked on the **Display Log** page.

SIP send failure -1 on socket -1 <event number>

Something went wrong when the Telecommuting Module tried to send a SIP packet to another SIP device. Maybe there was no TLS connection (if TLS should be used), or the device is known not to reply, or the Telecommuting Module has no network connection at all on the interface facing the other device. The event number is an internal parameter to keep track of different SIP events.

Destination <IP address>:<port> is known bad. Skipping.

The SIP device on <IP address> has been blacklisted by the Telecommuting Module. This happens when the other SIP device has sent an ICMP type 3 packet in response to a SIP packet, or when the other SIP device has not responded at all to previous SIP signaling. For the latter event, you can avoid the blacklisting by setting the **SIP blacklist interval** on the **Sessions and Media** page to 0.

Parse error at '<character>' in message from <IP address>, at line: <SIP line>

Something on the referred line in the SIP message does not comply with the SIP standard or is something else that the Telecommuting Module does not recognize as valid SIP syntax.

No answer from destination <IP address>:<port>

The Telecommuting Module sent a SIP packet to the IP address, but it hasn't responded before the message timed out. If this was a message to a SIP domain, the Telecommuting Module will try next server handling this domain.

sipfw: SIP <response code> response from <IP address> rejected, no state

Something in the received SIP response was unexpected. It could be a very late response to a SIP request, or a message where the topmost Via header does not indicate the Telecommuting Module, or something else that does not make it an invalid SIP packet in itself, but it doesn't match what has happened in the Telecommuting Module.

Starting SIP TCP server at port 5060

This message will be shown when the SIP module is started. This can happen when you apply settings where the SIP module just has been activated, or when you boot the Telecommuting Module or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the Telecommuting Module is now ready to receive SIP signaling over TCP.

Starting SIP UDP server at port 5060

This message will be shown when the SIP module is started. This can happen when you apply settings where the SIP module just has been activated, or when you boot the Telecommuting Module or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the Telecommuting Module is now ready to receive SIP signaling over UDP.

Stopped SIP TCP server

This message will be shown when the SIP module is stopped. This can happen when you apply settings where the SIP module just has been deactivated, or when you boot the Telecommuting Module or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the Telecommuting Module can no longer receive SIP signaling over TCP.

Stopped SIP UDP server

This message will be shown when the SIP module is stopped. This can happen when you apply settings where the SIP module just has been deactivated, or when you boot the Telecommuting Module or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the Telecommuting Module can no longer receive SIP signaling over UDP.

IPsec key negotiations

These log messages can appear when the **IPsec key negotiations** box has been checked on the **Display Log** page.

IPsec: "<peer name>-<tunnel number>" #<event number>: ignoring informational payload, type <payload type>

The IPsec peer *<peer name>* sent a message during negotiation which the Telecommuting Module ignores, because it can’t use it. The payload type (like IPSEC_RESPONDER_LIFETIME) will give you a hint about what is the matter. The event number is a counter for how many negotiation attempts has been performed for this peer.

IPsec: "<peer name>-<tunnel number>" <IP address> #<event number>: Issuer CRL not found

The Telecommuting Module has no Certification Revocation List for the CA of the peer’s certificate. This is not an error, but is perfectly normal. You only need a Certification Revocation List when you want to make some certificates invalid.

Configuration server logins

These log messages can appear when the **Configuration server logins** box has been checked on the **Display Log** page.

<Username> [<IP address>] (<privileges>) logged on to the configuration server using local password

The user <Username> logged on to the web user interface. You can also see the IP address the user came from and which privileges this user has in the web interface.

<Username> [<IP address>] (<privileges>) was logged out from the configuration server due to inactivity

The user <Username> has not saved any configuration, changed page in the web interface or done any other changes for the last ten minutes. Next time this user tries to do anything in the web interface, he will be prompted for his password again.

Appendix C. Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols

The following lists discuss the most important ports and the server services that belong to them, and the different types of ICMP messages. Client programs usually use ports between 1024 and 65535.

There are also lists over Internet protocols, reserved IP addresses and a mapping between netmasks and IP address intervals.

List of the most important reserved ports

This is a list of important ports. See /etc/services and http://www.iana.org/.

Name	Port/protocol	Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	users
daytime	13/tcp	
daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
smtp	25/tcp	mail
time	37/tcp	timeserver
time	37/udp	timeserver
rlp	39/udp	resource location
nicname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server

Name	Port/protocol	Description
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client
bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service
audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol
imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	
snmp-trap	162/tcp	
snmp-trap	162/udp	

Name	Port/protocol	Description
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo
at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk
at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	
ipx	213/udp	
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
microsoft-ds	445/tcp	
microsoft-ds	445/udp	
isakmp	500/udp	ISAKMP/IKE
fcp	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)

Name	Port/protocol	Description
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	talk
ntalk	518/udp	New Talk (ntalk)
ntalk	518/udp	SunOS talkd(8)
netnews	532/tcp	readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)
klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell -kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bwnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
kerberos-adm	749/tcp	Kerberos Administration
kerberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication--tcp
kerberos	750/udp	Kerberos
kerberos_master	751/udp	Kerberos authentication
kerberos_master	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation
	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos
ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
pptp	1723/tcp	pptp

Name	Port/protocol	Description
pptp	1723/udp	pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin
rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/tcp	
afs	7000-7009/udp	

List of ICMP types

The following list is taken from http://www.iana.org/, ICMP Parameters.

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	[JBP]
2	Unassigned	[JBP]
3	Destination Unreachable	[RFC792]
4	Source Quench	[RFC792]
5	Redirect	[RFC792]
6	Alternate Host Address	[JBP]
7	Unassigned	[JBP]
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Solicitation	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request	[RFC792]
16	Information Reply	[RFC792]
17	Address Mask Request	[RFC950]
18	Address Mask Reply	[RFC950]

Type	Name	Reference
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute	[RFC1393]
31	Datagram Conversion Error	[RFC1475]
32	Mobile Host Redirect	[David Johnson]
33	IPv6 Where-Are-You	[Bill Simpson]
34	IPv6 I-Am-Here	[Bill Simpson]
35	Mobile Registration Request	[Bill Simpson]
36	Mobile Registration Reply	[Bill Simpson]
37	Domain Name Request	[Simpson]
38	Domain Name Reply	[Simpson]
39	SKIP	[Markson]
40	Photuris	[RFC2521]
41-255	Reserved	[JBP]

ICMP codes

Some ICMP types have codes attached.

ICMP type	Name	Code	Description
0	Echo Reply	0	No Code
1	Unassigned		
2	Unassigned		
3	Destination Unreachable	0	Net Unreachable
		1	Host Unreachable
		2	Protocol Unreachable
		3	Port Unreachable
		4	Fragmentation Needed and Don’t Fragment was Set
		5	Source Route Failed
		6	Destination Network Unknown
		7	Destination Host Unknown
		8	Source Host Isolated
		9	Communication with Destination Network is Administratively Prohibited
		10	Communication with Destination Host is Administratively Prohibited

ICMP type	Name	Code	Description
		11	Destination Network Unreachable for Type of Service
		12	Destination Host Unreachable for Type of Service
		13	Communication is Administratively Prohibited
4	Source Quench	0	No Code
5	Redirect	0	Redirect Datagram for the Network (or subnet)
		1	Redirect Datagram for the Host
		2	Redirect Datagram for the Type of Service and Network
		3	Redirect Datagram for the Type of Service and Host
6	Alternate Host Address	0	Alternate Address for Host
7	Unassigned		
8	Echo	0	No Code
9	Router Advertisement	0	No Code
10	Router Selection	0	No Code
11	Time Exceeded	0	Time to Live exceeded in Transit
		1	Fragment Reassembly Time Exceeded
12	Parameter Problem	0	Pointer indicates the error
		1	Missing a Required Option
		2	Bad Length
13	Timestamp	0	No Code
14	Timestamp Reply	0	No Code
15	Information Request	0	No Code
16	Information Reply	0	No Code
17	Address Mask Request	0	No Code
18	Address Mask Reply	0	No Code
19	Reserved (for Security)		
20-29	Reserved (for Robustness Experiment)		
30	Traceroute		
31	Datagram Conversion Error		

ICMP type	Name	Code	Description
32	Mobile Host Redirect		
33	IPv6 Where-Are-You		
34	IPv6 I-Am-Here		
35	Mobile Registration Request		
36	Mobile Registration Reply		

Internet protocols and their numbers

The following table lists common Internet protocols and their protocol numbers. All these protocols run on IP. The list is extracted from http://www.iana.org/, Protocol Numbers.

