

Figure 58 Network Settings > Home Networking > 5th Ethernet Port

State : Enable Disable

Apply Cancel

The following table describes the fields in this screen.

Table 37 Network Settings > Home Networking > 5th Ethernet Port

LABEL	DESCRIPTION
State	Select Enable to use the Ethernet WAN port as a LAN port on the Device.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to exit this screen without saving.

8.10 The MoCA Screen

The VMG4381-B10A supports MoCA (Multimedia over Coax Alliance), which allows multimedia and home networking over coaxial cable. Data communication and audio/video streaming are allowed at the same time.

Click [Network Settings > Home Networking > MoCA](#) to open this screen.

Figure 59 [Network Settings > Home Networking > MoCA](#)

MoCA Configuration

MoCA Privacy : Enable

Privacy Password : (The password length is 13~17 characters.)

Enable Auto Scan : Enable

Last Operating Frequency : MHz

Apply Cancel

The following table describes the fields in this screen.

Table 38 [Network Settings > Home Networking > MoCA](#)

LABEL	DESCRIPTION
MoCA Privacy	Select the check box to enable MoCA privacy. If this is enabled, all devices connected via coaxial cable must use the same password.
Privacy Password	Enter the password for the MoCA connection.
Enable Auto Scan	Select the check box to enable auto scan for the operating frequency.
Last Operating Frequency	Manually select an operating frequency from the droplist.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to exit this screen without saving.

8.11 The LAN VLAN Screen

Click **Network Setting** > **Home Networking** > **LAN VLAN** to open this screen. Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports.

Figure 60 Network Setting > Home Networking > LAN VLAN

Lan Port	TAG Operation	802.1P Mark	VLAN ID
Lan1	Unchange ▼	Unchange ▼	<input type="text"/>
Lan2	Unchange ▼	Unchange ▼	<input type="text"/>
Lan3	Unchange ▼	Unchange ▼	<input type="text"/>
Lan4	Unchange ▼	Unchange ▼	<input type="text"/>
MoCA	Unchange ▼	Unchange ▼	<input type="text"/>

Note:

- The Lan VLAN operation only work in downstream traffic.
- If TAG Operation is "Add", the VLAN tag only add when downstream packet is Untag.

The following table describes the labels in this screen.

Table 39 Network Setting > Home Networking > LAN VLAN

LABEL	DESCRIPTION
Lan Port	These represent the Device's LAN ports.
Tag Operation	Select what you want the Device to do to the IEEE 802.1q VLAN ID and priority tags of downstream traffic before sending it out through this LAN port. <ul style="list-style-type: none"> Unchange - Don't do anything to the traffic's VLAN ID and priority tags. Add - Add VLAN ID and priority tags to untagged traffic. Remove - Delete one tag from tagged traffic. If the frame has double tags, this removes the outer tag. This does not affect untagged traffic. Remark - Change the value of the outer VLAN ID and priority tags.
802.1P Mark	Use this option to set what to do for the IEEE 802.1p priority tags when you add or remark the tags for a LAN port's downstream traffic. Either select Unchange to not modify the traffic's priority tags or select an priority from 0 to 7 to use. The larger the number, the higher the priority.
VLAN ID	If you will add or remark tags for this LAN port's downstream traffic, specify the VLAN ID (from 0 to 4094) to use here.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.12 TFTP Server Name Screen

Click **Network Setting** > **Home Networking** > **TFTP Server Name** to open this screen. Use this screen to access the TFTP (Trivial File Transfer Protocol) Server using DHCP option 66.

Figure 61 **Network Setting** > **Home Networking** > **TFTP Server Name**

TFTP Server Name :

The following table describes the labels in this screen.

Table 40 [Network Setting > Home Networking > TFTP Server Name](#)

<u>LABEL</u>	<u>DESCRIPTION</u>
TFTP Server Name	Type a name for the TFTP Server. This allows you to access the TFTP server using DHCP option 66. However, option 66 (open standard) supports only the IP address of the hostname or a single TFTP server.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

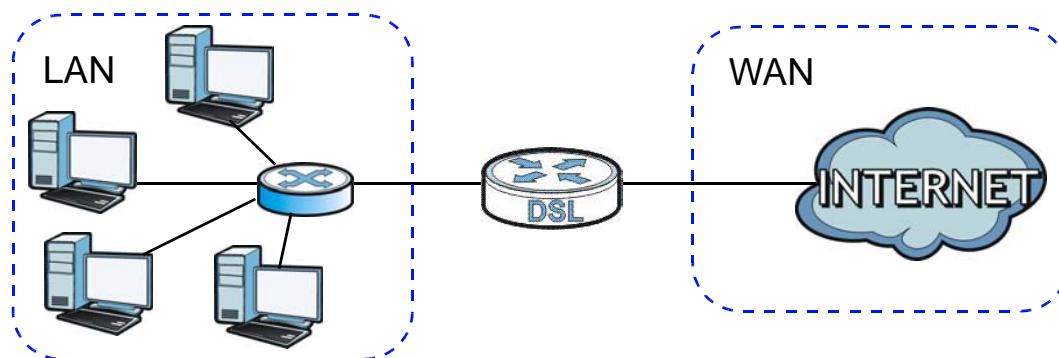
8.13 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.13.1 LANs, WANs and the Device

The actual physical connection determines whether the Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 62 LAN and WAN IP Addresses



8.13.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Device as a DHCP server or disable it. When configured as a server, the Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.13.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Device supports the IPCP DNS server extensions through the DNS proxy feature.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

8.13.4 LAN TCP/IP

The Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

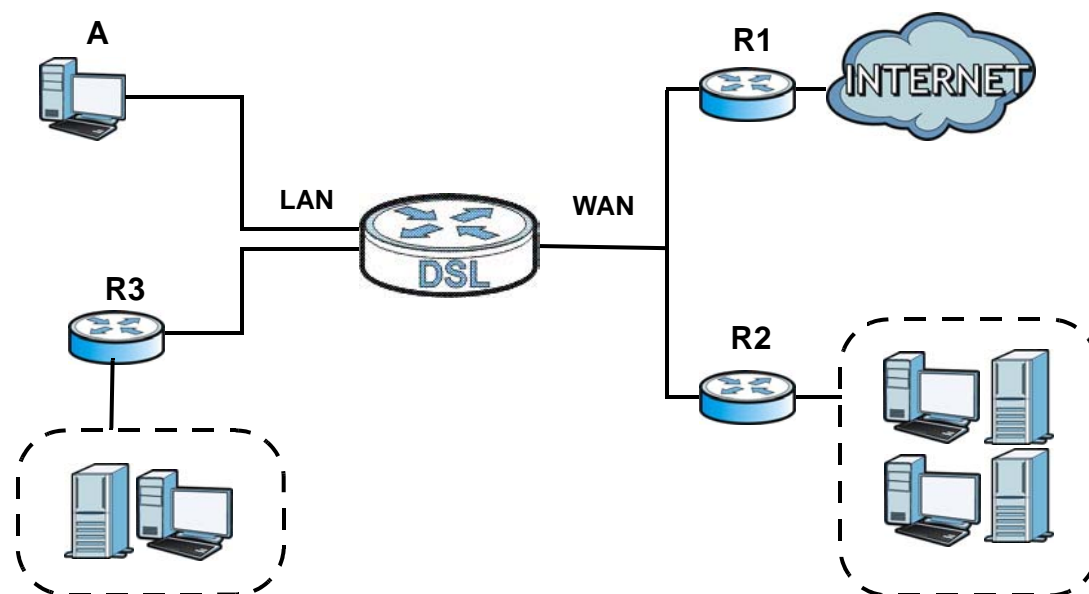
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

9.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Device's LAN interface. The Device routes most traffic from **A** to the Internet through the Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate WAN network behind a router **R3** connected to the LAN.

Figure 63 Example of Routing Topology



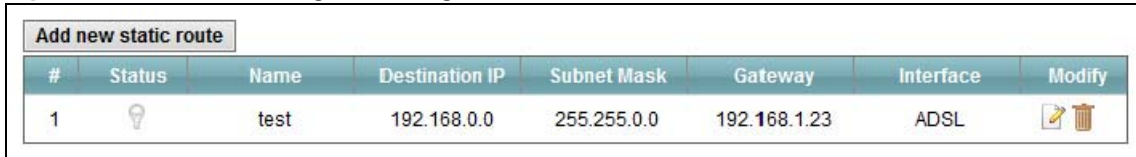
9.1.1 What You Can Do in this Chapter

- Use the **Static Route** screen to view and set up static routes on the Device ([Section 9.2 on page 158](#)).
- Use the **Policy Forwarding** screen to configure policy routing on the Device. ([Section 9.3 on page 159](#)).
- Use the **RIP** screen to set up RIP settings on the Device. ([Section 9.4 on page 161](#)).

9.2 The Routing Screen

Use this screen to view and configure the static route rules on the Device. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 64 Network Setting > Routing > Static Route



Add new static route							
#	Status	Name	Destination IP	Subnet Mask	Gateway	Interface	Modify
1		test	192.168.0.0	255.255.0.0	192.168.1.23	ADSL	

The following table describes the labels in this screen.

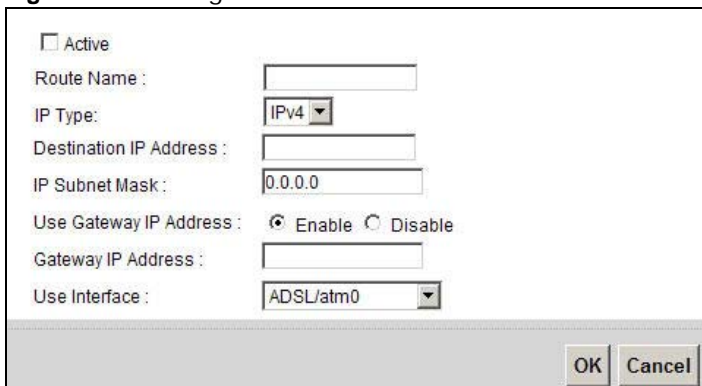
Table 41 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.
Modify	Click the Edit icon to edit the static route on the Device. Click the Delete icon to remove a static route from the Device. A window displays asking you to confirm that you want to delete the route.

9.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 65 Routing: Add/Edit



Active

Route Name :

IP Type:

Destination IP Address :

IP Subnet Mask :

Use Gateway IP Address : Enable Disable

Gateway IP Address :

Use Interface :

The following table describes the labels in this screen.

Table 42 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select this to enable the static route. Clear this to disable this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is IPv4 or IPv6 .
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
IP Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. If you want to use the gateway IP address, select Enable .
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.3 The Policy Forwarding Screen

Traditionally, routing is based on the destination address only and the Device takes the shortest path to forward a packet. Policy forwarding allows the Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

The **Policy Forwarding** screen let you view and configure routing policies on the Device. Click **Network Setting > Routing > Policy Forwarding** to open the following screen.

Figure 66 Network Setting > Routing > Policy Forwarding

Add new Policy Forward Rule												
#	Policy Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Destination IP	Destination Subnet Mask	Destination Port	Destination MAC	WAN	Modify
1	test	192.168.1.35	255.255.255.0	TCP			192.168.1.30	255.255.255.0			ADSL	 

The following table describes the labels in this screen.

Table 43 Network Setting > Routing > Policy Forwarding

LABEL	DESCRIPTION
Add new Policy Forward Rule	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.

Table 43 Network Setting > Routing > Policy Forwarding (continued)

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
WAN	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to edit this policy. Click the Delete icon to remove a policy from the Device. A window displays asking you to confirm that you want to delete the policy.

9.3.1 Add/Edit Policy Forwarding

Click **Add new Policy Forward Rule** in the **Policy Forwarding** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 67 Policy Forwarding: Add/Edit

The following table describes the labels in this screen.

Table 44 Policy Forwarding: Add/Edit

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (TCP or UDP).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
WAN	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the Broadband screens.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.4 The RIP Screen

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 68 RIP

#	Interface	Version	Operation	Enabled
1	atm0	2 ▼	Passive ▼	<input type="checkbox"/>

Note:
RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

The following table describes the labels in this screen.

Table 45 RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Device sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select Passive to have the Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the Device advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Quality of Service (QoS)

10.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 10.3 on page 165](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 10.4 on page 166](#)).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers ([Section 10.5 on page 168](#)).
- The **Policer Setup** screen lets you add, edit or delete QoS policers ([Section 10.5 on page 168](#)).
- The **Monitor** screen lets you view the Device's QoS-related packet statistics ([Section 10.7 on page 175](#)).

10.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

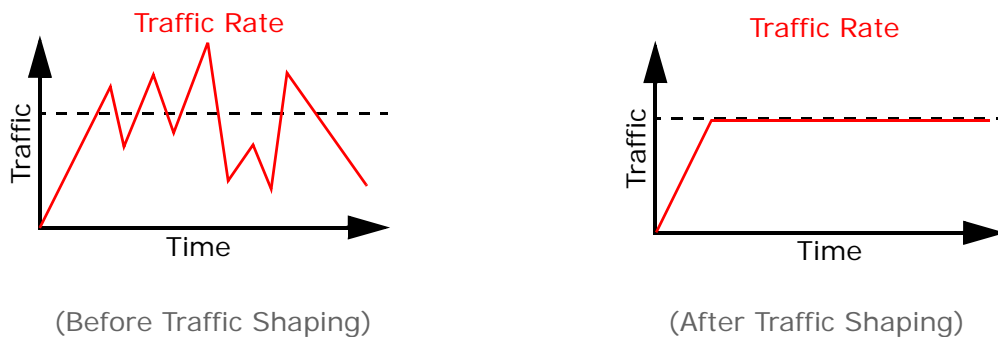
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

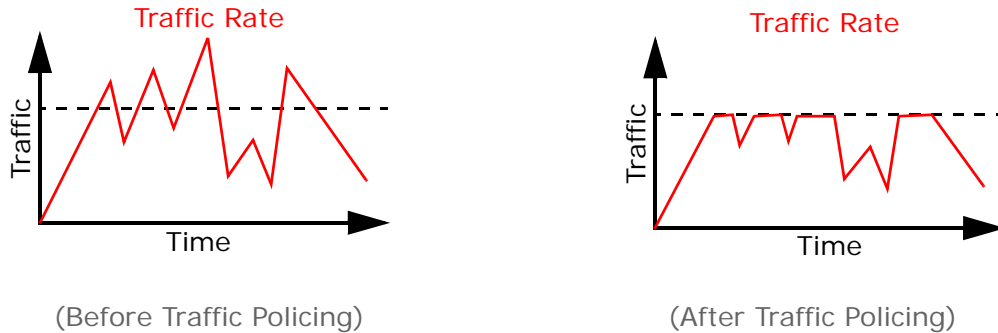
Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



The Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Section 10.8 on page 176](#) for more information on each metering algorithm.

10.3 The Quality of Service General Screen

Click **Network Setting > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See [Section 10.1 on page 163](#) for more information.

Figure 69 Network Settings > QoS > General

QoS Enable Disable (settings are invalid when disabled)

WAN Managed Upstream Bandwidth : (kbps)

LAN Managed Downstream Bandwidth : (kbps)

Upstream traffic priority Assigned by: ▼

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.

If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 46 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the Enable check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interfaces' actual transmission speed. The Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.</p> <p>You can also set this number lower than the interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.</p>
LAN Managed Downstream Bandwidth	<p>Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.</p> <p>You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the Device automatically sets this to the LAN interfaces' maximum supported connection speed.</p>
Upstream traffic priority Assigned by	<p>Select how the Device assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> • None: Disables auto priority mapping and has the Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. • IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. • Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

10.4 The Queue Setup Screen

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 70 Network Setting > QoS > Queue Setup

Add new Queue								
#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (Kbps)	Modify
1		DefaultQueue	WAN	8	1	DT	0	
2		PriQ1	WAN	1	1	DT	0	
3		PriQ2	WAN	2	1	DT	0	
4		PriQ3	WAN	3	1	DT	0	
5		PriQ4	WAN	4	1	DT	0	
6		PriQ5	WAN	5	1	DT	0	
7		PriQ6	WAN	6	1	DT	0	
8		PriQ7	WAN	7	1	DT	0	

Note:
maximum 8 configurable entries for WAN port, and maximum 3 configurable entries for each LAN port.
If queue is deleted, then related classifiers will be removed too.

The following table describes the labels in this screen.

Table 47 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

Click **Add new Queue** or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 71 Queue Setup: Add

The following table describes the labels in this screen.

Table 48 Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.5 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 72 Network Setting > QoS > Class Setup

Add new Classifier								
#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
1		example	From Intf: LAN Ether Type: IP	Unchange	Unchange	Unchange	DefaultQueue	

The following table describes the labels in this screen.

Table 49 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
#	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

10.5.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 73 Class Setup: Add/Edit

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active

Class Name : _____

Classification Order : Last ▾

Step2: Criteria configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- Basic**

From Interface : LAN ▾

Ether Type : NA ▾
- Source**

<input type="checkbox"/> Address	_____	Subnet Netmask	_____	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	_____~_____			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	_____	MAC Mask	_____	<input type="checkbox"/> Exclude
- Destination**

<input type="checkbox"/> Address	_____	Subnet Netmask	_____	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	_____~_____			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	_____	MAC Mask	_____	<input type="checkbox"/> Exclude
- Others**

<input type="checkbox"/> Service	Age of Empires ▾	<input type="checkbox"/> Exclude
<input type="checkbox"/> IP protocol	TCP ▾	<input type="checkbox"/> Exclude
<input type="checkbox"/> DHCP	_____ ▾	<input type="checkbox"/> Exclude
<input type="checkbox"/> Packet Length	_____~_____	<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP	_____ (0~63)	<input type="checkbox"/> Exclude
<input type="checkbox"/> 802.1P	0 BE ▾	<input type="checkbox"/> Exclude
<input type="checkbox"/> VLAN ID	_____ (0~4094)	<input type="checkbox"/> Exclude
<input type="checkbox"/> TCP ACK		<input type="checkbox"/> Exclude

Step3: Packet modification

The content of the packet can be modified by applying the following settings:

DSCP Mark : Unchange ▾ _____ (0~63)

802.1P Mark : Unchange ▾ _____

VLAN ID : Unchange ▾ _____ (0~4094)

Step4: Policy Forwarding

This module can route or bridge packets to certain interface according to the class settings:

Forward To Interface : Unchange ▾

Step5: Outgoing queue selection

Outgoing queue decide the priority of the traffic and how traffic should be shaped in the WAN interface. Choose "None" if you don't want to apply outgoing queue

To Queue Index : DefaultQueue ▾

Apply Cancel

The following table describes the labels in this screen.

Table 50 Class Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select this to enable this classifier.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list.
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IP , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 50 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Service	<p>This field is available only when you select IP in the Ether Type field.</p> <p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.</p>
IP Protocol	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p>
DHCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p>
Packet Length	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.</p>
DSCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p>
802.1P	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number.</p>
TCP ACK	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
Exclude	<p>Select this option to exclude the packets that match the specified criteria from this classifier.</p>
DSCP Mark	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select Mark, enter a DSCP value with which the Device replaces the DSCP field in the packets.</p> <p>If you select Unchange, the Device keep the DSCP field in the packets.</p>
802.1P Mark	<p>Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets.</p> <p>If you select Unchange, the Device keep the 802.1p priority field in the packets.</p>
VLAN ID	<p>If you select Remark, enter a VLAN ID number with which the Device replaces the VLAN ID of the frames.</p> <p>If you select Remove, the Device deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the Device treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the Device keep the VLAN ID in the packets.</p>
Forward to Interface	<p>Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange, the Device forward traffic of this class according to the default routing table.</p>

Table 50 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 74 Network Setting > QoS > Policer Setup

#	Status	Name	Regulated Classes	Meter Type	Rule	Action	Modify
1		test	Class 1: example	SimpleTokenBucket	Committed Rate: 200Kbps Committed Burst Size: 300Kbyte	Conforming Action: Pass Non-Conforming Action: Drop	

The following table describes the labels in this screen.

Table 51 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows the how the policer has the Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the Edit icon to edit the policer. Click the Delete icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

10.6.1 Add/Edit a QoS Policer

Click **Add new Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 75 Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 52 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to activate this policer.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. The Simple Token Bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size. The Single Rate Three Color Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The Two Rate Three Color Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Conforming Action	Specify what the Device does for packets within the committed rate and burst size (green-marked packets). <ul style="list-style-type: none"> Pass: Send the packets without modification. DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Non-Conforming Action	Specify what the Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). <ul style="list-style-type: none"> Drop: Discard the packets. DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.

Table 52 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Available Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.
Selected Class	Highlight a QoS classifier in the Available Class box and use the > button to move it to the Selected Class box. To remove a QoS classifier from the Selected Class box, select it and use the < button.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.7 The QoS Monitor Screen

To view the Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 76 Network Setting > QoS > Monitor

Monitor
Refresh Interval : ▾

Status :

- Interface Monitor**

#	Name	Pass Rate(bps)	Drop Rate(bps)
1	WAN	0	0
2	LAN		
- Queue Monitor**

#	Name	Pass Rate(bps)	Drop Rate(bps)
---	------	----------------	----------------

The following table describes the labels in this screen.

Table 53 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Device to update this screen. Select No Refresh to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Device.
Pass Rate	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate	This shows how many packets assigned to this queue are dropped.

10.8 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 54 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Device, the Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Device. On the Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 55 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250

Table 55 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size, so the bucket can hold up to b tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Device treats the packet in either one of the following ways:

In traffic shaping:

- Holds it in the queue until enough tokens are available in the bucket.

In traffic policing:

- Drops it.
- Transmits it but adds a DSCP mark. The Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

Network Address Translation (NAT)

11.1 Overview

This chapter discusses how to configure NAT on the Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 11.2 on page 182](#)).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network ([Section 11.3 on page 185](#)).
- Use the **Port Triggering** screen to add and configure the Device's trigger port settings ([Section 11.4 on page 186](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.5 on page 189](#)).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the Device ([Section 11.6 on page 190](#)).
- Use the **Address Mapping** screen to configure the Device's address mapping settings ([Section 11.7 on page 190](#)).

11.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the

WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See [Section 11.8 on page 192](#) for advanced technical information on NAT.

11.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

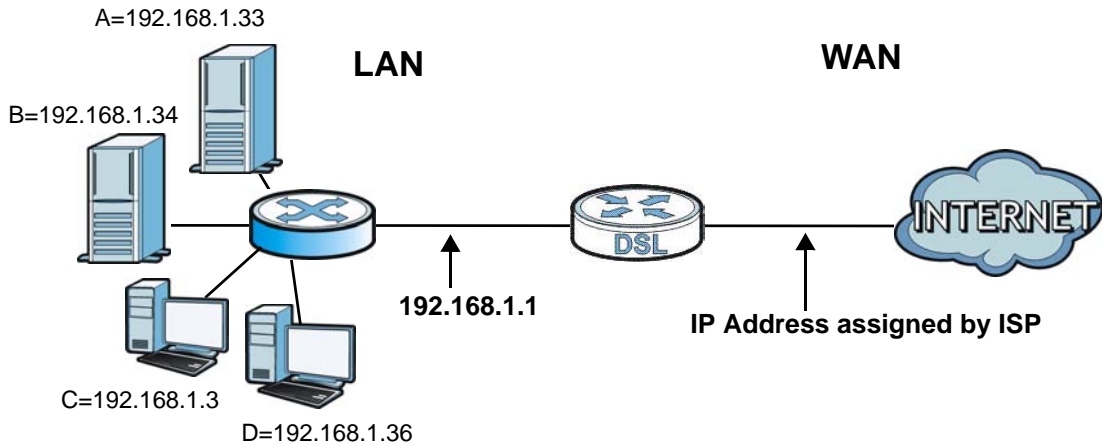
The most often used port numbers and services are shown in [Appendix F on page 353](#). Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 77 Multiple Servers Behind NAT Example



Click **Network Setting > NAT > Port Forwarding** to open the following screen.

See [Appendix F on page 353](#) for port numbers commonly used for particular services.

Figure 78 Network Setting > NAT > Port Forwarding

Add new rule											
#	Status	Service...	WAN In...	WAN IP	Server ...	Start Port	End Port	Transl...	Transl...	Protocol	Modify
1		test	ADSL	192.168.1	172.23...	21	21	21	21	TCP	

The following table describes the fields in this screen.

Table 56 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service's name.
WAN Interface	This shows the WAN interface through which the service is forwarded.
WAN IP	This field displays the incoming packet's destination IP address.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This shows the IP protocol supported by this virtual server, whether it is TCP , UDP , or TCP/UDP .
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.2.1 Add/Edit Port Forwarding

Click **Add new rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

Figure 79 Port Forwarding: Add/Edit

The following table describes the labels in this screen.

Table 57 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Clear the checkbox to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
WAN IP	Enter the WAN IP address for which the incoming service is destined. If the packet's destination IP address doesn't match the one specified here, the port forwarding rule will not be applied.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
Translation Start Port	This shows the port number to which you want the Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.

Table 57 Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

11.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Setting > NAT > Applications**. The following screen appears.

Figure 80 Network Setting > NAT > Applications

#	Application Forwarded	WAN interface	Server IP Address	Modify
1	Remote Desktop Connection	ADSL	192.168.1.23	

The following table describes the labels in this screen.

Table 58 Network Setting > NAT > Applications

LABEL	DESCRIPTION
Add new application	Click this to add a new NAT application rule.
Application Forwarded	This field shows the type of application that the service forwards.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Server IP Address	This field displays the destination IP address for the service.
Modify	Click the Delete icon to delete the rule.

11.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add new application** in the **Applications** screen to open the following screen.

Figure 81 Applications: Add

The following table describes the labels in this screen.

Table 59 Applications: Add

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface that you want to apply this NAT rule to.
Server IP Address	Enter the inside IP address of the application here.
Application Category	Select the category of the application from the drop-down list box.
Application Forwarded	Select a service from the drop-down list box and the Device automatically configures the protocol, start, end, and map port number that define the service.
View Rule	Click this to display the configuration of the service that you have chosen in Application Forwarded .
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

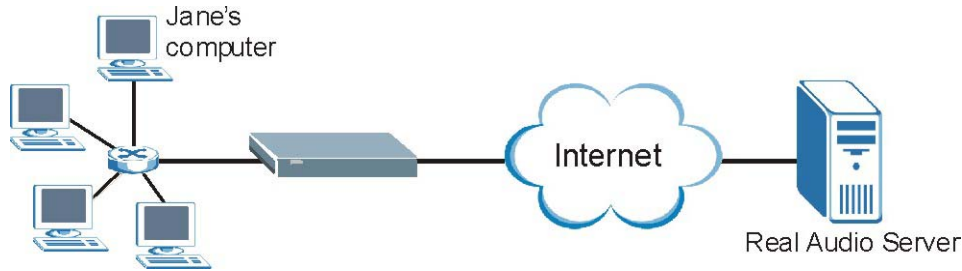
11.4 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Device's WAN port receives a response with a specific port number and protocol ("open" port), the Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 82 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the Device to record Jane's computer IP address. The Device associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Device's trigger port settings.

Figure 83 Network Setting > NAT > Port Triggering

Add new rule										
#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
1		Test	ADSL	5191	5191	TCP or UDP	5191	5191	TCP	

The following table describes the labels in this screen.

Table 60 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.

Table 60 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

Figure 84 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 61 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to enable this rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .

Table 61 Port Triggering: Configuration Add/Edit (continued)

LABEL	DESCRIPTION
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

11.5 The DMZ Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 85 Network Setting > NAT > DMZ

Default Server Address :

Note:
 Enter IP address and click "Apply" to activate the DMZ host.
 Clear the IP address field and click "Apply" to deactivate the DMZ host.

The following table describes the fields in this screen.

Table 62 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the NAT Port Forwarding screen. Note: If you do not assign a Default Server Address , the Device discards all packets received for ports that are not specified in the NAT Port Forwarding screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

11.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Device registers with the SIP register server, the SIP ALG translates the Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Device is behind a SIP ALG.

Use this screen to enable and disable the NAT and SIP (VoIP) ALG in the Device. To access this screen, click **Network Setting > NAT > ALG**.

Figure 86 Network Setting > NAT > ALG

NAT ALG : Enable Disable (settings are invalid when disabled)

SIP ALG : Enable Disable

Apply Cancel

The following table describes the fields in this screen.

Table 63 Network Setting > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

11.7 The Address Mapping Screen

Ordering your rules is important because the Device applies the rules in the order that you specify. When a rule matches the current packet, the Device takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

Figure 87 Network Setting > NAT > Address Mapping

Add new rule

Set	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.32		10.1.2.3		One-to-One	

The following table describes the fields in this screen.

Table 64 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Set	This is the index number of the address mapping set.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
Type	This is the address mapping type. One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
Modify	Click the Edit icon to go to the screen where you can edit the address mapping rule. Click the Delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

11.7.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 88 Address Mapping: Add/Edit

The screenshot shows a configuration window for adding or editing an address mapping rule. It contains the following elements:

- Type:** A dropdown menu currently set to "One-to-One".
- Local Start IP:** An empty text input field.
- Local End IP:** An empty text input field.
- Global Start IP:** An empty text input field.
- Global End IP:** An empty text input field.
- Set:** A dropdown menu currently set to "1".
- Buttons:** "OK" and "Cancel" buttons located at the bottom right of the window.

The following table describes the fields in this screen.

Table 65 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Type	Choose the IP/port mapping type from one of the following. One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
Set	Select the number of the mapping set for which you want to configure.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

11.8 Technical Reference

This part contains more information regarding NAT.

11.8.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 66 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.8.2 What NAT Does

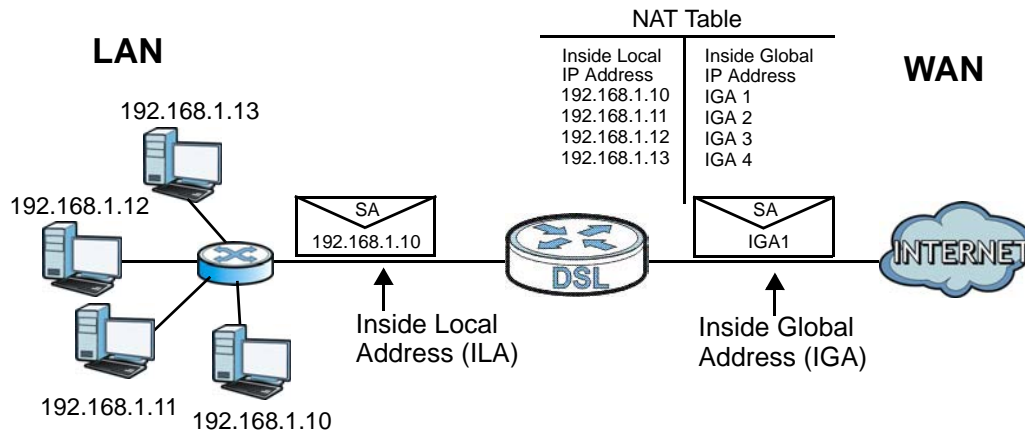
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

11.8.3 How NAT Works

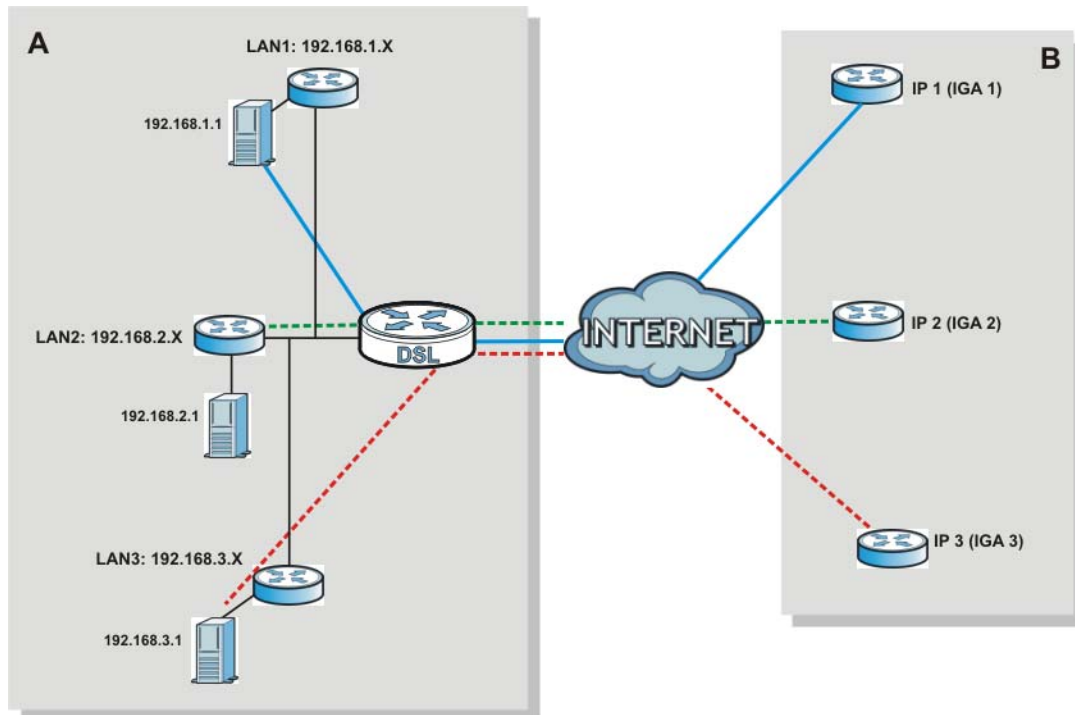
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 89 How NAT Works



11.8.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Device can communicate with three distinct WAN networks.

Figure 90 NAT Application With IP Alias

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 67 Services and Port Numbers

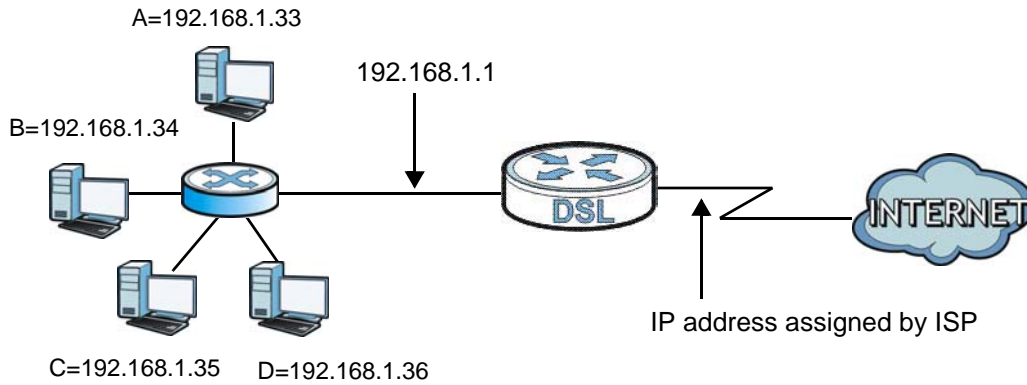
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a

third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 91 Multiple Servers Behind NAT Example



Dynamic DNS Setup

12.1 Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 198](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Device ([Section 12.3 on page 199](#)).

12.1.2 What You Need To Know

DYNDNS Wildcard



Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Figure 92 Network Setting > DNS > DNS Entry

Add new DNS entry			
#	FQDN	IP Address	Modify
1	Test.SBG3500	192.168.1.56	 

The following table describes the fields in this screen.

Table 68 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add new DNS entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Hostname	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule.

12.2.1 Add/Edit DNS Entry

You can manually add or edit the Device's DNS name and IP address entry. Click **Add new DNS entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 93 DNS Entry: Add/Edit

The following table describes the labels in this screen.

Table 69 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

12.3 The Dynamic DNS Screen

Use this screen to change your Device's DDNS. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 94 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 70 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select Enable to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Hostname	Type the domain name assigned to your Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.

Table 70 Network Setting > DNS > > Dynamic DNS (continued)

LABEL	DESCRIPTION
Password	Type the password assigned to you.
Email	If you select TZO in the Service Provider field, enter the user name you used to register for this service.
Key	If you select TZO in the Service Provider field, enter the password you used to register for this service.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Interface Group

13.1 Overview

By default, all LAN and WAN interfaces on the Device are in the same group and can communicate with each other. Create interface groups to have the Device assign the IP addresses in different domains to different groups. Each group acts as an independent network on the Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

13.1.1 What You Can Do in this Chapter

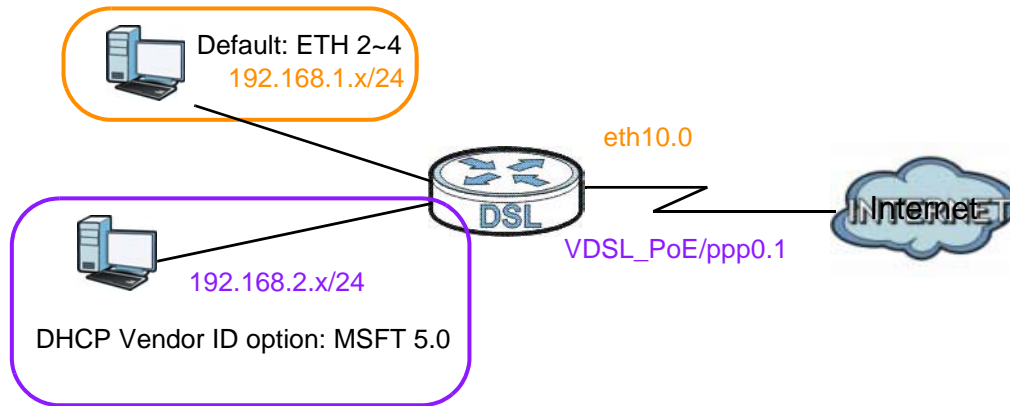
The **Interface Group** screens let you create multiple networks on the Device ([Section 13.2 on page 201](#)).