Protocol number	Keyword	Protocol
0	HOPOPT	IPv6 Hop-by-Hop Option
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
9	IGP	any private interior gateway
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
17	UDP	User Datagram
18	MUX	Multiplexing
19	DCN-MEAS	DCN Measurement Subsystems
20	HMP	Host Monitoring
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Protocol Class 4
30	NETBLT	Bulk Data Transfer Protocol
31	MFE-NSP	MFE Network Services Protocol
32	MERIT-INP	MERIT Internodal Protocol
34	3PC	Third Party Connect Protocol
37	DDP	Datagram Delivery Protocol
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
46	RSVP	Reservation Protocol

Protocol number	Keyword	Protocol
47	GRE	General Routing Encapsulation
48	MHRP	Mobile Host Routing Protocol
50	ESP	Encapsulation Security Payload
51	AH	Authentication Header
53	SWIPE	IP with Encryption
54	NHRP	NBMA Next Hop Resolution Protocol
61		any host internal protocol
63		any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
68		any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
75	PVP	Packet Video Protocol
80	ISO-IP	ISO Internet Protocol
84	TTP	TTP
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	EIGRP	EIGRP
91	LARP	Locus Address Resolution Protocol
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25 Frames
94	IPIP	IP-within-IP Encapsulation Protocol
95	MICP	Mobile Internetworking Control Pro.
97	ETHERIP	Ethernet-within-IP Encapsulation
98	ENCAP	Encapsulation Header
99		any private encryption scheme
100	GMTP	GMTP
115	L2TP	Layer Two Tunneling Protocol
255		Reserved

IP intervals

This is a list of the IP addresses available for different netmasks. The first column shows the number of bits used for the net address, i. e., is set to 1 in the netmask. The second column maps the number of bits to a netmask on the usual octet-dot format. The third column shows the address class for this netmask.

The second table shows the IP address interval for each class.

1-set bits	Mask	IP address class
0	0.0.0.0	0
1	128.0.0.0	1
2	192.0.0.0	2
3	224.0.0.0	3
4	240.0.0.0	4
5	248.0.0.0	5
6	252.0.0.0	6
7	254.0.0.0	7
8	255.0.0.0	0
9	255.128.0.0	1
10	255.192.0.0	2
11	255.224.0.0	3
12	255.240.0.0	4
13	255.248.0.0	5
14	255.252.0.0	6
15	255.254.0.0	7
16	255.255.0.0	0
17	255.255.128.0	1
18	255.255.192.0	2
19	255.255.224.0	3
20	255.255.240.0	4
21	255.255.248.0	5
22	255.255.252.0	6
23	255.255.254.0	7
24	255.255.255.0	0
25	255.255.255.128	1
26	255.255.255.192	2
27	255.255.255.224	3
28	255.255.255.240	4
29	255.255.255.248	5
30	255.255.255.252	6
31	255.255.255.254	7
32	255.255.255.255	8

Example: We want to split the network 130.234.250.0/25 (i.e., 130.234.250.0-130.234.250.127) into four subnets. The netmask for each subnet will be 27 bits, which means 255.255.255.224. This netmask is in IP class 3. The second table gives us the following available intervals: 0-31, 32-63, 64-95, and 96-127 (then we are out of IP addresses). One of the subnets will be 130.234.250.64/27

(130.234.250.64-130.234.250.95).

Class	IP intervals							
0	0-255							
1	0-127	128-255						
2	0-63	64-127	128-191	192-255				
3	0-31	32-63	64-95	96-127	128-159	160-191	192-223	224-255
4	0-15	16-31	32-47	48-63	64-79	80-95	96-111	112-127
	128-143	144-159	160-175	176-191	192-207	208-223	224-239	240-255
5	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
	64-71	72-79	80-87	88-95	96-103	104-111	112-119	120-127
	128-135	136-143	144-151	152-159	160-167	168-175	176-183	184-191
	192-199	200-207	208-215	216-223	224-231	232-239	240-247	248-255
6	0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
	32-35	36-39	40-43	44-47	48-51	52-55	56-59	60-63
	64-67	68-71	72-75	76-79	80-83	84-87	88-91	92-95
	96-99	100-103	104-107	108-111	112-115	116-119	120-123	124-127
	128-131	132-135	136-139	140-143	144-147	148-151	152-155	156-159
	160-163	164-167	168-171	172-175	176-179	180-183	184-187	188-191
	192-195	196-199	200-203	204-207	208-211	212-215	216-219	220-223
	224-227	228-231	232-235	236-239	240-243	244-247	248-251	252-255
7	0-1	2-3	4-5	6-7	8-9	10-11	...	254-255
8	0	1	2	3	4	5	...	255

You could have a large network, for example 130.234.128.0/18, which is interpreted from the tables as all IP addresses from 130.234.128.0 to 130.234.191.255, inclusive (18 is in class no. 2, giving an IP interval of 128-191). N.B.: The netmask only reaches the third byte, which means that all IP addresses in byte 4 are available.

Reserved IP addresses

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (see also RFC 1918):

- 10.0.0.0 - 10.255.255.255 (10/8)
- 172.16.0.0 - 172.31.255.255 (172.16/12)
- 192.168.0.0 - 192.168.255.255 (192.168/16)

Appendix D. Definitions of terms

AFS, Andrew File System

AFS is a more secure way of distributing file systems over a network. If files are mounted over the Internet, AFS is fairly secure. Normally, AFS uses Kerberos for security management.

ARP

ARP, Address Resolution Protocol, is a protocol for mapping an IP address to a physical machine address in the local network. A thorough description of ARP can be found in RFC 826.

Broadcast

Broadcast is a method of sending packets when you don't know the actual recipient. The packets are sent to all computers on the network.

Each network has a network address (the first address of the IP interval) and a broadcast address (the last address of the IP interval). On the network 192.168.0.0/24 (192.168.0.0-192.168.0.255), 192.168.0.255 is the broadcast address. When a computer wants to address all computers on the network, like when a Windows computer wants to map the resources, it sends a request to the broadcast address. All computers on the network receive this request and decides if they should reply.

Client program

A client program is one that the user runs on her computer. A client program connects to a server. One example of a client program is Mozilla (a web browser). One benefit of dividing up a service into server and client programs is that the server program can be run on a larger computer with better resources, and the users do not have to make their own copies of the databases. This allows the client programs to be run on less powerful computers.

Cracker

A person who breaks into computer systems and commits other criminal acts using a computer.

Daemon program

A daemon program is a server program for a service. This kind of program waits for and manages external calls. A typical example is FTP. A user starts his FTP client. The client connects to the FTP server. Now the user can transfer files to his own computer or to the server. See Server.

Denial of Service, DoS

A type of attack that tries to block a network service by overloading the server.