13.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Device assigns to the clients in the default and/or user-defined groups. If you set the Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 8 on page 133](#) for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 95 Interface Grouping Application

Click **Network Setting > Interface Group** to open the following screen.

Figure 96 Network Setting > Interface Group

Add New Interface Group					
St...	Group Name	802.1q	IPv4	Port Members	Modify
	Default	1	172.23.30.219/...	Untagged: LAN1,LAN2,LAN3,LAN4,WL_ZyXEL5F5B4 Tagged: -	

Note:
When new group is created, you can go to Network Setting->LAN->LAN Setup to select the group name and configure the DHCP or other settings for the new subnet.

The following table describes the fields in this screen.

Table 71 Network Setting > Interface Group

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the Delete icon to remove the group.
Add	Click this button to create a new group.

13.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

Figure 97 Interface Group Configuration

Group Name :

802.1p : ▼

802.1q : (1~4094)

VLAN Port Membership

Port	Member	Tagged
LAN1	<input type="checkbox"/>	<input type="checkbox"/>
LAN2	<input type="checkbox"/>	<input type="checkbox"/>
LAN3	<input type="checkbox"/>	<input type="checkbox"/>
LAN4	<input type="checkbox"/>	<input type="checkbox"/>
WL_ZyXEL5F5B4	<input type="checkbox"/>	
WL_ZyXEL5F5B4_Guest1	<input type="checkbox"/>	
WL_ZyXEL5F5B4_Guest2	<input type="checkbox"/>	
WL_ZyXEL5F5B4_Guest3	<input type="checkbox"/>	

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Remove
<input type="button" value="Add"/>			

Note:
If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

The following table describes the fields in this screen.

Table 72 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface and up to one ATM interface. Select None to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the Available LAN Interfaces list and use the left arrow to move them to the Grouped LAN Interfaces list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the Grouped LAN Interfaces , use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click Add to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 13.2.2 on page 204 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Remove	Click the Remove icon to delete this rule from the Device.

Table 72 Interface Group Configuration (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to exit this screen without saving.

13.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 98 Interface Grouping Criteria

The following table describes the fields in this screen.

Table 73 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard on DHCP option 60 option	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.

Table 73 Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
DUID type	<p>Select DUID-LLT (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device.</p> <p>Select DUID-EN (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor's registered enterprise number.</p> <p>Select DUID-LL (DUID Based on Link-layer Address) to enter the device's hardware type and hardware address (MAC address) in the following fields.</p> <p>Select Other to enter any string that identifies the device in the DUID field.</p>
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the device.
Model Name	Enter the model name of the device.
Serial Number	Enter the serial number of the device.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to exit this screen without saving.

USB Service

14.1 Overview

The Device has a USB port used to share files via a USB memory stick or a USB hard drive. In the **USB Service** screens, you can enable file-sharing server, media server, and printer server.

14.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server ([Section 14.2 on page 208](#)).
- Use the **Media Server** screen to enable or disable the sharing of media files ([Section 14.3 on page 210](#)).
- Use the **Printer Server** screen to enable the print server ([Section 14.4 on page 211](#)).

14.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

14.1.2.1 About File Sharing

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a “share”. If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS

protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

14.1.2.2 About Printer Server

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the RAW (port 9100) protocol.

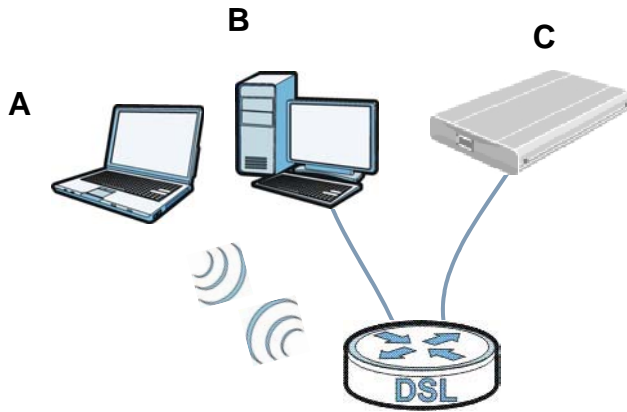
The following OSs support Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

14.2 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your Device with users on your network.

The following figure is an overview of the Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

Figure 99 File Sharing Overview

The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

14.2.1 Before You Begin

Make sure the Device is connected to your network and turned on.

- 1 Connect the USB device to one of the Device's USB port. Make sure the Device is connected to your network.
- 2 The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

Use this screen to set up file sharing using the Device. To access this screen, click **Network Setting > USB Service > File Sharing**.

Figure 100 Network Setting > USB Service > File Sharing

File Sharing Services : Enable Disable

Host Name

Each field is described in the following table.

Table 74 Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
File Sharing Services	Select Enable to activate file sharing through the Device.
Host Name	Enter the host name on the share.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

14.3 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Device (without having to copy them to another computer). The Device can function as a DLNA-compliant media server. The Device streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Device's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

Figure 101 Network Setting > USB Service > Media Server



The following table describes the labels in this menu.

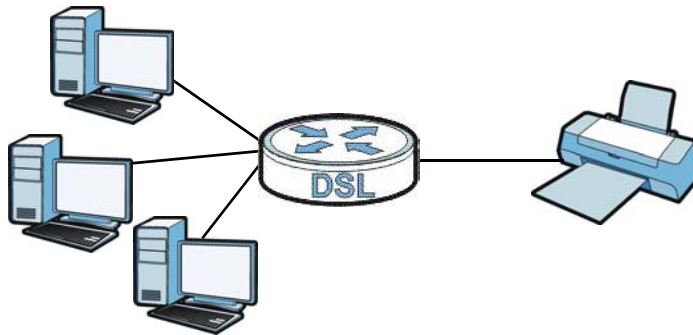
Table 75 Network Setting > USB Service > Media Server

LABEL	DESCRIPTION
Media Server	Select Enable to have the Device function as a DLNA-compliant media server. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

14.4 The Printer Server Screen

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then adding the printer on the computers connected to your network. See [Section 4.11 on page 62](#) for instructions on adding a printer on your computer.

Figure 102 Sharing a USB Printer



14.4.1 Before You Begin

To configure the print server you need the following:

- Your Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your Device.
- A USB printer with the driver already installed on your computer.
- See [Section 4.11 on page 62](#) for instructions on adding a printer on your computer.

Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

Use this screen to enable or disable sharing of a USB printer via your Device.

To access this screen, click **Network Setting > USB Service > Printer Server**.

Figure 103 Network Setting > USB Service > Printer Server

Print Server :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Printer Name :	<input type="text" value="USB_PRINTER"/>
Make and model :	<input type="text" value="USB_PRINTER"/>
Printer Name :	N/A
Note: To use the print server, define a network printer with URL http://192.168.1.1:631/printers/USB_PRINTER .	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this menu.

Table 76 Network Setting > USB Service > Print Server

LABEL	DESCRIPTION
Printer Server	Select Enable to have the Device share a USB printer.
Printer Name	Enter the name of the printer.
Make and model	Enter the manufacturer and model number of the printer.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

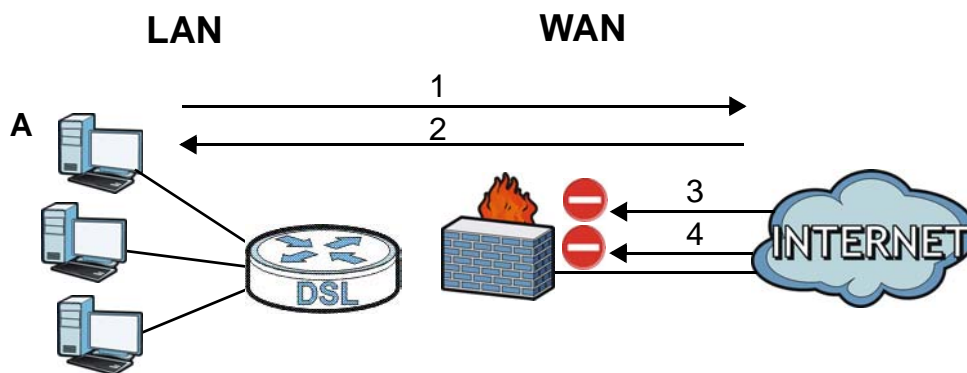
15.1 Overview

This chapter shows you how to enable and configure the Device's security settings. Use the firewall to protect your Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 104 Default Firewall Action



15.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Device ([Section 15.2 on page 215](#)).
- Use the **Service** screen to add or remove predefined Internet services and configure firewall rules ([Section 15.3 on page 215](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 15.4 on page 217](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 15.5 on page 220](#)).

15.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

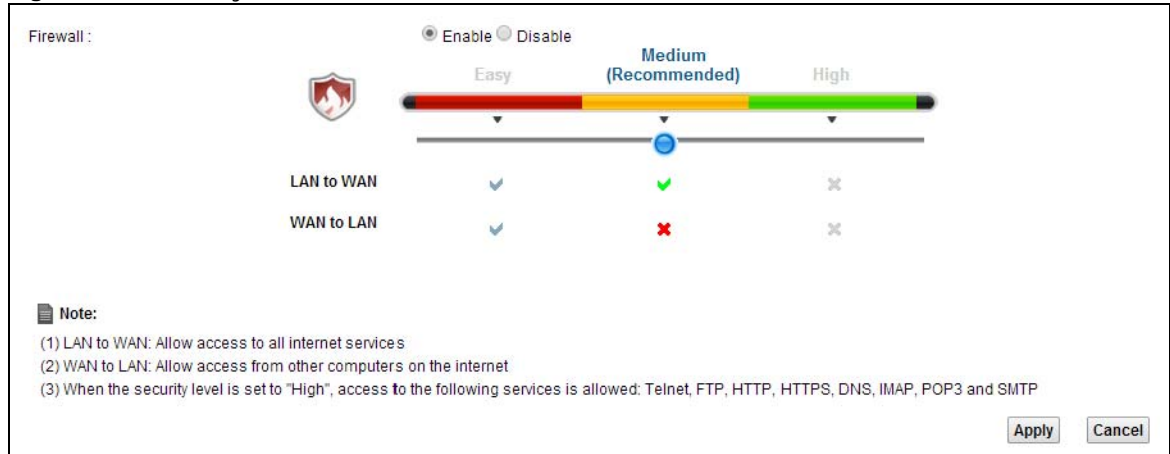
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

15.2 The Firewall Screen

Use this screen to set the security level of the firewall on the Device. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security** > **Firewall** to display the **General** screen.

Figure 105 Security > Firewall > General



The following table describes the labels in this screen.

Table 77 Security > Firewall > General

LABEL	DESCRIPTION
Firewall	Select Enable to activate the firewall feature on the Device.
Easy	Select Easy to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select Medium to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select High to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

15.3 The Service Screen

You can configure customized services and port numbers in the **Service** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix F on page 353](#) for some examples. [This screen is not applicable to VMG4381.](#)

Click **Security** > **Firewall** > **Service** to display the following screen.

Figure 106 Security > Firewall > Service



The following table describes the labels in this screen.

Table 78 Security > Firewall > Service

LABEL	DESCRIPTION
Add new service entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol (TCP , UDP , ICMP , or TCP/UDP) and the port number or range of ports that defines your customized service. Other and the protocol number displays if the service uses another IP protocol.
Modify	Click the Edit icon to edit the entry. Click the Delete icon to remove this entry.

15.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add new service entry** or the edit icon next to an existing service rule in the **Service** screen to display the following screen.

Figure 107 Service: Add/Edit

Protocol:

Source Port: -

Destination Port: -

Rule List

Protocol	Ports/Protocol Number	Modify
Service Name: <input type="text"/>		
Service Description: <input type="text"/>		

The following table describes the labels in this screen.

Table 79 Service: Add/Edit

LABEL	DESCRIPTION
Protocol	Choose the IP protocol (TCP , UDP , ICMP , or Other) that defines your customized port from the drop-down list box. Select Other to be able to enter a protocol number.
Source/ Destination Port	These fields are displayed if you select TCP or UDP as the IP port. Select Single to specify one port only or Range to specify a span of ports that define your customized service. If you select Any , the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Protocol Number	This field is displayed if you select Other as the protocol. Enter the protocol number of your customized port.
Add	Click this to add the protocol to the Rule List below.
Rule List	
Protocol	This is the IP port (TCP , UDP , ICMP , or Other) that defines your customized port.
Ports/Protocol Number	For TCP , UDP , ICMP , or TCP/UDP protocol rules this shows the port number or range that defines the custom service. For other IP protocol rules this shows the protocol number.
Modify	Click the Delete icon to remove the rule.
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Service Description	Enter a description for your customized port.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

15.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 108 Security > Firewall > Access Control

Rules Storage Space usage(%): 2%

Direction: From To

#	En	Name	From	To	Src IP	Dst IP	Service	Action	Modify
1		test	WAN	LAN	Any	Any	None: Any->Any	ACCEPT	

Note:

1. If an ACL rule is created that results in loss of management (e.g. Deny Any to Router) the unit must be restored to factory defaults.
2. An 'L' in the 'En' field of an ACL rule indicates logging enabled.
An 'R' in the 'En' field of an ACL rule indicates rate limit enabled.
An 'S' in the 'En' field of an ACL rule indicates scheduler rule set.

The following table describes the labels in this screen.

Table 80 Security > Firewall > Access Control

LABEL	DESCRIPTION
DoS Protection	DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Select the Enable check box to enable protection against DoS attacks.
Add new ACL rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to Any .
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to Any .
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (DROP), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (REJECT) or allows the passage of packets (ACCEPT).
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the Move To icon to change the order of the rule. Enter the number in the # field.

15.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 109 Access Control: Add/Edit

Filter Name:	<input type="text"/>
Order:	<input type="text" value="1"/>
Select Source Device:	<input type="text" value="Specific IP Address"/>
Source IP address:	<input type="text"/> [/prefix length]
Select Destination Device:	<input type="text" value="Specific IP Address"/>
Destination IP address:	<input type="text"/> [/prefix length]
IP Type:	<input type="text" value="IPv4"/>
Select Service:	<input type="text" value="Specific Service"/>
Protocol:	<input type="text"/>
Custom Source Port:	<input type="text"/> (port or port:port)
Custom Destination Port:	<input type="text"/> (port or port:port)
Policy:	<input type="text" value="ACCEPT"/>
Direction:	<input type="text" value="WAN to LAN"/>
Enable Rate Limit	<input type="checkbox"/>
	<input type="text"/> packet(s) per <input type="text" value="Minute"/> (1-512)
Scheduler Rules:	<input type="text"/> Add New Rule
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 81 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source Device	Select the source device to which the ACL rule applies. If you select Specific IP Address , enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select Specific IP Address , enter the destination IP address in the field below.
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is IPv4 or IPv6 .
Select Protocol	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the Security > Firewall > Service > Add screen display in this list. If you want to configure a customized protocol, select Specific Service .

Table 81 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Protocol	This field is displayed only when you select Specific Protocol in Select Protocol . Choose the IP port (TCP/UDP , TCP , UDP , ICMP , or ICMPv6) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select Specific Protocol in Select Protocol . Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select Specific Protocol in Select Protocol . Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click Add New Rule . This will bring you to the Security > Scheduler Rules screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

15.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 110 Security > Firewall > DoS

DoS Protection Blocking : Enable Disable (settings are invalid when disabled)

Deny Ping Response : Enable Disable

Apply **Cancel**

The following table describes the labels in this screen.

Table 82 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select Enable to enable protection against DoS attacks.
Deny Ping Response	Select Enable to block ping request packets.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

MAC Filter

16.1 Overview

You can configure the Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

16.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the Device. Click **Security > MAC Filter**. The screen appears as shown.

Figure 111 Security > MAC Filter

MAC Address Filter: Enable Disable (settings are invalid when disabled)

Set	Allow	Host name	MAC Address
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
29	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
30	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
31	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
32	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Note:
Only devices listed here are granted access to the network.

The following table describes the labels in this screen.

Table 83 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
Set	This is the index number of the MAC address.
Allow	Select Allow to permit access to the Device. MAC addresses not listed will be denied access to the Device. If you clear this, the MAC Address field for this set clears.
Host name	Enter the host name of the wireless or LAN clients that are allowed access to the Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Table 83 Security > MAC Filter (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Parental Control

17.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs parental control on a specific user.

17.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security** > **Parental Control** to open the following screen.

Figure 112 Security > Parental Control

The screenshot shows the 'Parental Control' configuration screen. Under the 'General' section, 'User Access Control' is set to 'Disable (settings are invalid when disabled)'. Below this is the 'User Access Control Profile' section, which includes an 'Add new profile' button and a table of existing profiles.

#	Status	Name	Network...	Internet Access Schedule	Network Service	Website Blocked	Modify
1		Max-PC	unknown...	M T W T F S S	00:00-24:00	None	Configured

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the screen.

The following table describes the fields in this screen.

Table 84 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Select Enable to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.

Table 84 Security > Parental Control (continued)

LABEL	DESCRIPTION
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.
Website Block	This shows whether the website block is configured. If not, None will be shown.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

17.2.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 113 Parental Control Rule: Add/Edit

General

Active

User Access Control Profile Name :

Network User :

Internet Access Schedule

Day : Everyday Monday Tuesday Wednesday Thursday Friday
 Saturday Sunday

Time (Start - End) : **00:00-24:00**

No access Authorized access

Network Service

Network Service Setting : selected service(s)

Add new service

#	<input type="checkbox"/>	Service Name	Protocol:Port	Modify

Blocked Site/URL Keyword

The following table describes the fields in this screen.

Table 85 Parental Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select Block , the Device prohibits the users from viewing the Web sites with the URLs listed below. If you select Allow , the Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Name of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Blocked Site/ URL Keyword	Click Add to show a screen to enter the URL of web site or URL keyword to which the Device blocks access. Click Delete to remove it.
Apply	Click this button to save your settings back to the Device.
Cancel	Click Cancel to restore your previously saved settings.

Scheduler Rules

18.1 Overview

You can define time periods and days during which the Device performs scheduled rules of certain features (such as Firewall Access Control, Parental Control) on a specific user in the **Scheduler Rules** screen.

18.2 The Scheduler Rules Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rules** to open the following screen.

Figure 114 Security > Scheduler Rules

#	Rule Name	Day	Time	Description	Modify
1	Example1	S M T W T F	08:00 - 17:00	Business	

The following table describes the fields in this screen.

Table 86 Security > Scheduler Rules

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the Edit icon to edit the schedule. Click the Delete icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

18.2.1 Add/Edit a Schedule

Click the **Add** button in the **Scheduler Rules** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 115 Scheduler Rules: Add/Edit

Rule Name :	<input type="text"/>
Day :	<input type="checkbox"/> SUN <input type="checkbox"/> MON <input type="checkbox"/> TUE <input type="checkbox"/> WED <input type="checkbox"/> THU <input type="checkbox"/> FRI <input type="checkbox"/> SAT
Time of Day Range :	From: <input type="text"/> To: <input type="text"/> (hh:mm)
Description :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the fields in this screen.

Table 87 Scheduler Rules: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the Device to perform this scheduler rule.
Time if Day Range	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Description	Enter a description for this scheduler rule.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Certificates

19.1 Overview

The Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

19.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Device's CA-signed certificates ([Section 19.4 on page 237](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Device ([Section 19.4 on page 237](#)).

19.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

19.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the Device's summary list of certificates and certification requests.

Figure 116 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 88 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password??	Select the checkbox and enter the private key into the text box to store it on the Device. The private key should not exceed 63 ASCII characters (not including spaces).
Browse...	Click this to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Device.
Create Certificate Request	Click this button to go to the screen where you can have the Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click Load Signed to import the signed certificate. Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

19.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Device generate a certification request.

Figure 117 Create Certificate Request

The screenshot shows a dialog box titled 'Create Certificate Request'. It has the following fields and controls:

- Certificate Name:** A text input field.
- Common Name:** A text input field with two radio buttons: 'Auto' (selected) and 'Customize'.
- Organization Name:** A text input field.
- State/Province Name:** A text input field.
- Country/Region Name:** A dropdown menu with 'US (United States)' selected.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom right.

The following table describes the labels in this screen.

Table 89 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select Auto to have the Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the Device. Otherwise click **Back** to return to the **Local Certificates** screen.

Figure 118 Certificate Request Created

Certificate Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	test
Type	request
Subject	CN=cc5d4e-DSL-491HNU-B1Bv2-S090Y0000000/O=abc/ST=tw/C=US
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBDCCAQECAQAwWDEuMCwGA1UEAxMY2M1ZDRILURTTTC00OTFITUuQjFCdjt

Load_Signed Close

19.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** icon to import the signed certificate into the Device.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 119 Load Signed Certificate

Paste signed certificate.

Certificate Name: test

Certificate: -----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----

Apply Cancel

The following table describes the labels in this screen.

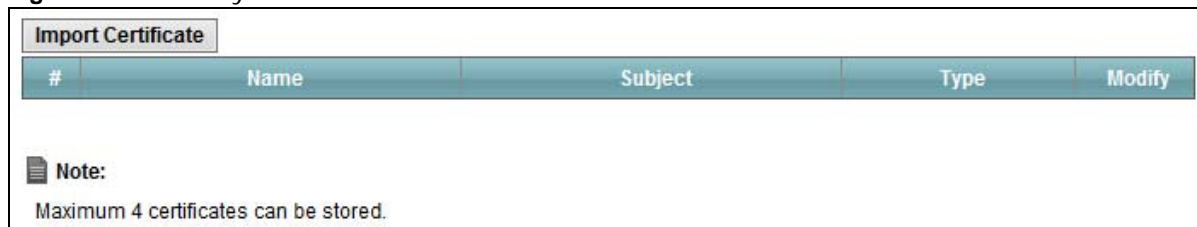
Table 90 Load Signed Certificate

LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the Device.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

19.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the Device to accept as trusted. The Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 120 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

Table 91 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

19.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 121 Trusted CA: View

Name	certnew.cer
Type	ca
Subject	DC=com/DC=ZyxEL/CN=ZyxELCA
Certificate	<pre>-----BEGIN CERTIFICATE----- MIIEaTCCA1GgAwIBAgIQGKaoaDflmLIDGHjntb31jANBgkqhkiG9w0BAQUFADA+ MRMwEQYKCZImiZPyLQGQGRYDY29tMRUwEwYKCZImiZPyLQGQGRYFWhiYRUwxED AO BgNVBAMTB1p5WEVVMQ0EwHhcNMDcwMjA1MDMwMTI0WhcNMTcwMjA1MDMwOTQ5 WjA+ MRMwEQYKCZImiZPyLQGQGRYDY29tMRUwEwYKCZImiZPyLQGQGRYFWhiYRUwxED AO BgNVBAMTB1p5WEVVMQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ DS</pre>
Back	

The following table describes the fields in this screen.

Table 92 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	<p>This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Back	Click Back to return to the previous screen.

19.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 122 Trusted CA: Import Certificate

The certificate is in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

Certificate File Path :

Enable Trusted CA for 802.1x Authentication

The following table describes the fields in this screen.

Table 93 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click Browse ... to find it.
Enable Trusted CA for 802.1x Authentication	If you select this checkbox, the trusted CA will be used for 802.1x authentication. The selected trusted CA will be displayed in the Network Setting > Broadband > 802.1x: Edit screen.
Certificate	Copy and paste the certificate into the text box to store it on the Device.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

20.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Device log and then display the logs or have the Device send them to an administrator (as e-mail) or to a syslog server.

20.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 20.2 on page 242](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 20.3 on page 243](#)).

20.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 94 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

Table 94 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

20.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 123 System Monitor > Log > System Log

The screenshot shows the System Log interface. At the top, there are two dropdown menus: one for 'Alert' (set to 'Alert') and one for 'All' (set to 'All'). Below these are three buttons: 'Clear Log', 'Refresh', and 'Export Log'. At the bottom, there is a table header with five columns: '#', 'Time', 'Facility', 'Level', and 'Messages'.

The following table describes the fields in this screen.

Table 95 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Logs Setting screen.
System Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

20.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 124 System Monitor > Log > Security Log

The screenshot shows the Security Log interface. At the top, there are two dropdown menus: the first is set to 'Emergency' and the second to 'All'. Below these are three buttons: 'Clear Log', 'Refresh', and 'Export Log'. At the bottom, there is a table header with five columns: '#', 'Time', 'Facility', 'Level', and 'Messages'.

The following table describes the fields in this screen.

Table 96 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Logs Setting screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

Traffic Status

21.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN and LAN interfaces.

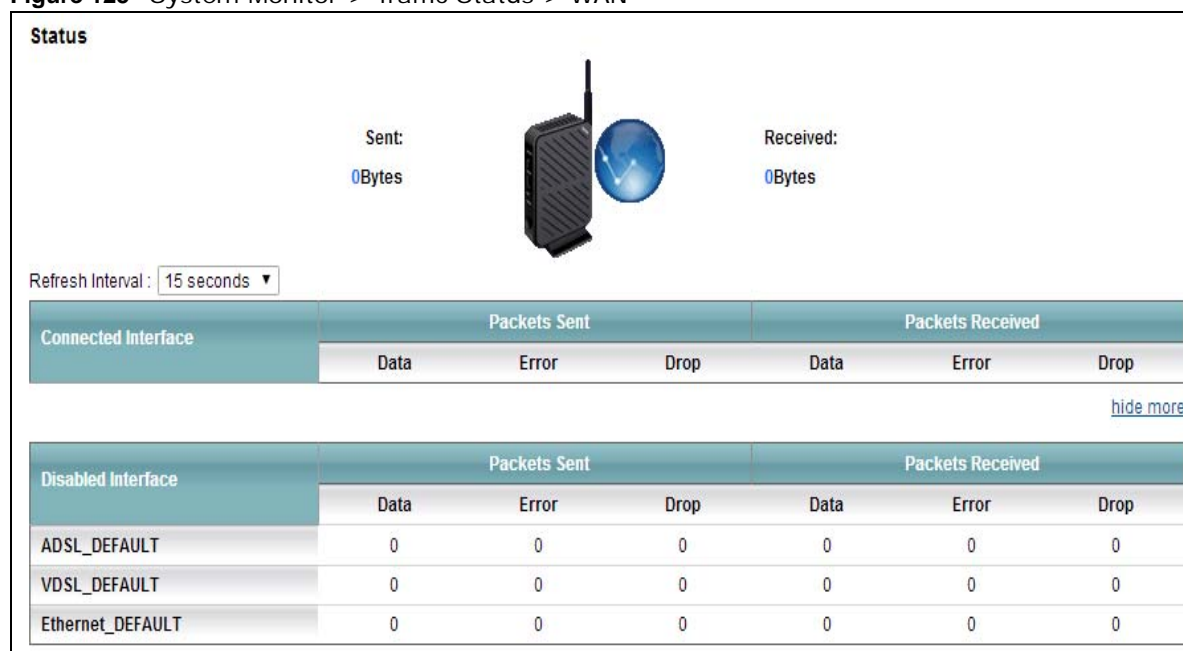
21.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 21.2 on page 245](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 21.3 on page 246](#)).

21.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the Device.

Figure 125 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 97 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
more...hide more	Click more... to show more information. Click hide more to hide them.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

21.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the Device.

Figure 126 System Monitor > Traffic Status > LAN

Refresh Interval :	15 seconds ▼				
Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Bytes Sent	0	0	0	1,027,178	0

The following table describes the fields in this screen.

Table 98 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.

Table 98 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
more...hide more	Click more... to show more information. Click hide more to hide them.
Interface	This shows the LAN or WLAN interface.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

ARP Table

22.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

22.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

22.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor > ARP Table**.

Figure 127 System Monitor > ARP Table

#	IP Address	MAC Address	Device
1	172.23.30.4	00:16:41:ee:e5:55	LAN
2	172.23.30.6	10:78:d2:c5:19:cd	LAN
3	172.23.30.8	00:1e:0b:24:f8:93	LAN

The following table describes the labels in this screen.

Table 99 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a port.

Table 99 System Monitor > ARP Table (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click on the device type to go to its configuration screen.

Routing Table

23.1 Overview

Routing is based on the destination address only and the Device takes the shortest path to forward a packet.

23.2 The Routing Table Screen

Click **System Monitor > Routing Table** to open the following screen.

Figure 128 System Monitor > Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.23.30.0	*	255.255.255.0	U	0	0	br0

The following table describes the labels in this screen.

Table 100 System Monitor > Routing Table

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of this route.
Flag	This indicates the route status. U-Up: The route is up. !-Reject: The route is blocked and will force a route lookup to fail. G-Gateway: The route uses a gateway to forward traffic. H-Host: The target of the route is a host. R-Reinstate: The route is reinstated for dynamic routing. D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect. M-Modified (redirect): The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".

Table 100 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Service	This indicates the name of the service used to forward the route.
Interface	This indicates the name of the interface through which the route is forwarded. br0 indicates the LAN interface. ptm0 indicates the WAN interface using IPoE or in bridge mode. ppp0 indicates the WAN interface using PPPoE.

IGMP Status

24.1 Overview

Use the **IGMP Status** screens to look at IGMP group status and traffic statistics.

24.2 The IGMP Group Status Screen

Use this screen to look at the current list of multicast groups the Device has joined and which ports have joined it. To open this screen, click **System Monitor > IGMP Group Status**.

Figure 129 System Monitor > IGMP Group Status

Interface	Multicast Group	Filter Mode	Source List
-----------	-----------------	-------------	-------------

The following table describes the labels in this screen.

Table 101 System Monitor > IGMP Group Status

LABEL	DESCRIPTION
Interface	This field displays the name of an interface on the Device that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	INCLUDE means that only the IP addresses in the Source List get to receive the multicast group's traffic. EXCLUDE means that the IP addresses in the Source List are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.

xDSL Statistics

25.1 The xDSL Statistics Screen

Use this screen to view detailed DSL statistics. Click **System Monitor > xDSL Statistics** to open the following screen.

Figure 130 System Monitor > xDSL Statistics

```

Monitor
Refresh Interval : 
Line : 

Status :
=====
xDSL Training Status: Idle
                    Mode: G.DMT
                    Traffic Type: Inactive
                    Link Uptime: N/A
=====

xDSL Port Details      Upstream      Downstream
Line Rate:            0.000 Mbps      0.000 Mbps
Actual Net Data Rate: 0.000 Mbps      0.000 Mbps
Trellis Coding:       N/A              N/A
SNR Margin:           0.0 dB          0.0 dB
Actual Delay:         0 ms            0 ms
Transmit Power:       0.0 dBm         0.0 dBm
Receive Power:       0.0 dBm         0.0 dBm
Actual INP:           0.0 symbols     0.0 symbols
Total Attenuation:   0.0 dB          0.0 dB
Attainable Net Data Rate: 0.000 Mbps      0.000 Mbps
=====

xDSL Counters

                Downstream      Upstream
Since Link time = 0 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             26507            0
LOS:             0                0
LOF:             0                0
LOM:             0                0
Latest 1 day time = 8 hours 14 min 13 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             26507            26507
LOS:             0                0
LOF:             0                0
LOM:             0                0
Latest 15 minutes time = 14 min 13 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             760              760
LOS:             0                0
LOF:             0                0
LOM:             0                0
Previous 1 day time = 0 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             0                0
LOS:             0                0
LOF:             0                0
LOM:             0                0
Previous 15 minutes time = 15 min 0 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             813              813
LOS:             0                0
LOF:             0                0
LOM:             0                0
Total time = 8 hours 14 min 13 sec
FEC:             0                0
CRC:             0                0
ES:              0                0
SES:             0                0
UAS:             26507            26507
LOS:             0                0
LOF:             0                0
LOM:             0                0
=====

```

The following table describes the labels in this screen.

Table 102 Status > xDSL Statistics

LABEL	DESCRIPTION
Refresh Interval	Select the time interval for refreshing statistics.
Line	Select which DSL line's statistics you want to display.
xDSL Training Status	This displays the current state of setting up the DSL connection.
Mode	This displays the ITU standard used for this connection.
Traffic Type	This displays the type of traffic the DSL port is sending and receiving. Inactive displays if the DSL port is not currently sending or receiving traffic.
Link Uptime	This displays how long the port has been running (or connected) since the last time it was started.
xDSL Port Details	
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Line Rate	These are the data transfer rates at which the port is sending and receiving data.
Actual Net Data Rate	These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic.
Trellis Coding	This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.
Actual Delay	This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.
Transmit Power	This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much power the service provider is using to transmit to the port.
Receive Power	Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider.
Actual INP	Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.
Total Attenuation	This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line).
Attainable Net Data Rate	These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic.
xDSL Counters	

Table 102 Status > xDSL Statistics (continued)

LABEL	DESCRIPTION
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
FEC	This is the number of Far End Corrected blocks.
CRC	This is the number of Cyclic Redundancy Checks.
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.
UAS	This is the number of UnAvailable Seconds.
LOS	This is the number of Loss Of Signal seconds.
LOF	This is the number of Loss Of Frame seconds.
LOM	This is the number of Loss of Margin seconds.

User Account

26.1 Overview

In the **Users Account** screen, you can change the password of the user account that you used to log in the Device.

26.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 131 Maintenance > User Account

The screenshot shows a form with the following fields and buttons:

- User Name :** A text input field containing the text "admin".
- Old Password :** A password input field.
- New Password :** A password input field.
- Retype to confirm :** A password input field.
- Apply** and **Cancel** buttons are located at the bottom right of the form.

The following table describes the labels in this screen.

Table 103 Maintenance > User Account

LABEL	DESCRIPTION
User Name	This field displays the name of the account that you used to log in the system.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Device.
Retype to confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Remote Management

27.1 Overview

Remote Management allows you to manage your Device from a remote location through the following interfaces:

- LAN
- WAN
- Trust Domain

Note: The Device is managed using the Web Configurator.

27.2 The Remote MGMT Screen

Use this screen to configure through which interface(s) users can use which service(s) to manage the Device.

Click **Maintenance > Remote MGMT** to open the following screen.

Figure 132 Maintenance > Remote MGMT

Services	LAN/WLAN	WAN	Trust Domain	Port
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22

Trust Domain

Status : Disable

IP Address :

Add
Delete
Edit

Certificate

HTTPS Certificate:

The following table describes the fields in this screen.

Table 104 Maintenance > Remote MGMT

LABEL	DESCRIPTION
Trust Domain	
Status	This field displays whether the Trust Domain is active or not.
IP Address	Enter the Trust Domain IP address.
Services	This is the service you may use to access the Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the Device from the LAN/WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Device from the WAN.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Device from the Trust Domain.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Certificate	
HTTPS Certificate	Select a certificate the HTTPS server (the Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the Certificates screen.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to restore your previously saved settings.

TR-069 Client

28.1 Overview

This chapter explains how to configure the Device's TR-069 auto-configuration settings.

28.2 The TR-069 Client Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Device. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Maintenance > TR-069 Client** to open the following screen. Use this screen to configure your Device to be managed by an ACS.

Figure 133 Maintenance > TR-069 Client

The screenshot shows the TR-069 Client configuration screen with the following fields and options:

- Inform:** Radio buttons for Enable and Disable.
- Inform Interval:** Text input field containing the value 300.
- ACS URL:** Empty text input field.
- ACS User Name:** Text input field containing the value admin.
- ACS Password:** Password input field with masked characters (dots).
- WAN Interface used by TR-069 client:** Dropdown menu showing Any_WAN.
- Display SOAP messages on serial console:** Radio buttons for Enable and Disable.
- Connection Request Authentication:** Checked checkbox.
- Connection Request User Name:** Text input field containing the value admin.
- Connection Request Password:** Password input field with masked characters (dots).
- Connection Request URL:** Empty text input field.
- Local certificate used by TR-069 client:** Dropdown menu.

At the bottom right of the form are two buttons: **Apply** and **Cancel**.

The following table describes the fields in this screen.

Table 105 Maintenance > TR-069 Client

LABEL	DESCRIPTION
Inform	Select Enable for the Device to send periodic inform via TR-069 on the WAN. Otherwise, select Disable .
Inform Interval	Enter the time interval (in seconds) at which the Device sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select Any_WAN , you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select Enable to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Device, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the Device.
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the Security > Certificates > Local Certificates screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

29.1 Overview

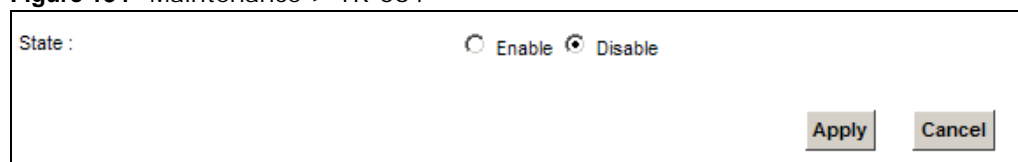
This chapter explains how to configure the Device's TR-064 auto-configuration settings.