DHCP

DHCP, Dynamic Host Configuration Protocol, is a protocol for handing out IP addresses and other configuration information to computers without having to log on to every single machine. Instead, the computers themselves send out requests about this information at boot, and gets appropriate configuration parameters from a DHCP server. A thorough description of DHCP can be found in RFC 2131.

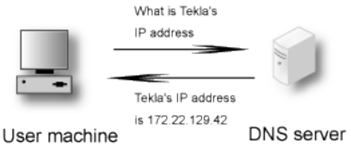
DMZ

A DMZ is a computer network that is accessible from several other computer networks that have no direct contact with each other. Often, one of these networks is the Internet and the other is a local, internal network. There is no direct connection between the Internet and the local network, but both of them can access an intermediate network, a demilitarized zone.

DMZs are often used for special servers, such as web servers, which must be accessible from two separate networks.

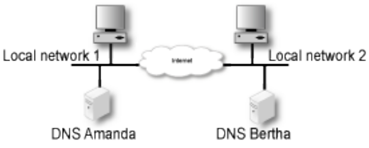
DNS, Domain Name System

A DNS server is the Internet equivalent of dialing telephone information. If you know the name of a computer, you can access its IP address and vice versa. The server keeps track of names and IP addresses. Imagine that a user wants to connect to the computer "Tekla" through a Telnet (terminal) connection. The Telnet program asks the DNS server about Tekla and receives Tekla’s IP address. If the DNS server does not know a name, it asks its nearest DNS server. See the figure.


What is Tekla's IP address
Tekla's IP address is 172.22.129.42
User machine
DNS server

DNS servers are usually named *primary*, *secondary*, or *other*. If you have several networks with several DNS servers, they can communicate with each other. It is a good idea to make them secondary DNS servers to each other. Secondary DNS servers work as extra DNS servers if the primary server is not working.

A secondary DNS server updates its information from the primary DNS server at regular intervals. You can specify how often. Only the manager of the DNS server can set it up as a secondary DNS server for someone else. In the figure below, we have two local networks with separate DNS servers. If DNS server Amanda does not work, a machine in network 1 may ask the DNS server in network 2, Bertha, if this server is set up as secondary DNS server for Amanda. Other DNS servers outside network 1 and 2 belong to the *other* category.



The DNS server responds to name queries on port 53. Both TCP and UDP are used for name queries.

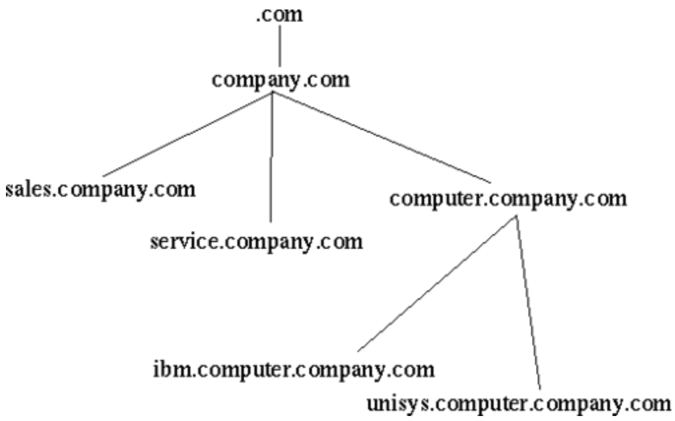
Domain

A domain is a country, organization, or subdivision. All countries have one top domain for the country, except for the United States, which is divided into a commercial domain (*.com*), a non-profit organizational domain (*.org*), a university domain (*.edu*), a military domain (*.mil*), a governmental domain (*.gov*), and a network domain (*.net*). All domains are hierarchical and each domain is responsible for the domains directly under it.

A domain can have several sub-domains, which in turn can have sub-domains and so on. The structure combines the domain name of the organization with the overlying domain name.

For example, Stanford University has the domain name stanford, which is under the university domain of USA, .edu; together they form the domain stanford.edu. The university also has different departments under stanford.edu.

The departments of a company or organization can request a sub-domain from the domain manager. If the tech support people in the company's service division want their own domain, they can go to their domain manager and request a domain called, for instance, service. Below, we have 'Company Inc.,' which consists of three departments: A sales department, a service department, and a computer department. The computer department is divided into an IBM section and a Unisys section.



Contact your internet service provider to register a domain.

Dynamic routing

Dynamic routing is used when the traffic between two computers have several routes available. The route for the packets can be changed if a connection is broken or a router is turned off. RIP is a protocol handling dynamic routing.

Firewall

A device that prevents unauthorized access to a computer network.

Forwarding

See Relay.

FTP (File Transfer Protocol)

Imagine that you have an account on a UNIX machine. You can retrieve and store files on the UNIX machine with FTP. The program that manages this is called the *FTP* *server*. You can also establish an area of files that are accessible to others. Anyone can log in as user anonymous and enter his email address as a password. They can then access all files in this area, but nothing else. A computer with an FTP server and a freely available area is usually called an *FTP site*.

Gateway

Gateway is an old name for a Router.

Hacker

A person who is skilled and knowledgeable about computers and likes to examine the details of a computer system and what can be done with it. A hacker is good at programming and achieves good results. A hacker is not to be confused with a computer criminal; see Cracker.

HTTPS

HTTPS is WWW traffic (HTTP traffic) over an encrypted connection. The encrypted connection is established using the SSL protocol.

ICMP protocol

ICMP is used to forward information, primarily error messages. To see if a computer is running, the ‘ping’ program sends an echo request, which is an ICMP packet. If a problem occurs with a connection, a response is sent using ICMP that something is not right (the computer is not responding, the network is down, etc). If there are two possible paths for a connection, a router along the way may tell the computer to use the other path. The router sends an ICMP redirect. ICMP uses the IP protocol to send data over the network.

IP address

IP addresses are used to connect to computers, and are the Internet equivalent to telephone numbers. An IP address is divided into four groups, each of which is a number from 0 to 255. The groups are separated by dots. An example of an IP address is 192.165.122.42. Several IP addresses are required to connect several computers in a network; one for each computer.

IP addresses can be divided into *public* and *private* addresses. Public IP addresses are unique throughout the Internet, and can be reached by all computers connected to the Internet. Private IP addresses can be used on several local networks, but can’t be reached from other networks. When a computer with a private IP address wants to connect to a computer on the Internet, the traffic must be NATed (see also NAT). See also appendix C, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols, for a list of private IP addresses.

IP

IP is short for Internet Protocol. This is a protocol that is used to send data between two computers on the same or different networks. IP performs no security checks. It works analogous to standard mail. Peter sends four postcards to Christy from the other side of the world. Christy gets postcard two first, then postcard one and postcard four. Postcard three disappears on the way. Peter and Christy know each other’s addresses, and the post office knows how to read addresses and send postcards in the right direction. But

Peter and Christy cannot know if all of their postcards will arrive, and Christy doesn't know what order the postcards were sent in.

For more information about IP addresses, see IP address.

Kerberos

Kerberos is a system to secure connections between several computers over networks. The Kerberos system uses a Kerberos server to manage security. Connections that go through Kerberos are often encrypted.

Masquerading

See NAT.

Name server

See DNS.

NAT

NAT (Network Address Translation), also known as masquerading, is a way to hide a network from outside computers. Used with firewalls to hide the computers on the internal network from the rest of the world.

Netmask

See network mask.

Network mask

A network mask tells what computers can be accessed locally without using a gateway, and what computers can only be reached through a gateway. The bits in the network mask determine what is a network and what is a computer. The total number of bits is 32 and the "one-bits" are for networks. The network mask can be specified as the number of one-bits grouped in the same way as IP addresses. For what formerly was called a class C network, the network mask is 24, which can also be expressed as 255.255.255.0 (i.e., 24 one-bits grouped in octets and then interpreted as binary numbers). If this network is divided into several parts, the network mask is different, depending on how the division is done. For example, the network mask 255.255.255.224 gives a network with 32 IP addresses in it. See also the table of network masks in appendix C, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols.

News

News is a distributed, loose conference system, which includes the entire Internet and more. News originated in email, so it has many similarities to email. It can also be called Usenet News and NetNews.

News is a conference system for exchange of ideas, questions and answers, and so on, just like in a BBS or COM system. What is written in News is not stored on a central computer; it is sent out all over the world and stored in several places. Your organization may choose to retrieve News and store all texts locally.

To keep track of everything, News is divided into news groups. A news group focuses on a specific area of interest. Each news group can have divisions and subgroups.

rec.motorcycles.harley is an example of a group name. rec is the main group, Recreational, which includes hobbies, recreation and the arts. A subgroup of rec is motorcycles, which is solely about motorcycles. A subgroup of rec.motorcycles is harley, which is only about Harley Davidson motorcycles. Another example is sci.geo.geology. Anyone can post articles to News; remember that several million people may be reading what you write. Make sure that all users are aware of this and are restrictive of what they write.

News servers use the NNTP protocol to communicate with each other. Many client programs also use NNTP to communicate with the news server. NNTP communication uses port 119.

NFS, Network File System

NFS is a protocol for mounting disks from other computers over the network. NFS should be blocked against unsecure external networks. NFS uses port 2049.

NIS/YP, Network Information Service/Yellow Pages®

NIS/YP is used to distribute central information to client machines in a network. Passwords and e-mail aliases are typical examples of such information. This also often used to allow users to sit at any work station, log in as themselves, and access their user accounts. NIS/YP should be blocked against unsecure external networks.

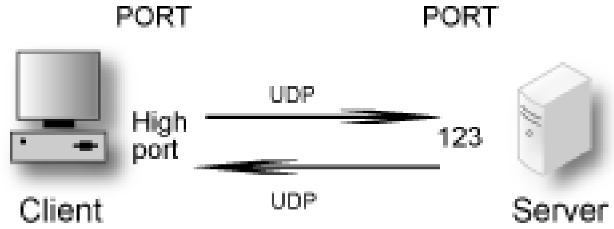
NNTP

See News.

NTP

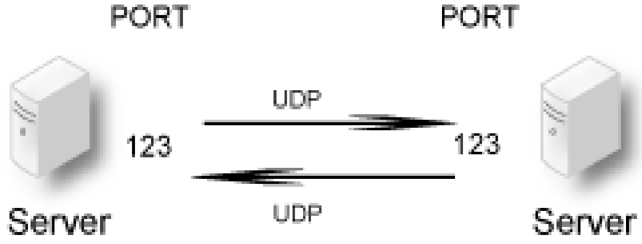
NTP is short for Network Time Protocol and is used for synchronizing computer clocks. The synchronization normally uses a computer with a very accurate clock, e. g., a computer with an atomic clock.

A client computer wanting to synchronize with a server via NTP usually uses a high port on the client, port 123 on the server and the UDP protocol. The server returns data using UDP from port 123 to a high port on the client computer.



The time interval between connections to the NTP server depends on the difference between the computer clock and the server clock. When NTP is started on a computer, it connects rather often to check that the time is correct and that it doesn't gain or lose time compared to the server clock. After that, it will connect with lower frequency just to check that it keeps the correct time.

Two NTP servers communicating with each other use port 123 and the UDP protocol.



Open Windows

Open Windows is a window system that is used by several work stations. A similar window system is the X Window System, which Open Windows is based on. The X Window System and Open Windows use ports 6000 and upward for traffic to the work stations. It is a good idea to block ports 6000-6010 for incoming traffic from an unsecure outside network.

Packet

When something is sent over a computer network, for example, a file or an email, it is divided up into sections. These sections are called packets. They make up a sort of jigsaw puzzle, each piece sent individually. The receiving computer has to reassemble the pieces.

Ping

Ping is used to examine whether a computer works and is accessible over a network. Ping sends ICMP traffic to the computer in question, and the target computer replies with a reply ICMP packet if it is running and reachable from the network.

You can also ping a whole network, and thereby use ping to examine which computers exist on a certain network. Therefore it is not advisable to allow ping into an internal network.

The client computer sends a type 8 ICMP packet, echo-request, to find out whether the target computer is working and accessible. The target computer ("server" in the picture below) replies with a type 0 ICMP packet, echo-reply, to tell it is working and accessible over the network.

Ports

When two computers use UDP or TCP to connect, ports are used. A client machine that wants access to a certain service on a server connects to the standard port for that particular service on the server. The programs on the client machine receive an available port over 1023. For example, if a user on the computer Tekla wants to run a Telnet session to the computer Winona, the user’s Telnet client program receives an available port over 1023 to connect to port 23 on Winona. If two server programs contact each other, one can act as a client program, receiving an available port over 1023 on its local machine. However, many server programs have special definitions of how servers communicate with each other, where both servers user their standard port.

PPP

PPP is short for Point-to-Point Protocol. This is usually used to send IP packets over modem connections. See also IP.

Protocols

Protocols are sets of rules for how programs communicate with each other. For example, a web server can use the protocols HTTP and HTTPS.

Proxy

Proxies are devices through which web pages, FTP files, and so on can be retrieved for a local network. This can be good to combine with a cache memory, which will store pages and files once fetched from the Internet site. When another user wants to look at a page already in the cache, it acts as a web server, sending the cached page instead of fetching a new copy through the Internet.

In your web browser, specify a computer and cache/proxy to be used to store this information.

Relay

When the local network is connected to the Internet through a firewall, all types of services are usually blocked. It is as if the network is not connected to the Internet. Relays can then be set up to allow certain services, such as the WWW, to pass through under controlled circumstances. Think of it as a giant stone wall with a gate and a specialized gate keeper. The gate keeper only lets certain visitors pass. To allow others to pass through, you set up another gate with another specialized gate keeper.

Request-URI

A Request-URI is used by the SIP protocol to indicate where a SIP request should be sent. The Request-URI can contain a username, a SIP domain or an IP address. It also contains the sip/sips parameter (sips if the request should be sent encrypted all the way, sip if not) and the SIP version (usually SIP/2.0).

RFC

An RFC (Request For Comments) is a document which standardizes some aspect of the Internet traffic. RFC:s are available at http://rfc.dotsrc.org/rfc-url.sgml.

RIP

RIP is a protocol that manages dynamic routing. Dynamic routing means that the path for traffic can be changed. RIP selects the path that goes through the least number of routers, but does not consider the bandwidth or load on the network. RIP is only used in local networks. Fixed paths for traffic are called static routing.

Router

A router is a machine that is used to connect several smaller and larger networks. Often, a router is used to connect a local network to the Internet. This router only lets traffic to the Internet out; all other traffic remains on the local network. A router can also be called a gateway.

Routing

A routing is a path for the traffic between different computers.

Server

A server can be a program that performs a service on a network or a computer that runs one or more server programs. One example is a computer that stores files centrally, which makes it a kind of server, usually called a *file server*. The program that manages traffic so that people from the outside can access an organization's web pages is a *server program*.

SIP

SIP, Session Initiation Protocol, is a protocol for creating, maintaining and terminating various media stream sessions over an IP network. SIP is used to negotiate which media streams the parts can send and receive, and which parts should be involved in the exchange. When this is established, the media streams are sent according to their own protocols (e.g. HTTP). A thorough description of SIP can be found in RFC 2543.