29.2 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Maintenance > TR-064** to open the following screen.

Figure 134 Maintenance > TR-064



State : Enable Disable

Apply Cancel

The following table describes the fields in this screen.

Table 106 Maintenance > TR-064

LABEL	DESCRIPTION
State	Select Enable to activate management via TR-064 on the LAN.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Time Settings

30.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

30.2 The Time Screen

To change your Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Device's time based on your local time zone.

Figure 135 Maintenance > Time Setting

The screenshot shows the 'Maintenance > Time Setting' configuration screen. It is organized into several sections:

- Current Date/Time:** Shows 'Current Time : 06:12:22' and 'Current Date : 04 Jan 2011'.
- NTP Time Server:** Contains five rows for 'First NTP time server' through 'Fifth NTP time server'. Each row has a dropdown menu and a text input field. The values are: 'time.nist.gov', 'ntp1.tummy.com', 'None', 'None', and 'None'.
- Time Zone:** A dropdown menu showing '(GMT-05:00) Eastern Time'.
- Daylight Saving:**
 - State:** Radio buttons for 'Enable' (selected) and 'Disable'.
 - Start rule:**
 - Day:** Radio buttons for 'Day' and 'Second' (selected). 'Second' is followed by a dropdown menu showing 'Sunday'.
 - Month:** A dropdown menu showing 'March'.
 - Time:** Two dropdown menus showing '2' and '0'.
 - End rule:**
 - Day:** Radio buttons for 'Day' and 'First' (selected). 'First' is followed by a dropdown menu showing 'Sunday'.
 - Month:** A dropdown menu showing 'November'.
 - Time:** Two dropdown menus showing '2' and '0'.

At the bottom right of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the fields in this screen.

Table 107 Maintenance > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	<p>This field displays the time of your Device.</p> <p>Each time you reload this page, the Device synchronizes the time with the time server.</p>
Current Date	<p>This field displays the date of your Device.</p> <p>Each time you reload this page, the Device synchronizes the date with the time server.</p>
NTP Time Server	
First ~ Fifth NTP time server	<p>Select an NTP time server from the drop-down list box.</p> <p>Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.</p> <p>Select None if you don't want to configure the time server.</p> <p>Check with your ISP/network administrator if you are unsure of this information.</p>
Time Zone	
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
State	Select Enable if you use Daylight Saving Time.
Start rule:	<p>Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to Second, Sunday, the month to March and the time to 2 in the Hour field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday and the month to March. The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End rule	<p>Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to First, Sunday, the month to November and the time to 2 in the Hour field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday, and the month to October. The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

Table 107 Maintenance > Time Setting (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

E-mail Notification

31.1 Overview

A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

31.2 The Email Notification Screen

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add mail server information on the Device.

Figure 136 Maintenance > Email Notification

Mail Server Address	Username	Password	Email Address	Remove

The following table describes the labels in this screen.

Table 108 Maintenance > Email Notification

LABEL	DESCRIPTION
Add New Email	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.
Password	This field displays the password of the sender's mail account.
Email Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Device sends.
Remove	Click this button to delete the selected entry(ies).

31.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 137 Email Notification > Add

Email Notification Configuration

Mail Server Address: (SMTP Server NAME or IP)

Authentication Username:

Authentication Password:

Account Email Address:

Apply Cancel

The following table describes the labels in this screen.

Table 109 Email Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the Account Email Address field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the Account Email Address field.
Authentication Password	Enter the password associated with the user name above.
Account Email Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Device sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Apply	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to begin configuring this screen afresh.

Logs Setting

32.1 Overview

You can configure where the Device sends logs and which logs and/or immediate alerts the Device records in the **Logs Setting** screen.

32.2 The Log Settings Screen

To change your Device's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

Figure 138 Maintenance > Logs Setting

Syslog Setting

Syslog Logging : Enable Disable (settings are invalid when disabled)

Mode:

Syslog Server : (Server NAME or IP Address)

UDP Port : (Server Port)

E-mail Log Settings

Mail Server:

System Log Mail Subject:

Security Log Mail Subject:

Send Log to: (E-Mail Address)

Send Alarm to: (E-Mail Address)

Alarm Interval: second

Allowed Capacity Before Email Notification: %

Clear log after sending mail: Enable Disable (settings are invalid when disabled)

Active Log and Alert

System Log <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> DHCP Client <input checked="" type="checkbox"/> PPPoE <input type="checkbox"/> Wireless <input checked="" type="checkbox"/> DHCP Server <input type="checkbox"/> UPnP <input type="checkbox"/> NAT <input type="checkbox"/> Static Route <input type="checkbox"/> DDNS <input type="checkbox"/> IGMP <input type="checkbox"/> QoS <input type="checkbox"/> TR-069 <input type="checkbox"/> NTP	Security Log <input type="checkbox"/> Firewall <input type="checkbox"/> MAC Filter <input type="checkbox"/> Forward Web Sites <input type="checkbox"/> Blocked Web Sites <input type="checkbox"/> Attack <input type="checkbox"/> Certificate <input type="checkbox"/> IPSec <input checked="" type="checkbox"/> Account	Send immediate alert <input type="checkbox"/> Attacks <input type="checkbox"/> Blocked Web Sites
--	---	---

The following table describes the fields in this screen.

Table 110 Maintenance > Logs Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Device sends a log to an external syslog server. Select Enable to enable syslog logging.
Mode	Select the syslog destination from the drop-down list box. If you select Remote , the log(s) will be sent to a remote syslog server. If you select Local File , the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select Local File and Remote .
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the Device sends.
Send Log to	The Device sends logs to the e-mail address specified in this field. If this field is left blank, the Device does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
Allowed Capacity Before Email	Set what percent of the Device's log storage space can be filled before the Device sends a log e-mail.
Clear log after sending mail	Select this to delete all the logs after the Device sends an E-mail of the logs.
Active Log and Alert	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Send immediate alert	Select log categories for which you want the Device to send E-mail alerts immediately.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

32.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

- "End of Log" message shows that a complete log has been sent.

Figure 139 E-mail Log Example

```
Subject:
  Firewall Alert From
Date:
  Fri, 07 Apr 2000 10:05:42
From:
  user@zyxel.com
To:
  user@zyxel.com
1|Apr  7 00 |From:192.168.1.1      To:192.168.1.255  |default policy  |forward
  | 09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>         |
2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |default policy  |forward
  | 09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>         |
3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10    |match           |forward
  | 09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>         |
.....{snip}.....
.....{snip}.....
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255  |match           |forward
  | 10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>         |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255  |match           |forward
  | 10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>         |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255  |match           |forward
  | 10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>         |
End of Firewall Log
```


Firmware Upgrade

33.1 Overview

This chapter explains how to upload new firmware to your Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.

33.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the Device while firmware upload is in progress!

Figure 140 Maintenance > Firmware Upgrade

The following table describes the labels in this screen.

Table 111 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the firmware updating screen, wait two minutes before logging into the Device again.

Figure 141 Firmware Uploading



The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

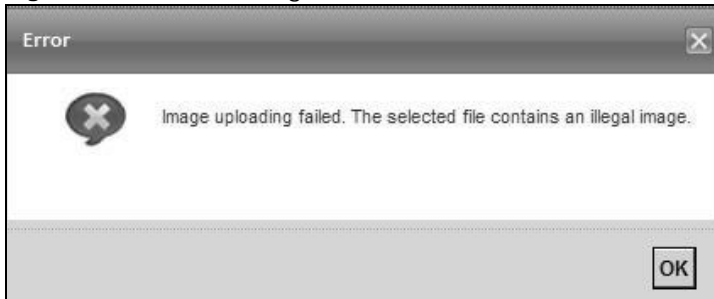
Figure 142 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 143 Error Message



Configuration


34.1 Overview

The **Configuration** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

34.2 The Configuration Screen

Click **Maintenance > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 144 Maintenance > Configuration



The screenshot displays the Configuration screen with three main sections:

- Backup Configuration:** Includes the instruction "Click Backup to save the current configuration of your system to your computer." and a **Backup** button.
- Restore Configuration:** Features a "File Path" input field, a **Browse...** button, and an **Upload** button.
- Back to Factory Defaults:** Contains the instruction "Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the" followed by two bullet points: "- LAN IP address will be 192.168.1.1" and "- DHCP will be reset to server". A **Reset** button is located at the bottom right of this section.

Backup Configuration

Backup Configuration allows you to back up (save) the Device's current configuration to a file on your computer. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Device.

Table 112 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the Device while configuration file upload is in progress.

After the Device configuration has been restored successfully, the login screen appears. Login again to restart the Device.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

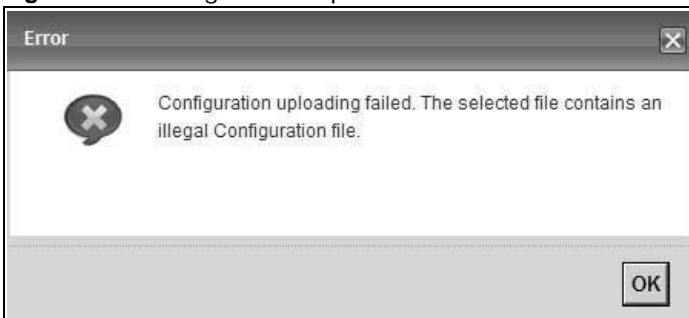
Figure 145 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix A on page 295](#) for details on how to set up your computer's IP address.

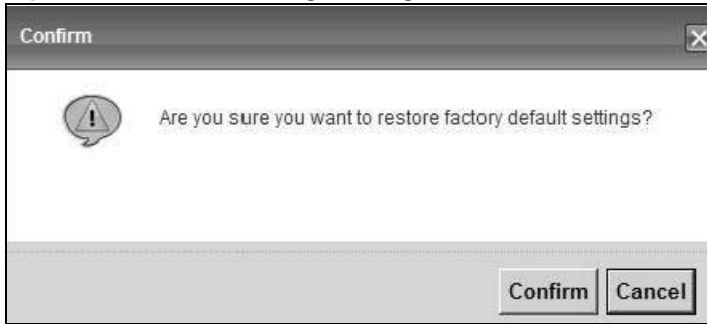
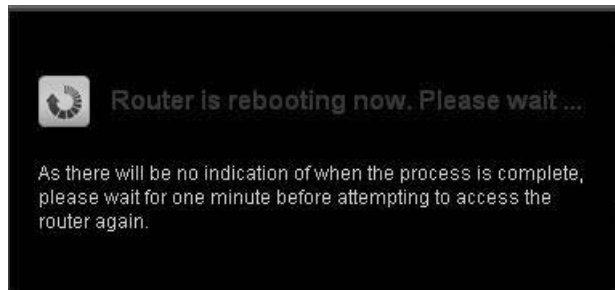
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 146 Configuration Upload Error



Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

Figure 147 Reset Warning Message**Figure 148** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Device. Refer to [Section 1.6 on page 22](#) for more information on the **RESET** button.

34.3 The Reboot Screen

System restart allows you to reboot the Device remotely without turning the power off. You may need to do this if the Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the Device reboot. This does not affect the Device's configuration.

Figure 149 Maintenance > Reboot

35.1 Overview

The **Diagnostic** screens display information to help you identify problems with the Device.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

35.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host ([Section 35.3 on page 283](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 35.5 on page 285](#)).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. ([Section 35.5 on page 285](#)).

35.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

35.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping & TraceRoute & NsLookup** to open the screen shown next.

Figure 150 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

The following table describes the fields in this screen.

Table 113 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IP address that you entered.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

35.4 802.1ag

Click **Maintenance > Diagnostic > 8.2.1ag** to open the following screen. Use this screen to perform CFM actions.

Figure 151 Maintenance > Diagnostic > 802.1ag

802.1ag Connectivity Fault Management

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Test the connection to another Maintenance End Point (MEP)

Linktrace Message (LTM):

The following table describes the fields in this screen.

Table 114 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Destination MAC Address	Enter the target device's MAC address to which the Device performs a CFM loopback test.
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
VDSL Traffic Type	This shows whether the VDSL traffic is activated.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any in-order or out-of-order Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Set MD Level	Click this button to configure the MD (Maintenance Domain) level.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

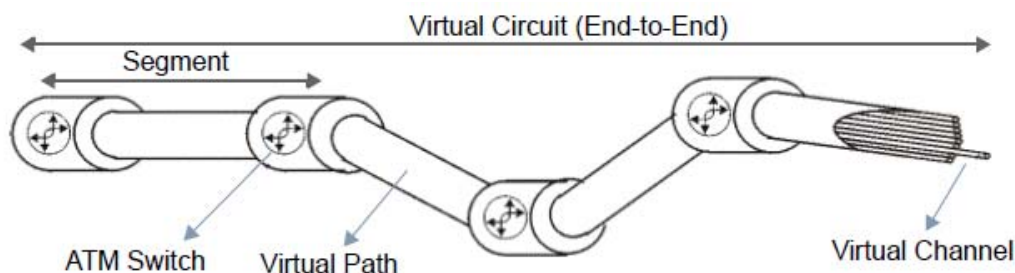
35.5 OAM Ping Test

Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Device. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 152 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefined Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

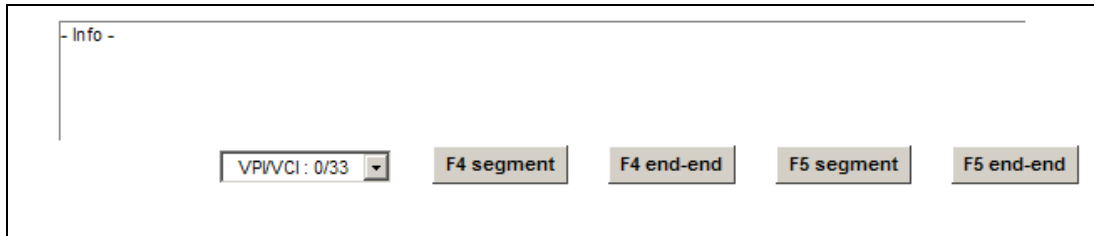
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 153 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 115 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [Device Access and Login](#)
- [Internet Access](#)
- [Wireless Internet Access](#)
- [USB Device Connection](#)
- [UPnP](#)

36.1 Power, Hardware Connections, and LEDs

The Device does not turn on. None of the LEDs turn on.

- 1 Make sure the Device is turned on.
- 2 Make sure you are using the power adaptor or cord included with the Device.
- 3 Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Device off and on.
- 5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 21](#).
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Device off and on.

- 5 If the problem continues, contact the vendor.

36.2 Device Access and Login

I forgot the IP address for the Device.

- 1 The default LAN IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 22](#).

I forgot the password.

- 1 The default admin password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 22](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.1.
 - If you changed the IP address ([Section 8.2 on page 135](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.5 on page 21](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix C on page 323](#).
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).

- 5 Reset the device to its factory defaults, and try to access the Device with the default IP address. See [Section 1.6 on page 22](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Device using another service, such as Telnet. If you can access the Device, check the remote management settings and firewall rules to find out why the Device does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Device.

- 1 Make sure you have entered the password correctly. The default admin password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the Device. Log out of the Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 36.1 on page 287](#).

I cannot Telnet to the Device.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

36.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 21](#).
 - 2 Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
 - 3 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Device.
 - 4 Disconnect all the cables from your device and reconnect them.
 - 5 If the problem continues, contact your ISP.
-

I cannot access the Internet through a DSL connection.

- 1 Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
 - 2 Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
 - 3 Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Group**).
 - 4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.
-

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

- 1 Your session with the Device may have expired. Try logging into the Device again.
-

- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 21](#).
- 3 Turn the Device off and on.
- 4 If the problem continues, contact your ISP.

36.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

What wireless security modes does my Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your Device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

36.5 USB Device Connection

The Device fails to detect my USB device.

- 1 Disconnect the USB device.
- 2 Reboot the Device.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the Device.

36.6 UPnP

When using UPnP and the Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

- 1 Disconnect the Ethernet cable from the Device's LAN port or from your computer.
- 2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

- 1 Wait more than three minutes.
- 2 Restart the applications.

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

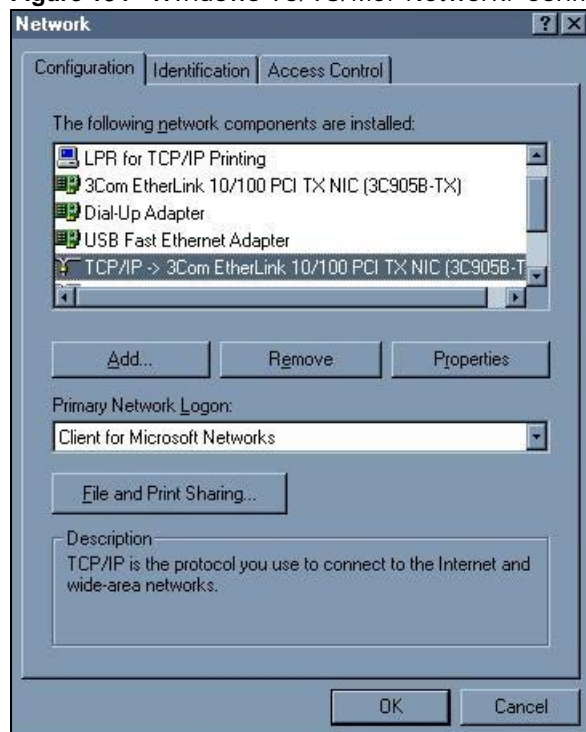
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 154 Windows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

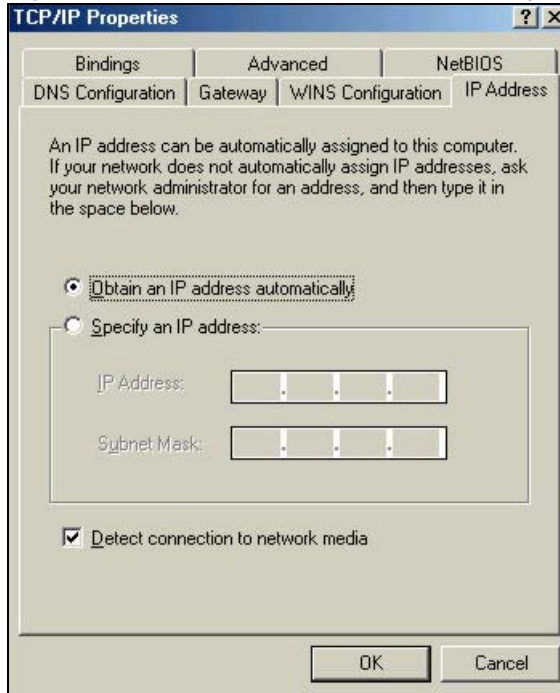
- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

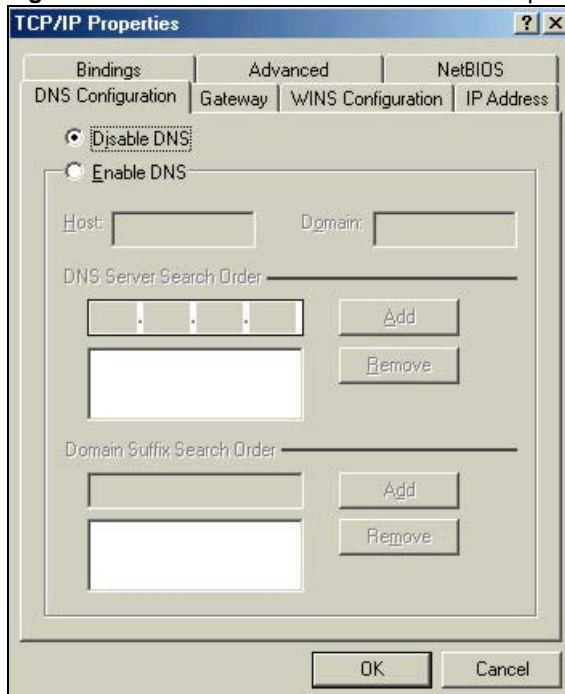
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 155 Windows 95/98/Me: TCP/IP Properties: IP Address**3** Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 156 Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
 - 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
 - 7 Turn on your Device and restart your computer when prompted.