SLIP

SLIP is short for Serial Line IP. This is usually used to send IP packets over modem connections. See IP.

SLIRP

SLIRP is a program that sends IP packets over serial connections, such a modem connections. SLIRP is run as a user program. SLIRP does not need its own IP address; it uses the server's IP address. The program works with both SLIP and PPP clients. See IP.

SMTP

Simple Mail Transfer Protocol, a protocol for sending e-mail between e-mail servers. SMTP uses port 25.

SNMP

A protocol used for network monitoring. SNMP uses ports 161 and 162.

Sockets

When two computers connect to each other, they use their IP addresses and port numbers. The combination of an IP address and a port number is called a socket. See IP addresses and Ports.

SSH, Secure SHell

SSH is a system for secure, encrypted connections between two computers over a network. SSH uses one open and one secret key. In contrast to Kerberos, SSH does not use a central server for security. SSH uses port 22.

SSL

SSL is short for Secure Sockets Layer. The SSL protocol handles establishing of encrypted computer connections. Usually HTTP and WWW traffic is sent on SSL. HTTP on SSL is called HTTPS.

Static Routing

A fixed path for the contact between computers. With a static routing, traffic cannot be redirected to another path if the connection is broken. This would require dynamic routing, for example, with RIP.

Syslog

Syslog is a service for logging data. In UNIX, regular programs do not log any information; they send all data to a syslog server that saves data in a log file. One example is a web server that sends data over the computers that connects to the server and sends error messages for web pages that it could not locate. Messages to a syslog server can also be sent over the network. Syslog uses the UDP protocol. A syslog server listens to port 514 for syslog messages.

TCP protocol

TCP connects two computers and makes sure that all data gets through and in the right order. TCP uses IP. IP manages addresses and makes sure that data is sent out to the network. When TCP connects, it receives a response from the TCP protocol layer on the receiving end. The recipient sends a little data along with a confirmation that the sender's data arrived. When a connection is made, a confirmation is always sent with all data packets. This can be compared with Peter and Christy sending postcards and, along with their message, commenting that they received the other's postcard. TCP shortens this confirmation to ACK (acknowledgment).

You know if a TCP packet is a connection attempt if it does not have ACK.

TCP keeps track of connections for different services using different port numbers. See Ports.

UDP protocol

UDP does not make a connection. It examines data that comes from outside for accuracy, by checksums. This is like examining a postcard to ensure that it has not been torn up. UDP does not keep track of whether or not all data gets through or if it is in the right order; this is the job of the application. So the data does not have an ACK confirmation. Peter and Christy, sending postcards, have to keep track of their own postcards and Peter has to tell Christy the order in which they should be read. UDP keeps track of the contacts using port numbers, just like TCP.

UUCP

UNIX to UNIX Copy, an old protocol for copying files between two UNIX computers. This is sometimes used to send e-mail between two computers.

WWW, World Wide Web

The WWW is currently the best known Internet service. The World Wide Web consists of millions of documents that are interconnected all over the world. A document can contain text, pictures, sound, and even video sequences. The WWW is based on the client-server concept. This means that each document is in a database on a web server. The user runs a client program, such as Netscape or Internet Explorer, that connects to a server, which could be anywhere in the world, and request a document. This document is displayed on the user's screen and the user can use his client program to click on other documents to display them. WWW usually runs on the HTTP and HTTPS protocols, using ports 80 and 443, respectively.

X Window System

A window system that is used by several work stations. A similar window system is Open Windows. The X Window System and Open Windows uses port numbers starting at 6000 and upward for traffic to the work stations. It is a good idea to block ports 6000-6010 from incoming traffic from an insecure outside network.

Appendix E. License Conditions

3Com VCX IP Telecommuting Module contains third party software that is subject to the following license agreements.

To fulfill the license conditions, we must either attach the source code with the software, or send a written offer, valid at least three years, to give a copy of the source code to anyone who wants it. According to 3b) of the license, we are entitled to charge for the distribution of the source code.

3Com Corporation offer the source code for all third party software included in 3Com VCX IP Telecommuting Module and licensed under GPL. This offer is valid for this version of 3Com VCX IP Telecommuting Module and is valid for three years after deliverance of your 3Com VCX IP Telecommuting Module unit. Contact 3Com Corporation for current information.

Software developed by Peter Åstrand

Terms

Modules under this license

subprocess-py 2.4

BSD derived licenses

Terms

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Modules under this license

libpcap 0.8.3 tcpdump 3.8.2

Software developed by Carnegie Mellon University

Terms

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

   Office of Technology Transfer
   Carnegie Mellon University
   5000 Forbes Avenue
   Pittsburgh, PA 15213-3890
   (412) 268-4387, fax: (412) 268-7395
   `<tech-transfer@andrew.cmu.edu>`

4. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

ppp 2.4.2_20030503

Software developed by Gregory M Christy

Terms

Copyright (c) 1991 Gregory M. Christy. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Gregory M. Christy. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Modules under this license

ppp 2.4.2_20030503

Software developed by Cisco Systems

Terms

Copyright (c) 2001-2006, Cisco Systems, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

srtp 1.4.4_cvs20070524

Software developed by Digital Equipment Corporation

Terms

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

DHCP 3.0.6

The DHCP license

Terms

Copyright (c) 1995 RadioMail Corporation.

Copyright (c) 2004-2007 by Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
<info@isc.org>
http://www.isc.org/

Modules under this license

DHCP 3.0.6

Software developed by Jason Downs

Terms

Copyright (c) 1997, Jason Downs. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR

ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

nologin

Software developed by Brian Gladman

Copyright (c) 2001, Dr Brian Gladman <`brg@gladman.uk.net`>, Worcester, UK. All rights reserved.

Terms

Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The copyright holder's name must not be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

Modules under this license

openswan-kernel 2.4.9

Software developed by Brian Gladman

Terms

I retain copyright in this code but I encourage its free use provided that I don't carry any responsibility for the results. I am especially happy to see it used in free and open source software. If you do use it I would appreciate an acknowledgement of its origin in the code or the product that results and I would also appreciate knowing a little about the use to which it is being put. I am grateful to Frank Yellin for some ideas that are used in this implementation.

Dr B. R. Gladman <`brg@gladman.uk.net`> 6th April 2001.

Modules under this license

openswan-kernel 2.4.9

Software developed by Google, Inc

Terms

By Frank Cusack <frank@google.com>. Copyright (c) 2002 Google, Inc. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that the above copyright notice appears in all copies. This software is provided without any warranty, express or implied.

Modules under this license

ppp 2.4.2_20030503

GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software - to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF

THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Modules under this license

bash 2.05b
busybox 1.8.3
coreutils 4.5.3
cpio 2.5
diffutils 2.8.1
dmiwriter 2.8
e2fsprogs 1.32
ed 0.2
ethtool 5
fdisk
findutils 4.1.7
glibc 2.3.3
gmp 4.1.2
gnupg 1.4.6
grep 2.5.1
iproute 2.6.20
ipset 2.2.6
iptables 1.4.0
iputils 20020927
libcap 1.10
libgcc 3.2.2
libnetfilter_queue 0.0.15
libnfnetlink 0.0.30
libstdc++ 3.2.2
libtermcap 2.0.8
linux 2.6.24.7
lrzsz 0.12.20
lyspython 0.0
MAKEDEV 3.3.2
module-init-tools 3.1
net-tools 1.60
openswan 2.4.13
openswan-kernel 2.4.9
pcre 3.9
ppp 2.4.2_20030503
pptpd 1.3.4
procps 2.0.11
psmisc 21.2
readline 4.3
sed 4.0.5
snort_inline 2.6.1.5
stunnel 4.04
SysVinit 2.84
tar 1.13.25
util-linux 2.11y

IBM Public License

Terms

Portions Copyright (c) 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission.

To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product.

THE SOFTWARE IS PROVIDED "AS IS", AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR

PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

Modules under this license

DHCP 3.0.6

Software developed by Ingate Systems

Terms

Copyright(c) 2005 Ingate Systems AB All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

srtp 1.4.4_cvs20070524

Software developed in the GIE DYADE cooperation

Terms

Copyright (c) 1995, 1996, 1997 <`Francis.Dupont@inria.fr`>, INRIA Rocquencourt, <`Alain.Durand@imag.fr`>, IMAG, <`Jean-Luc.Richier@imag.fr`>, IMAG-LSR.

Modules under this license

ppp 2.4.2_20030503

Software developed by Tommi Komulainen

Terms

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without specific prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Tommi Komulainen <`Tommi.Komulainen@iki.fi`>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

ppp 2.4.2_20030503

GNU Library General Public License (LGPL) v 2

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor
Boston, MA 02110-1301
USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE

This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

      (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary

GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

   When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and

distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF

THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Modules under this license

coreutils 4.5.3	gmp 4.1.2	libtermcap 2.0.8
cpio 2.5	grep 2.5.1	pptpd 1.3.4
e2fsprogs 1.32	iputils 20020927	procps 2.0.11

GNU Lesser General Public License (LGPL) v 2.1

Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages - typically libraries - of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code,

which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

   When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights

under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

    This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Modules under this license

coreutils 4.5.3
glibc 2.3.3
pyOpenSSL 0.6
tzdata 2006a

Software in the GNU C distribution

Terms

This file contains the copying permission notices for various files in the GNU C Library distribution that have copyright owners other than the Free Software Foundation. These notices all require that a copy of the notice be included in the accompanying documentation and be distributed with binary distributions of the code, so be sure to include this file along with any binary distributions derived from the GNU C Library.

All code incorporated from 4.4 BSD is distributed under the following license:

The DNS resolver code, taken from BIND 4.9.5, is copyrighted both by UC Berkeley and by Digital Equipment Corporation. The DEC portions are under the following license:

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The Sun RPC support (from rpcsrc-4.0) is covered by the following license:

Copyright (C) 1984, Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

The following CMU license covers some of the support code for Mach, derived from Mach 3.0:

Mach Operating System Copyright (C) 1991,1990,1989 Carnegie Mellon University All Rights Reserved.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Carnegie Mellon requests users of this software to return to

Software Distribution Coordinator School of Computer Science Carnegie Mellon University
Pittsburgh PA 15213-3890

or Software.Distribution@CS.CMU.EDU any improvements or extensions that they make and grant Carnegie Mellon the rights to redistribute these changes.

The file if_ppp.h is under the following CMU license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY CARNEGIE MELLON UNIVERSITY AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following license covers the files from Intel's "Highly Optimized Mathematical Functions for Itanium" collection:

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The files inet/getnameinfo.c and sysdeps/posix/getaddrinfo.c are copyright (C) by Craig Metz and are distributed under the following license:

The Inner Net License, Version 2.00

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

1. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
2. All terms of the all other applicable copyrights and licenses must be followed.
3. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
4. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
5. [The copyright holder has authorized the removal of this clause.]
6. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIA-

BILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

If these license terms cause you a real problem, contact the author.

Modules under this license

glibc 2.3.3

More software in the GNU C distribution

Terms

The include/err.h and src/err.c files contain this license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   > This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

src/strsep.c contains the same notice, but with no copyright claim of Dug Song.

src/strlcat.c and src/strlcpy.c uses this license:

The rest of the libdnet package uses this license:

src/fw-pktfilter.c is:

Copyright (c) 2002 Dug Song <dugsong@monkey.org>

Copyright (c) 2001 Jean-Baptiste Marchand, Hervé Schauer Consultants.

src/rand.c is:

Copyright (c) 2000 Dug Song <dugsong@monkey.org>

Copyright (c) 1996 David Mazieres <dm@lcs.mit.edu>

src/route-bsd.c is:

Copyright (c) 2001 Dug Song <dugsong@monkey.org>

Copyright (c) 1999 Masaki Hirabaru <masaki@merit.edu>

Modules under this license

libdnet 1.11

License exceptions for gcc/libgcc2.c

Terms

gcc/libgcc2.c contains this exception to the GNU General Public License:

In addition to the permissions in the GNU General Public License, the Free Software Foundation gives you unlimited permission to link the compiled version of this file into combinations with other programs, and to distribute those combinations without any restriction coming from the use of this file. (The General Public License restrictions do apply in other respects; for example, they cover modification of the file, and distribution when not linked into a combine executable.)

Various assembler files contain this exception to the GNU General Public License:

As a special exception, if you link this library with files compiled with GCC to produce an executable, this does not cause the resulting executable to be covered by the GNU General Public License. This exception does not however invalidate any other reasons why the executable file might be covered by the GNU General Public License.

Modules under this license

libgcc 3.2.2

License exceptions for libstdc++

Terms

libstdc++ comes with the following so called "runtime exception" to GPLv2:

As a special exception, you may use this file as part of a free software library without restriction. Specifically, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other files to produce an executable, this file does not by itself cause the resulting executable to be covered by the GNU General Public License. This exception does not however invalidate any other reasons why the executable file might be covered by the GNU General Public License.

Modules under this license

libstdc++ 3.2.2

License for lilo

Terms

LInux LOader (LILO) program code, documentation, and auxiliary programs are Copyright 1992-1998 Werner Almesberger. Copyright 1999-2005 John Coffman. All rights reserved.

License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the names of the author(s) nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Disclaimer

SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIA-

BILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(Note: The above license is copied from the BSD license at: http://www.opensource.org/licenses/bsd-license.html, substituting the appropriate references in the template.)

Modules under this license

lilo 22.7.3

Software developed by Paul Mackerras

Terms

Copyright (c) 1984, 1989-2002 Paul Mackerras. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without specific prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

> "This product includes software developed by Paul Mackerras <`paulus@samba.org`>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

ppp 2.4.2_20030503

Software developed by Pedro Roque Marques

Terms

Copyright (c) 1995 Pedro Roque Marques. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Pedro Roque Marques `<pedro_m@yahoo.com>`"

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

ppp 2.4.2_20030503

Software developed at M I T

Terms

Copyright 1987, 1988 by MIT Student Information Processing Board.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose is hereby granted, provided that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Modules under this license

e2fsprogs 1.32

License for Net-SNMP

Terms

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like)

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD)

Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD)

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD)

Copyright Â© 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Part 5: Sparta, Inc copyright notice (BSD)

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD)

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD)

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003 oss@fabasoft.com Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

net-snmp 5.4.1

License for NTP

Terms

Copyright (c) David L. Mills 1992-2001

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

Modules under this license

ntp 4.1.2

License for OpenSSH

Terms

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1. Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

   As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

   [Tatu continues]

   However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

   [However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

   - RSA is no longer included, found in the OpenSSL library
   - IDEA is no longer included, its use is deprecated
   - DES is now external, in the OpenSSL library
   - GMP is no longer used, and instead we call BN code from OpenSSL
   - Zlib is now external, in a library
   - The make-ssh-known-hosts script is no longer included
   - TSS has been removed
   - MD5 is now external, in the OpenSSL library
   - RC4 support has been replaced with ARC4 support from OpenSSL
   - Blowfish is now external, in the OpenSSL library

   [The licence continues]

   Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at http://www.cs.hut.fi/crypto.