Verifying Settings

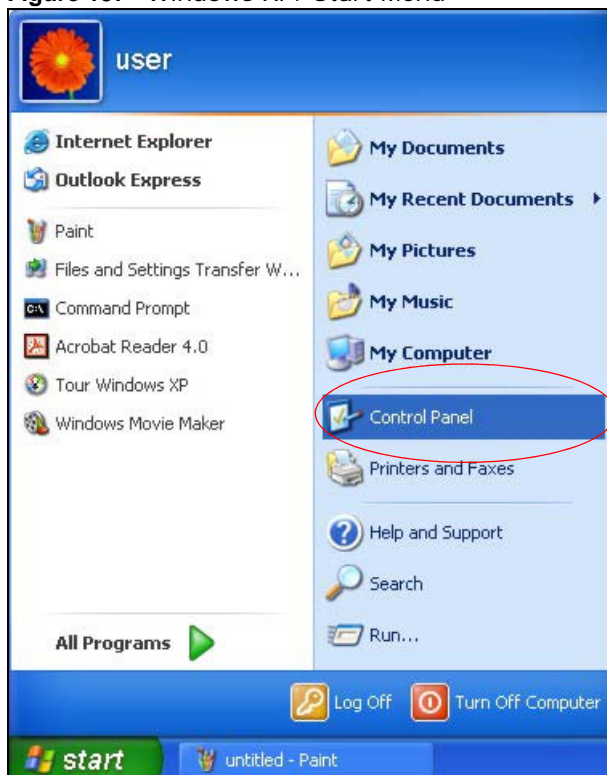
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 157 Windows XP: Start Menu



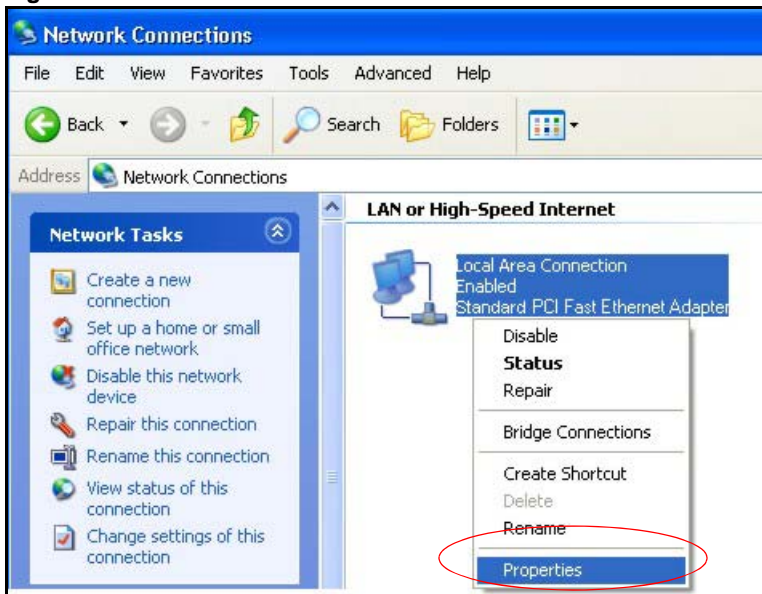
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 158 Windows XP: Control Panel

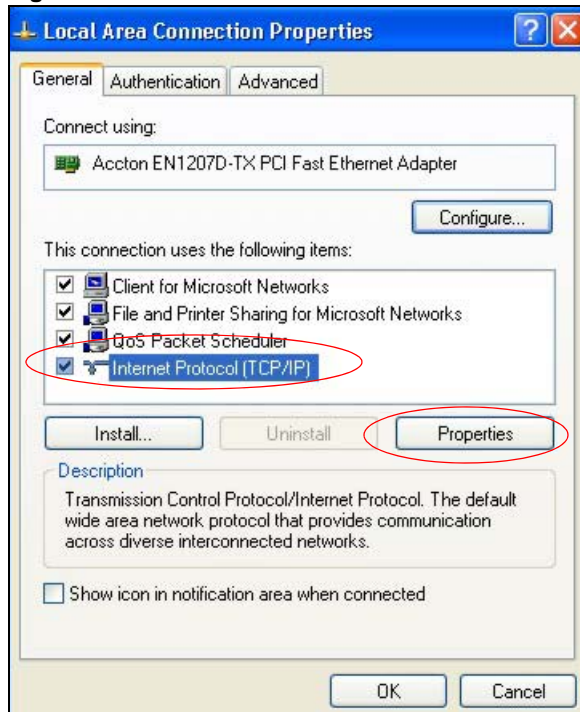


- 3 Right-click **Local Area Connection** and then click **Properties**.

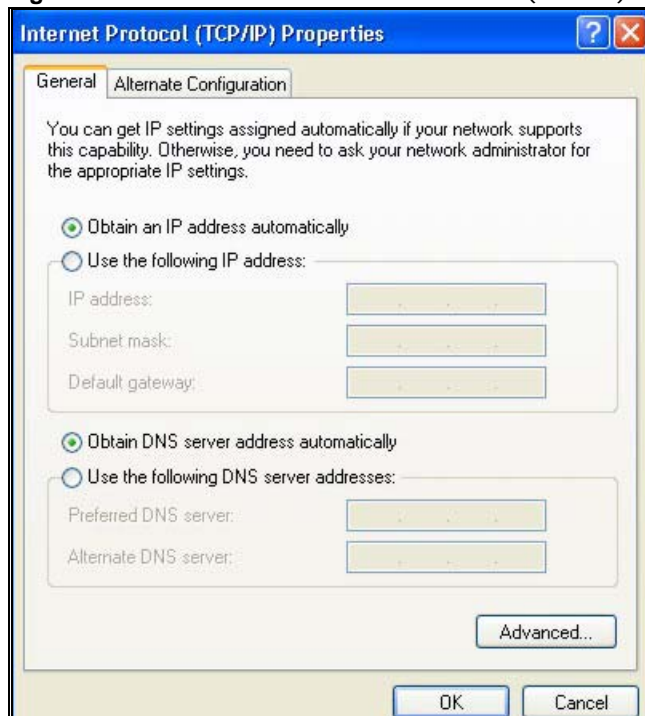
Figure 159 Windows XP: Control Panel: Network Connections: Properties



- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 160 Windows XP: Local Area Connection Properties

- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
- If you have a dynamic IP address click **Obtain an IP address automatically**.
 - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
 - Click **Advanced**.

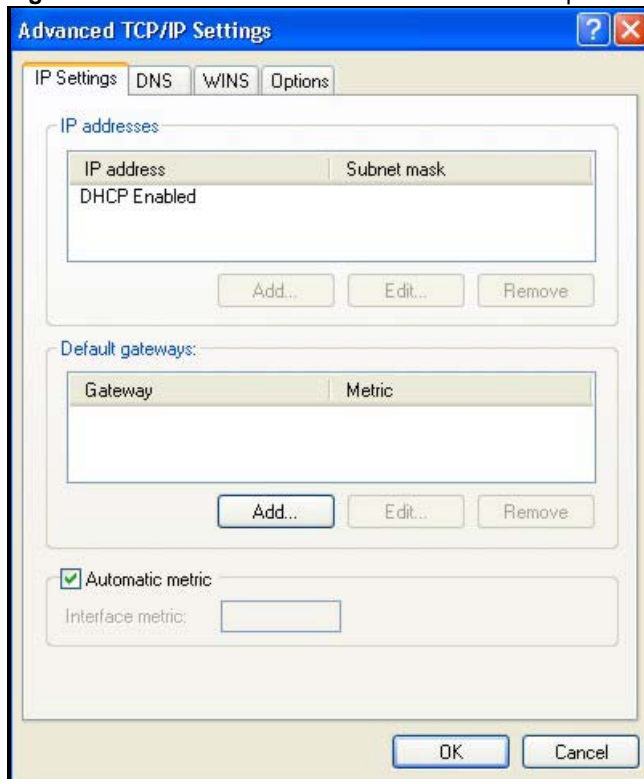
Figure 161 Windows XP: Internet Protocol (TCP/IP) Properties

- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

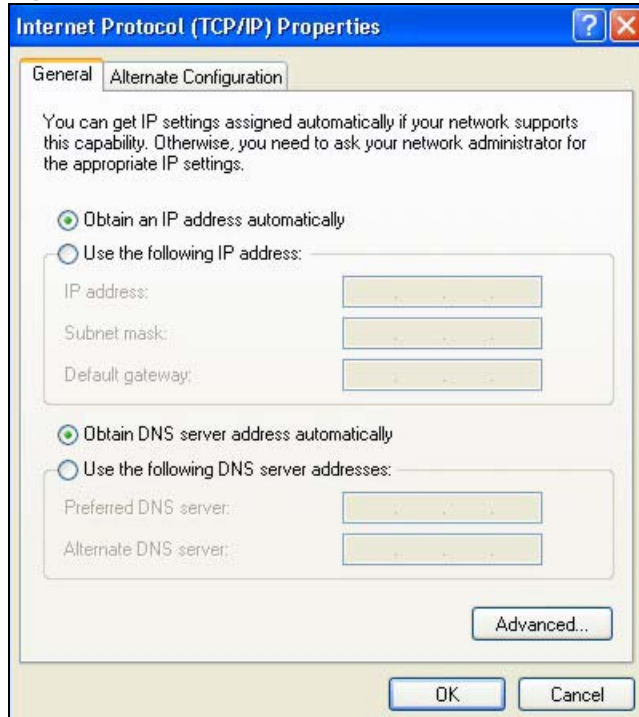
Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 162 Windows XP: Advanced TCP/IP Properties



- 7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 163 Windows XP: Internet Protocol (TCP/IP) Properties

- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Turn on your Device and restart your computer (if prompted).

Verifying Settings

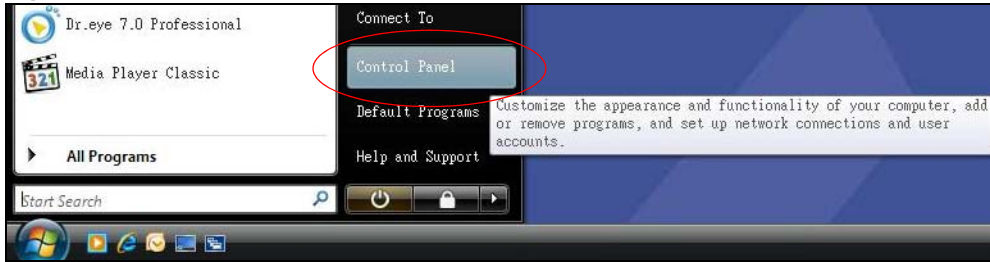
- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

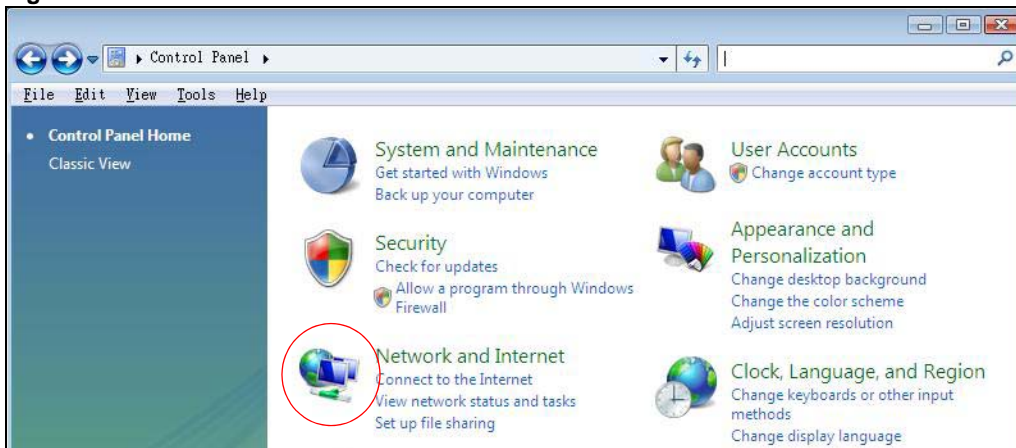
- 1 Click the **Start** icon, **Control Panel**.

Figure 164 Windows Vista: Start Menu



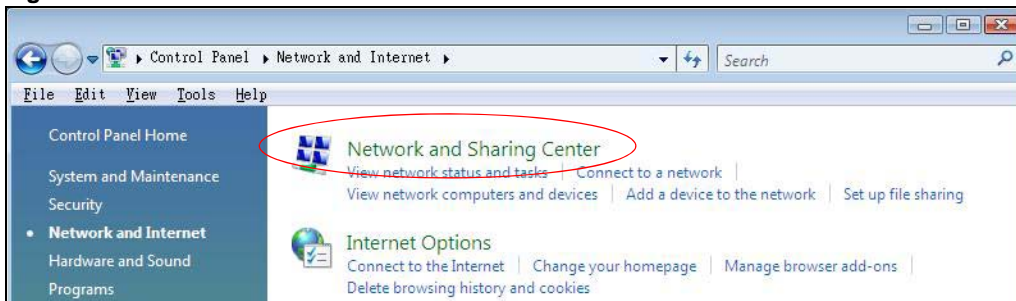
- 2 In the **Control Panel**, double-click **Network and Internet**.

Figure 165 Windows Vista: Control Panel



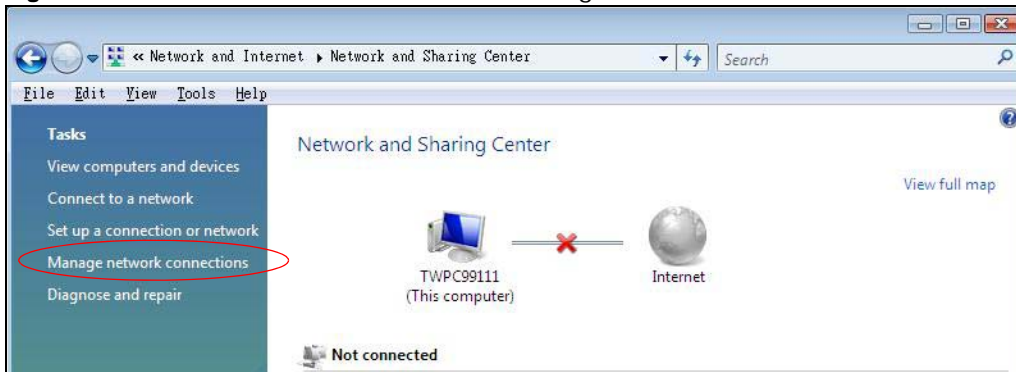
- 3 Click **Network and Sharing Center**.

Figure 166 Windows Vista: Network And Internet



- 4 Click **Manage network connections**.

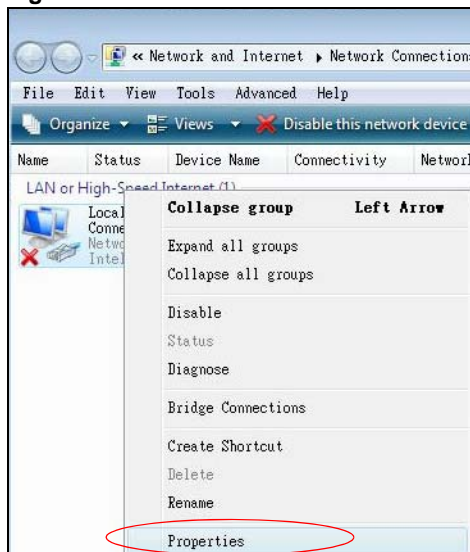
Figure 167 Windows Vista: Network and Sharing Center



- 5 Right-click **Local Area Connection** and then click **Properties**.

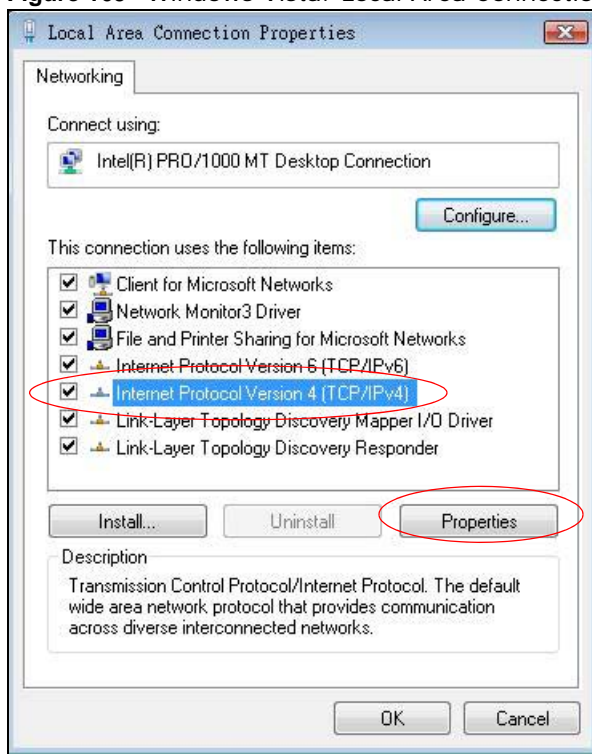
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 168 Windows Vista: Network and Sharing Center



- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

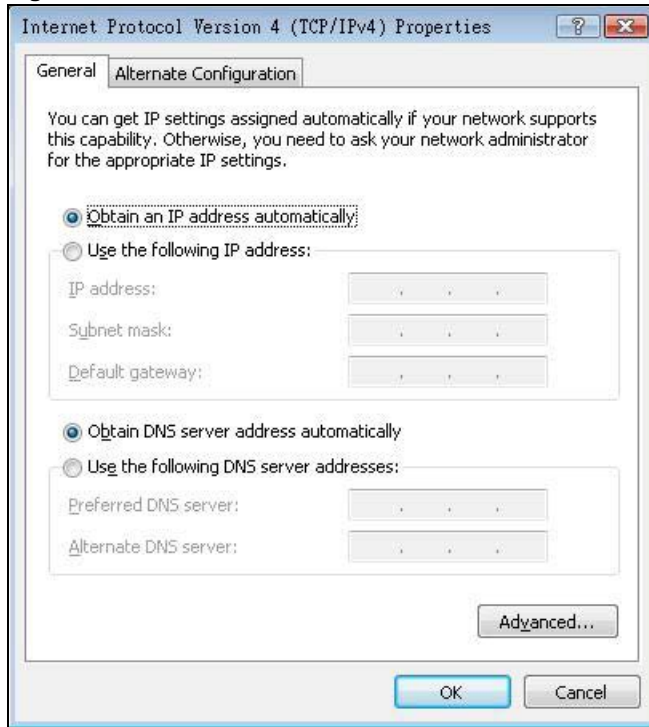
Figure 169 Windows Vista: Local Area Connection Properties



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General** tab).
 - If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

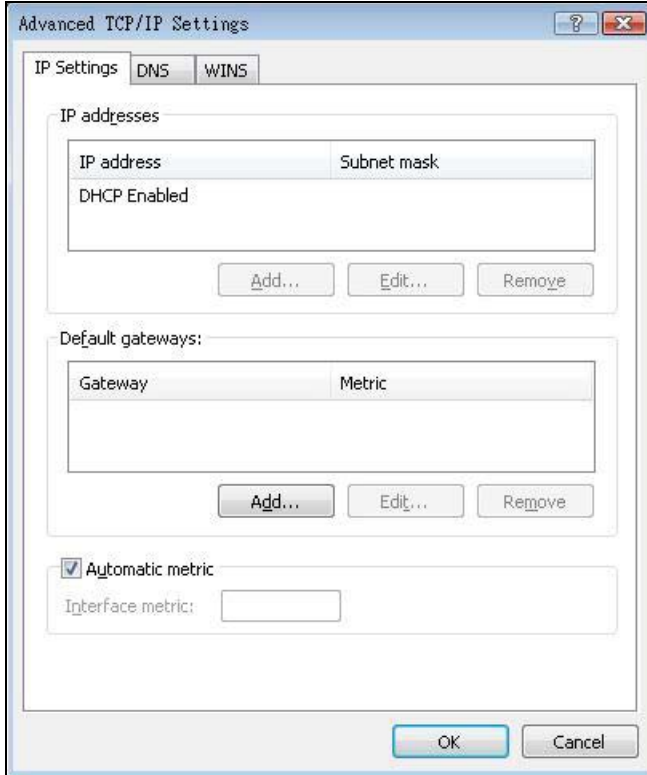
Figure 170 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



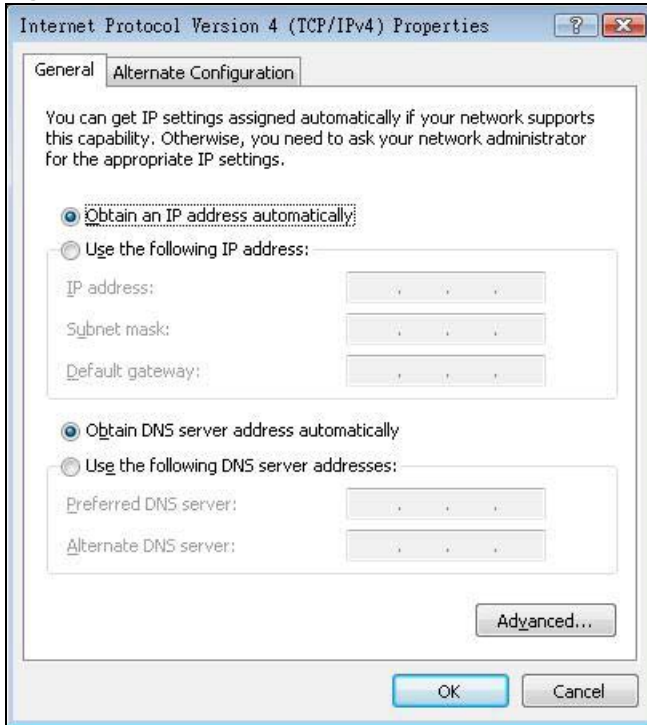
- 8** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 171 Windows Vista: Advanced TCP/IP Properties

- 9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General** tab):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 172 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

- 10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.
- 11 Click **Close** to close the **Local Area Connection Properties** window.
- 12 Close the **Network Connections** window.
- 13 Turn on your Device and restart your computer (if prompted).

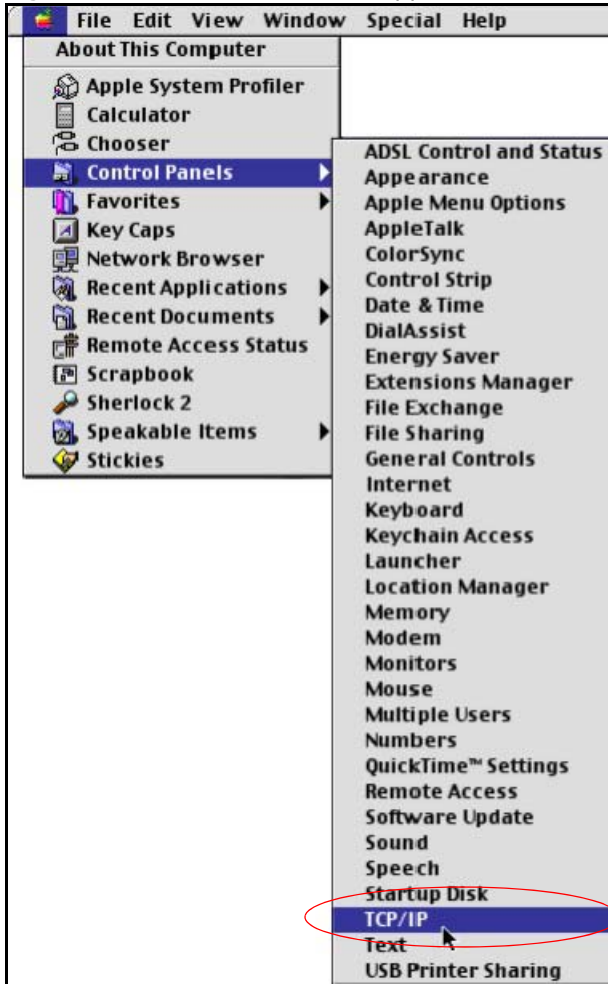
Verifying Settings

- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

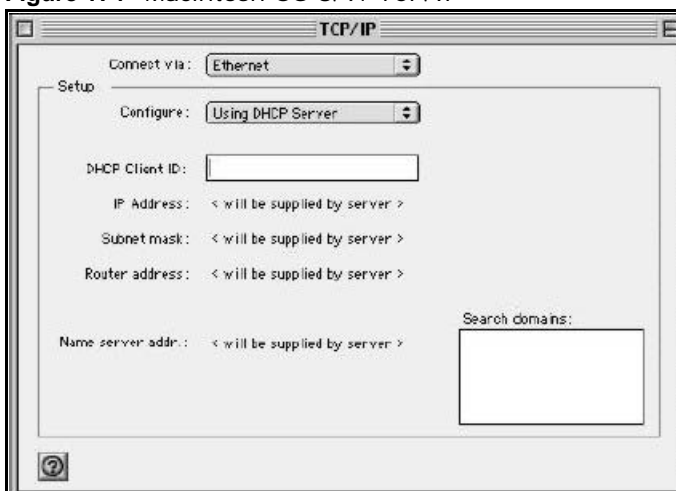
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 173 Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

Figure 174 Macintosh OS 8/9: TCP/IP



- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Device in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
 - 6 Click **Save** if prompted, to save changes to your configuration.
 - 7 Turn on your Device and restart your computer (if prompted).

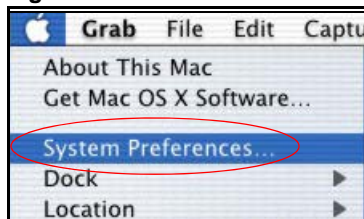
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

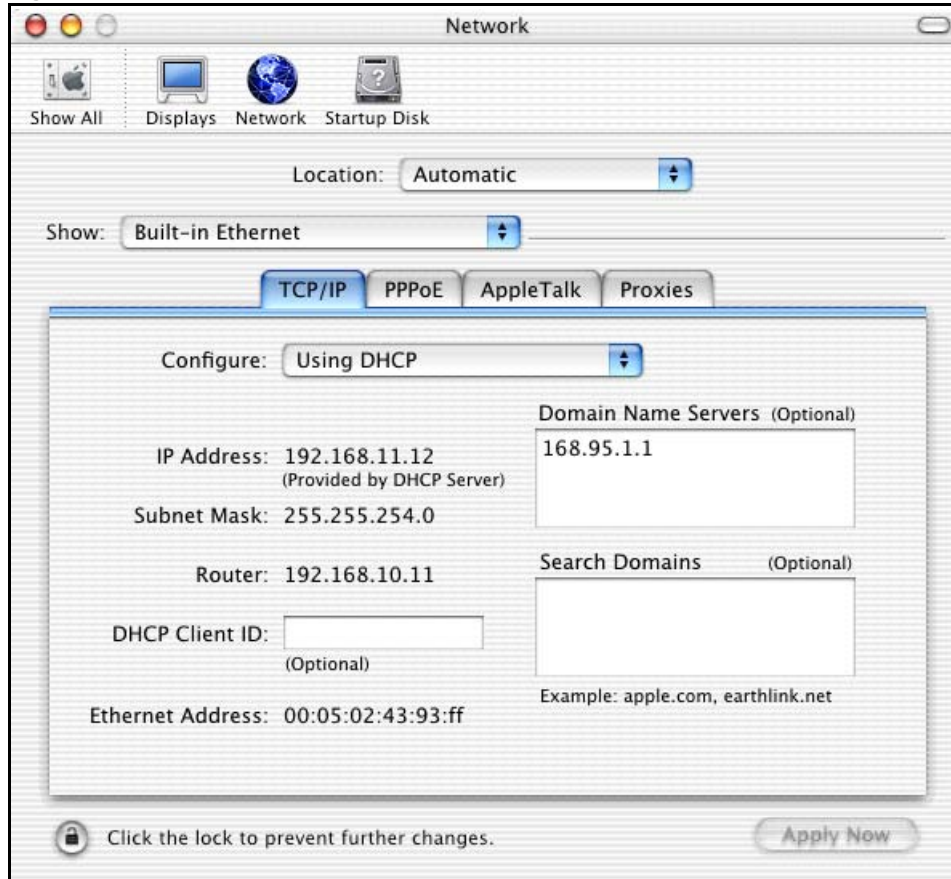
Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 175 Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 176 Macintosh OS X: Network

- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Device in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

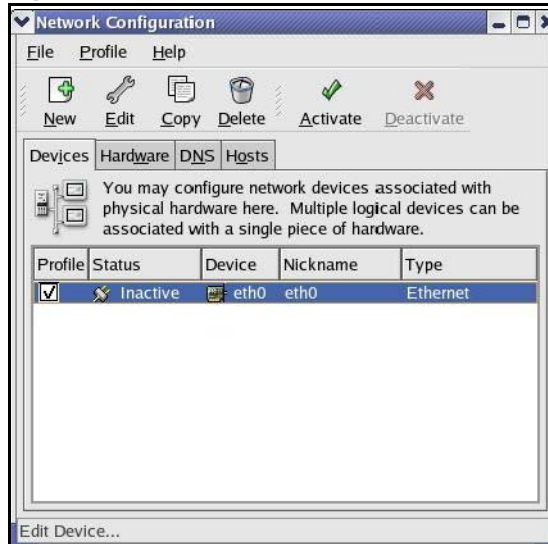
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 177 Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

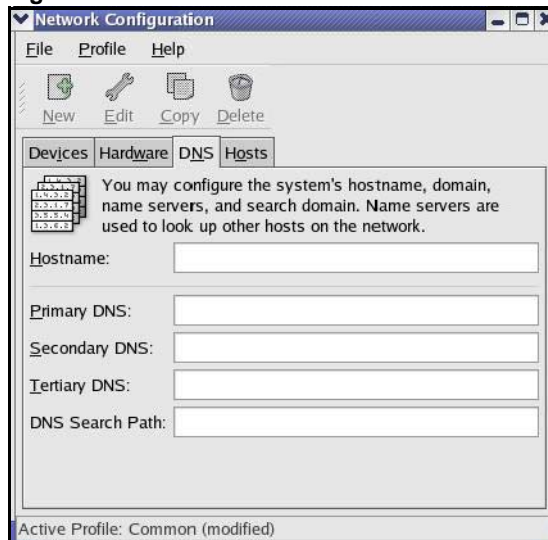
Figure 178 Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
 - If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

- 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 179 Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens**.

Figure 180 Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 181 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet

```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 182 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet

```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 183 Red Hat 9.0: DNS Settings in resolv.conf

```

nameserver 172.23.5.1
nameserver 172.23.5.2

```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 184 Red Hat 9.0: Restart Ethernet Card

```

[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:           [OK]
Setting network parameters:                 [OK]
Bringing up loopback interface:             [OK]
Bringing up interface eth0:                 [OK]

```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 185 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

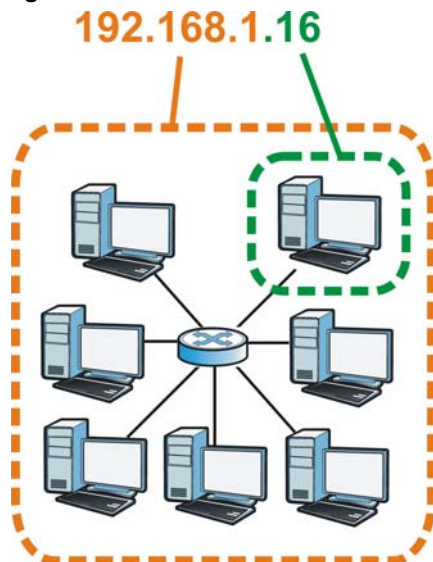
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 186 Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 116 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 117 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 118 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 119 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

Table 119 Alternative Subnet Mask Notation (continued)

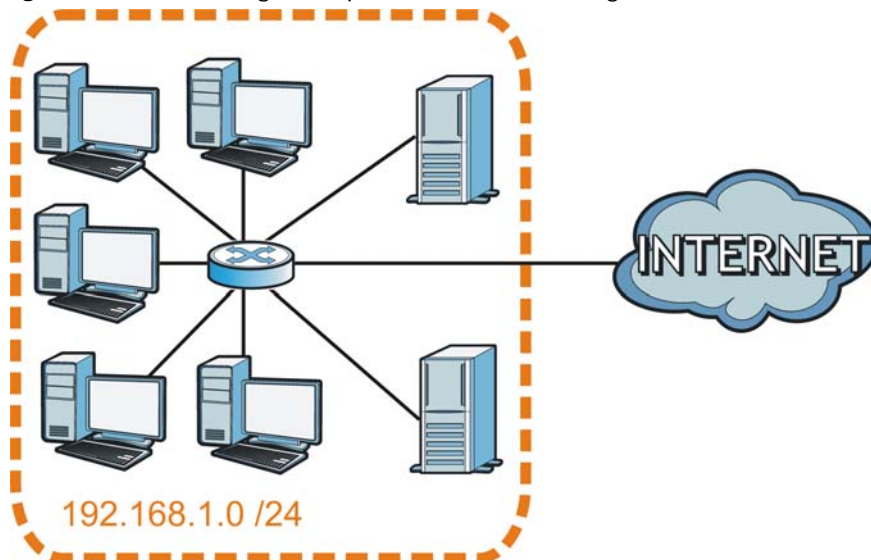
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

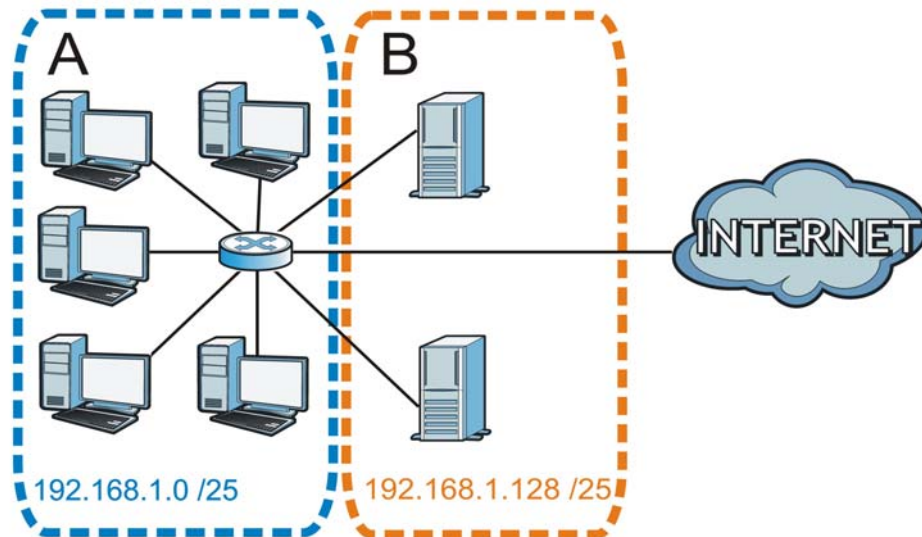
The following figure shows the company network before subnetting.

Figure 187 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 188 Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 120 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 121 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 122 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 123 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 124 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 125 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 126 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Device.