   The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

   NO WARRANTY

   BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLI-

CABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

   Cryptographic attack detector for ssh - source code

   Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

   All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

   THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

   Ariel Futoransky <`futo@core-sdi.com`> http://www.core-sdi.com

3. ssh-keyscan was contributed by David Mazieres under a BSD-style license.

   Copyright 1995, 1996 by David Mazieres <`dm@lcs.mit.edu`>.

   Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4. The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

   @version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <`vincent.rijmen@esat.kuleuven.ac.be`>

@author Antoon Bosselaers <`antoon.bosselaers@esat.kuleuven.ac.be`>

@author Paulo Barreto <`paulo.barreto@terra.com.br`>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5. One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

   Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

   Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

   a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

   b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

   c. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

   THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6. Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

   Markus Friedl
   Theo de Raadt
   Niels Provos
   Dug Song
   Aaron Campbell
   Damien Miller
   Kevin Steves
   Daniel Kouril
   Wesley Griffin
   Per Allansson
   Nils Nordman
   Simon Wilkinson

   Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

   Ben Lindstrom
   Tim Rice
   Andre Lucas
   Chris Adams
   Corinna Vinschen
   Cray Inc.
   Denis Parker
   Gert Doering
   Jakob Schlyter
   Jason Downs
   Juha Yrjölä
   Michael Stone
   Networks Associates Technology, Inc.
   Solar Designer
   Todd C. Miller
   Wayne Schroeder
   William Jones
   Darren Tucker
   Sun Microsystems
   The SCO Group

   Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

   a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
   b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

   THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS

7. Portable OpenSSH contains the following additional licenses:

   a. md5crypt.c, md5crypt.h

      "THE BEER-WARE LICENSE" (Revision 42):

      <`phk@login.dknet.dk`> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

   b. snprintf replacement

      Copyright Patrick Powell 1995

      This code is based on code written by Patrick Powell (<`papowell@astart.com`>) It may be used for any purpose as long as this notice remains intact on all source code distributions

   c. Compatibility code (openbsd-compat)

      Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

      Some code is licensed under a 3-term BSD license, to the following copyright holders:

      Todd C. Miller
      Theo de Raadt
      Damien Miller
      Eric P. Allman
      The Regents of the University of California
      Constantin S. Svintsoff

      Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

      a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
      b. Redistributions in binary form must reproduce the above copyright notice, this

list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.
Todd C. Miller
Reyk Floeter
Chad Mynhier

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Modules under this license

openssh 4.5p1

License for OpenSSL

Terms

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org (mailto:openssl-core@openssl.org).

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

openssl 0.9.7a

License for OpenSWAN

Terms

Except for the DES library, MD5 code, and linux/net/ipsec/radij.c this software is under the GNU Public License, see the file COPYING. See the file CREDITS for details on origins of more of the code.

The linux/net/ipsec/radij.c code is derived from BSD 4.4lite code from sys/net/radix.c.

In addition to the terms set out under the GPL, permission is granted to link the software against the libdes, md5c.c, and radij.c libraries just mentioned.

The following additional notes apply if if you are NOT using CrytpoAPI:

> The DES library is under a BSD style license, see linux/crypto/ciphers/des/COPYRIGHT. Note that this software has a advertising clause in it.

The MD5 implementation is from RSADSI, so this package must include the following phrase:

> "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm". It is not under the GPL; see details in linux/net/ipsec/ipsec_md5c.c.

Modules under this license

openswan 2.4.13

The Python license

A. HISTORY OF THE SOFTWARE

Python was created in the early 1990s by Guido van Rossum at Stichting Mathematisch Centrum (CWI, see http://www.cwi.nl/) in the Netherlands as a successor of a language called ABC. Guido remains Python's principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for National Research Initiatives (CNRI, see http://www.cnri.reston.va.us/) in Reston, Virginia where he released several versions of the software.

In May 2000, Guido and the Python core development team moved to BeOpen.com to form the BeOpen PythonLabs team. In October of the same year, the PythonLabs team moved to Digital Creations (now Zope Corporation, see http://www.zope.com/). In 2001, the Python Software Foundation (PSF, see http://www.python.org/psf/) was formed, a non-profit organization created specifically to own Python-related Intellectual Property. Zope Corporation is a sponsoring member of the PSF.

All Python releases are Open Source (see http://www.opensource.org/ for the Open Source Definition). Historically, most, but not all, Python releases have also been GPL-compatible; the table below summarizes the various releases.

Release	Derived from	Year	Owner	GPL- compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.2	2.1.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes
2.1.3	2.1.2	2002	PSF	yes
2.2.1	2.2	2002	PSF	yes
2.2.2	2.2.1	2002	PSF	yes
2.2.3	2.2.2	2003	PSF	yes
2.3	2.2.2	2002-2003	PSF	yes
2.3.1	2.3	2002-2003	PSF	yes
2.3.2	2.3.1	2002-2003	PSF	yes

Release	Derived from	Year	Owner	GPL- compatible? (1)
2.3.3	2.3.2	2002-2003	PSF	yes
2.3.4	2.3.3	2004	PSF	yes
2.3.5	2.3.4	2004-2005	PSF	yes
2.3.6	2.3.5	2006	PSF	yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON

PSF LICENSE AGREEMENT FOR PYTHON 2.3

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.3 software in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.3 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004 Python Software Foundation; All Rights Reserved" are retained in Python 2.3 alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.3 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.3.
4. PSF is making Python 2.3 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.3 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.3 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.3, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python 2.3, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").
2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.
3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permis-

sion to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".
3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.
4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the

extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

python 2.3.6

License for Python Imaging Library

Terms

The Python Imaging Library is

Copyright (c) 1997-2003 by Secret Labs AB

Copyright (c) 1995-2003 by Fredrik Lundh

By obtaining, using, and/or copying this software and/or its associated documentation, you agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its associated documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies, and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Secret Labs AB or the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Modules under this license

Imaging 1.1.4

License for Rdisc

Terms

Rdisc (this program) was developed by Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Rdisc without charge, and they may freely distribute it.

RDISC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Rdisc is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY RDISC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California

94043

Modules under this license

iputils 20020927

Software developed by RSA Data Security, Inc

Terms

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Modules under this license

ntp 4.1.2   openswan 2.4.13   openswan-kernel 2.4.9

More software developed by RSA Data Security, Inc

Terms

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message- Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Modules under this license

ppp 2.4.2_20030503

License for SSL

Terms

Copyright (C) 1995-1998 Eric Young (<eay@cryptsoft.com>) All rights reserved.

This package is an SSL implementation written by Eric Young (<eay@cryptsoft.com>). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (<tjh@cryptsoft.com>).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   > "This product includes cryptographic software written by Eric Young (<eay@cryptsoft.com>)"
   >
   > The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (<tjh@cryptsoft.com>)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE-

MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Modules under this license

DHCP 3.0.6	openswan 2.4.13
openssl 0.9.7a	openswan-kernel 2.4.9

License for stunnel

Terms

stunnel is distributed under GNU GPL version 2 license. See COPYRIGHT.GPL file for the full text of the license.

In addition, as a special exception, Michal Trojnara gives permission to link the code of this program with the OpenSSL library (or with modified versions of OpenSSL that use the same license as OpenSSL), and distribute linked combinations including the two. You must obey the GNU General Public License in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

Modules under this license

stunnel 4.04

Software developed by Sun Microsystems, Inc

Terms

Copyright (c) 2000 by Sun Microsystems, Inc. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that the above copyright notice appears in all copies.

SUN MAKES NO REPRESENTATION OR WARRANTIES ABOUT THE SUITABILITY OF THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SUN SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES.

Modules under this license

ppp 2.4.2_20030503

More software developed by Sun Microsystems, Inc

Terms

Copyright (c) 2001 by Sun Microsystems, Inc. All rights reserved.

Non-exclusive rights to redistribute, modify, translate, and use this software in source and binary forms, in whole or in part, is hereby granted, provided that the above copyright notice is duplicated in any source form, and that neither the name of the copyright holder nor the author is used to endorse or promote products derived from this software.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Modules under this license

ppp 2.4.2_20030503

License for Sun RPC

Terms

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue

Mountain View, California
94043

Modules under this license

openssl 0.9.7a rpc

License for termcap

COPYRIGHTS AND OTHER DELUSIONS

The BSD ancestor of this file had a standard Regents of the University of California copyright with dates from 1980 to 1993.

Some information has been merged in from a terminfo file SCO distributes. It has an obnoxious boilerplate copyright which I'm ignoring because they took so much of the content from the ancestral BSD versions of this file and didn't attribute it, thereby violating the BSD Regents' copyright.

Not that anyone should care. However many valid functions copyrights may serve, putting one on a termcap/terminfo file with hundreds of anonymous contributors makes about as much sense as copyrighting a wall-full of graffiti -- it's legally dubious, ethically bogus, and patently ridiculous.

This file deliberately has no copyright. It belongs to no one and everyone. If you claim you own it, you will merely succeed in looking like a fool. Use it as you like. Use it at your own risk. Copy and redistribute freely. There are no guarantees anywhere. Svaha!

Modules under this license

termcap 11.0.1

Software developed by Trusted Information Systems, Inc

Terms

Portions Copyright (c) 1995-1998 by Trusted Information Systems, Inc.

Permission to use, copy modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TRUSTED INFORMATION SYSTEMS DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TRUSTED INFORMATION SYSTEMS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION,

Modules under this license

DHCP 3.0.6

Software developed by Andrew Tridgell

Terms

Modules under this license

ppp 2.4.2_20030503

Software developed by Paul Vixie

Terms

Modules under this license

vixie-cron 3.0.1

Vovida Software License v 1.0

The Vovida Software License, Version 1.0

Copyright (c) 2000 Vovida Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names "VOCAL", "Vovida Open Communication Application Library", and "Vovida Open Communication Application Library (VOCAL)" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact vocal@vovida.org.
4. Products derived from this software may not be called "VOCAL", nor may "VOCAL" appear in their name, without prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DAMAGES IN EXCESS OF $1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Modules under this license

stund 0.92_Jun06

Software developed by Rayan S Zachariassen

Terms

Random number generator is:

> Copyright 1988 by Rayan S. Zachariassen, all rights reserved. This will be free software, but only when it is finished.

Used in ntp by permission of the author. If copyright is annoying to you, read no further. Instead, look up the reference, write me an equivalent to this and send it back to me.

Modules under this license

ntp 4.1.2

License for zlib

Terms

This software is provided ’as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly	Mark Adler
`<jloup@gzip.org>`	`<madler@alumni.caltech.edu>`

Modules under this license

gnupg 1.4.6	ppp 2.4.2_20030503
openswan-kernel 2.4.9	zlib 1.1.4

Software developed at University of California

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

Copyright (c) 1988 The Regents of the University of California. All rights reserved.

This code is derived from software written by Ken Arnold and published in UNIX Review, Vol. 6, No. 8.

vixie-cron 3.0.1

Copyright (c) 1985, 1987, 1988, 1989 The Regents of the University of California.

All rights reserved.

ntp 4.1.2 tzdata 2006a util-linux 2.11y

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Paul Vixie.

vixie-cron 3.0.1

Terms

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

Copyright (c) 1987, 1993 The Regents of the University of California. All rights reserved. (c) UNIX System Laboratories, Inc.

All or some portions of this file are derived from material licensed to the University of California by American Telephone and Telegraph Co. or Unix System Laboratories, Inc. and are reproduced herein with the permission of UNIX System Laboratories, Inc.

util-linux 2.11y

Copyright (c) 1982, 1986, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2004

The Regents of the University of California. All rights reserved.

arpwatch 2.1a13
DHCP 3.0.6
fdisk
ftp 0.17
iputils 20020927
openswan 2.4.13
openswan-kernel 2.4.9
util-linux 2.11y

Copyright (c) 1989, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Kim Letkeman.

util-linux 2.11y

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Muuss.

iputils 20020927

This code is derived from software contributed to Berkeley by Arthur David Olson of the National Cancer Institute.

ntp 4.1.2

This code is derived from software contributed to Berkeley by Chris Torek.

arpwatch 2.1a13 libdnet 1.11 ntp 4.1.2

This code is derived from software contributed to Berkeley by James A. Woods, derived from original work by Spencer Thomas and Joseph Orost.

ppp 2.4.2_20030503

Terms

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   > This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

ppp 2.4.2_20030503

ppp 2.4.2_20030503

Terms

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

libevent 1.1

readlink 1.18

Terms

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author must not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Appendix F. Obtaining Support for Your 3Com Products

3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at:

http://www.3com.com/voip/

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

3Com offers these support tools:

- 3Com Knowledgebase - Helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

  http://knowledgebase.3com.com/

  It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

http://www.3com.com/

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

You are entitled to *bug fix / maintenance releases* for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

http://www.3com.com/voip/

To obtain software releases that follow the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

Contact Us

3Com offers telephone, internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

http://www.3com.com/voip/

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at http://www.3com.com/voip/. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

http://csoweb4.3com.com/contactus/

Asia, Pacific Rim - Telephone Technical Support and Repair

Country	Telephone Number	Country	Telephone Number
Australia	1 800 678 515	Pakistan	+61 2 9937 5083
Hong Kong	800 933 486	Philippines	1235 61 266 2602 or 1800 1 888 9469
India	+61 2 9424 5179 or 000800 650 1111	P.R. of China	800 810 3033
Indonesia	001 803 61009	Singapore	800 6161 463
Japan	00531 616 439 or 03 5977 7991	S. Korea	080 333 3308
Malaysia	1800 801 777	Taiwan	00801 611 261
New Zealand	0800 446 398	Thailand	001 800 611 2000

You can also obtain support in this region at this e-mail address:

`<apr_technical_support@3com.com>`

Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048

Europe, Middle East, and Africa - Telephone Technical Support and Repair

From anywhere in these regions, call: +44 (0)1442 435529 From the following countries, call the appropriate number:

Country	Telephone Number	Country	Telephone Number
Austria	01 7956 7124	Luxembourg	342 0808128
Belgium	070 700 770	Netherlands	0900 777 7737
Denmark	7010 7289	Norway	815 33 047
Finland	01080 2783	Poland	00800 441 1357
France	0825 809 622	Portugal	707 200 123
Germany	01805 404 747	South Africa	0800 995 014
Hungary	06800 12813	Spain	9 021 60455
Ireland	01407 3387	Sweden	07711 14453
Israel	1800 945 3794	Switzerland	08488 50112
Italy	199 161346	U.K.	0870 909 3266

You can also obtain support in this region using this URL:

http://emea.3com.com/support/email.html

Latin America - Telephone Technical Support and Repair

Country	Telephone Number	Country	Telephone Number

Country	Telephone Number	Country	Telephone Number
Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region in the following ways:

- Spanish speakers, enter the URL: http://lat.3com.com/lat/support/form.html
- Portuguese speakers, enter the URL: http://lat.3com.com/br/support/form.html
- English speakers in Latin America, send e-mail to: <`lat_support_anc@3com.com`>

US and Canada - Telephone Technical Support and Repair

All locations:	Network Jacks; Wired or Wireless Network Interface Cards:	1 847-262-0070
	All other 3Com products:	1 800 876 3266

Index