Once you have decided on the network number, pick an IP address for your Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

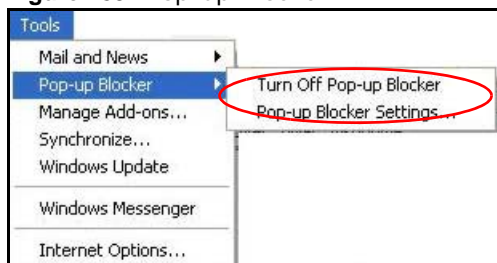
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

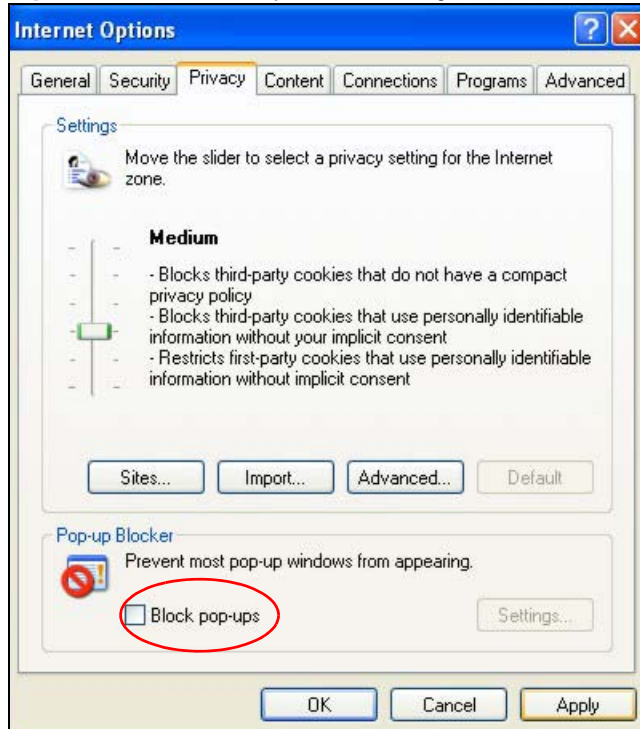
- 1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 189 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 190 Internet Options: Privacy

- 3 Click **Apply** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 191 Internet Options: Privacy

- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 192 Pop-up Blocker Settings

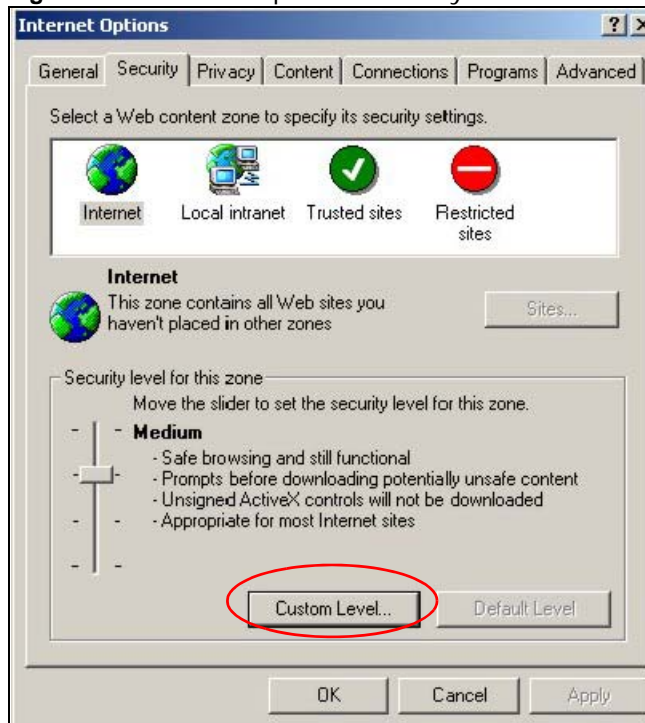
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

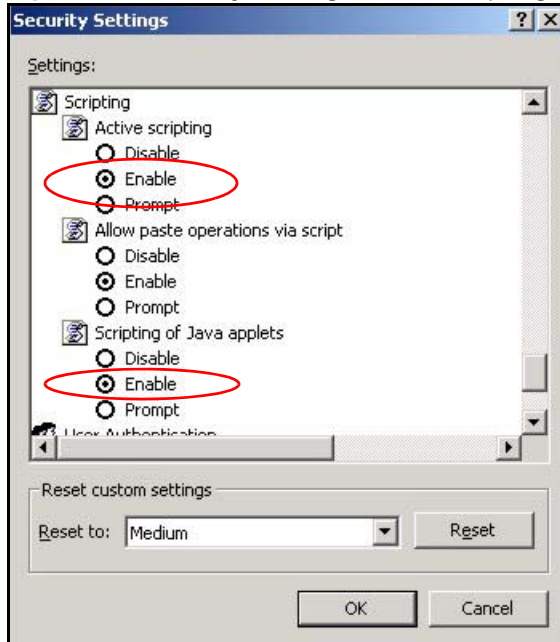
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 193 Internet Options: Security



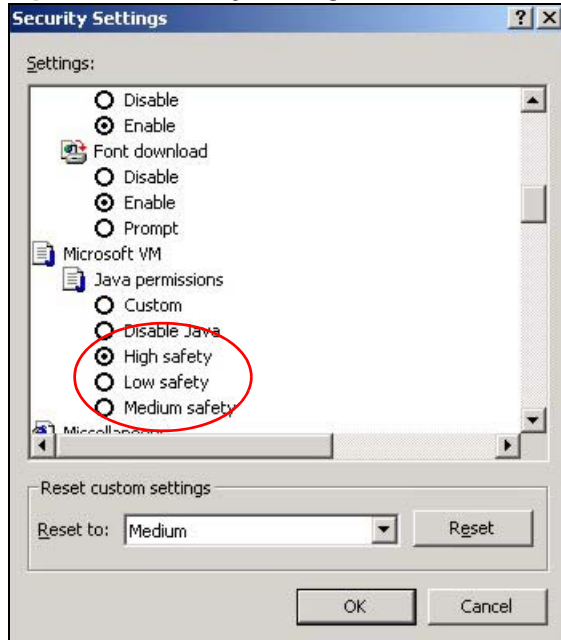
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 194 Security Settings - Java Scripting

Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

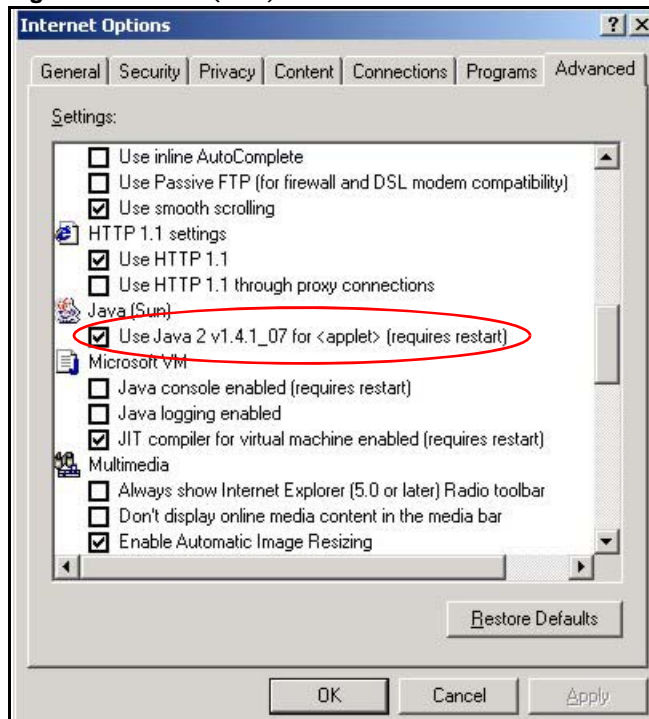
Figure 195 Security Settings - Java



JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 196 Java (Sun)

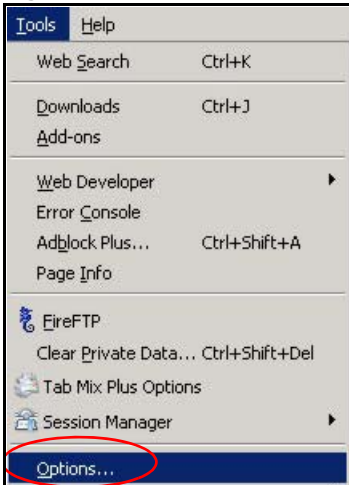


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

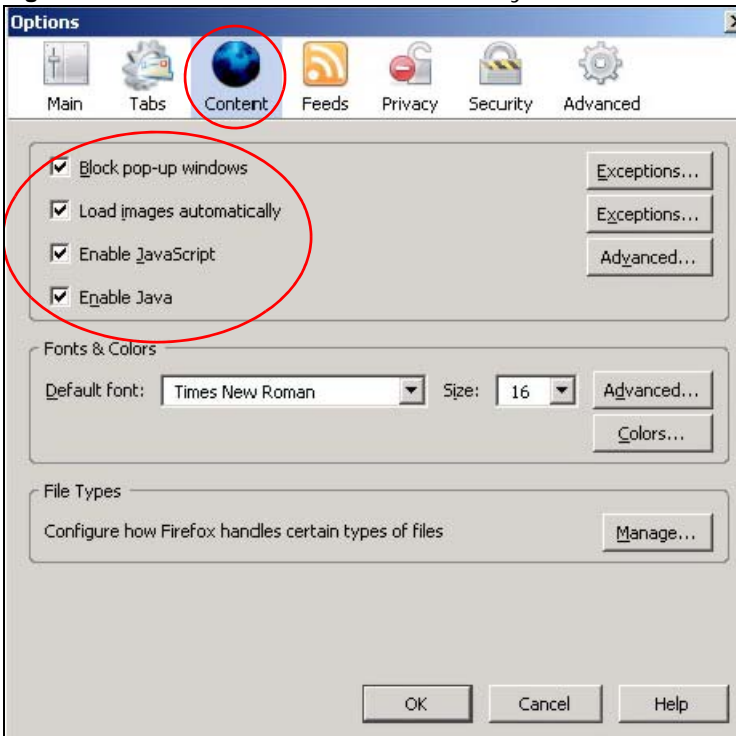
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 197 Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 198 Mozilla Firefox Content Security



Wireless LANs

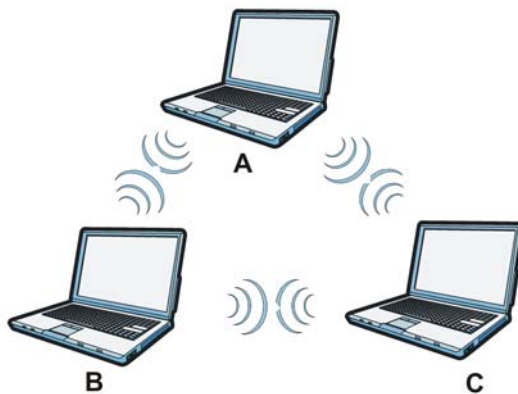
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

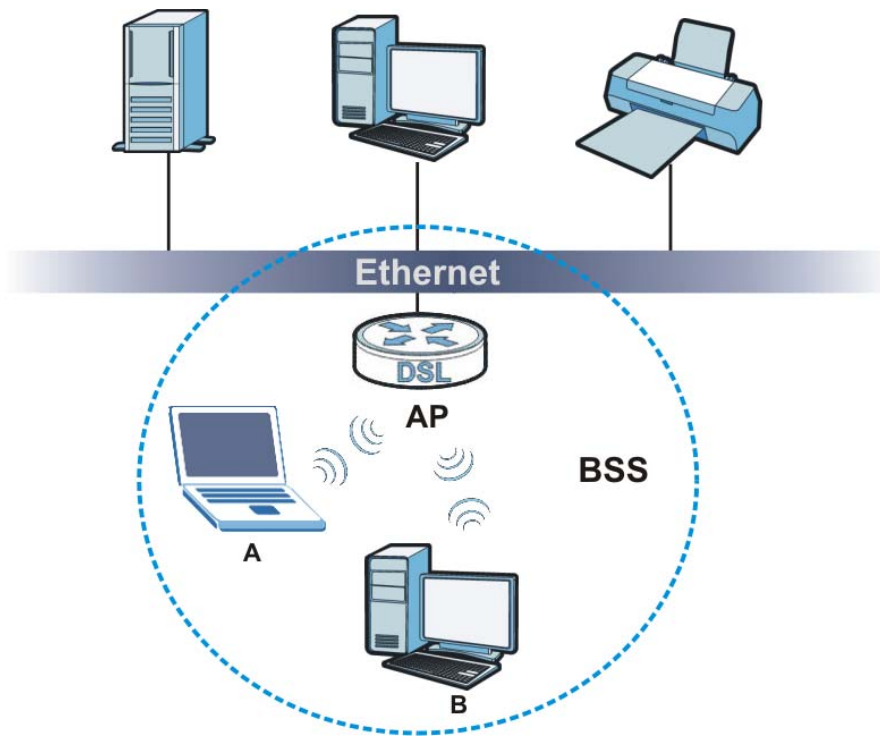
Figure 199 Peer-to-Peer Communication in an Ad-hoc Network



BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

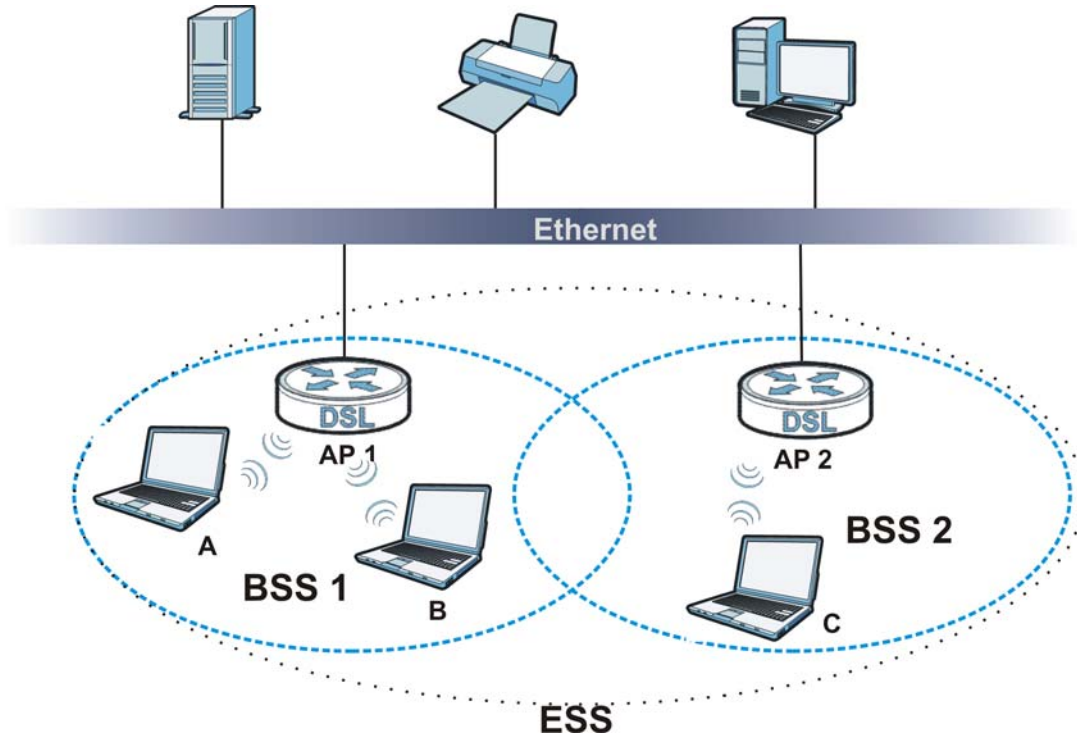
Figure 200 Basic Service Set

ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 201 Infrastructure WLAN

Channel

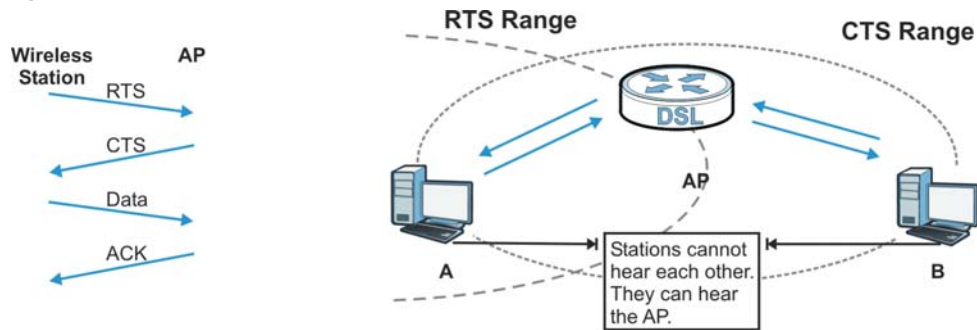
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 202 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 127 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/ 54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Device.

Table 128 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client

authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 129 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange

messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

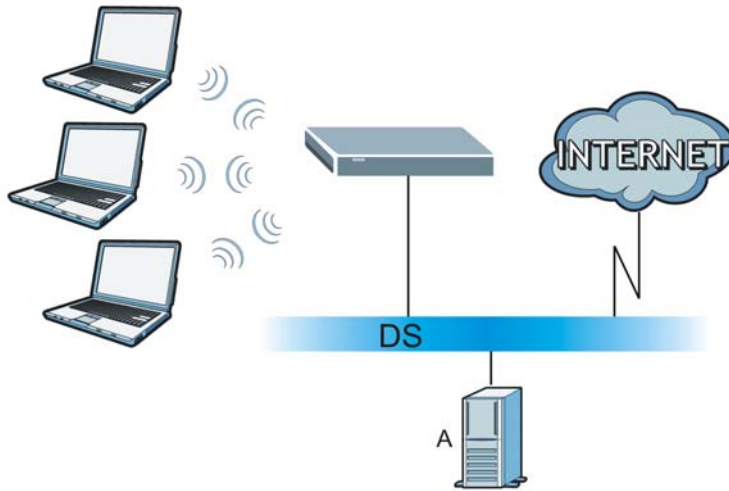
A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 203 WPA(2) with RADIUS Application Example

WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 204 WPA(2)-PSK Authentication

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 130 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately

2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of `fe80::/10`. The link-local unicast address format is as follows.

Table 131 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 132 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 133 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0

Table 133 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits ffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

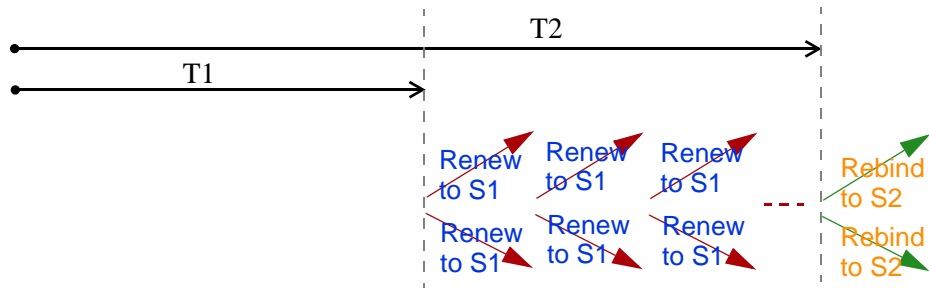
MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If

the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.

- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Device also sends out a neighbor solicitation message. When the Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Device creates an entry in the default router list cache if the router can be used as a default router.

When the Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is un-link, the address is considered as the next hop. Otherwise, the Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

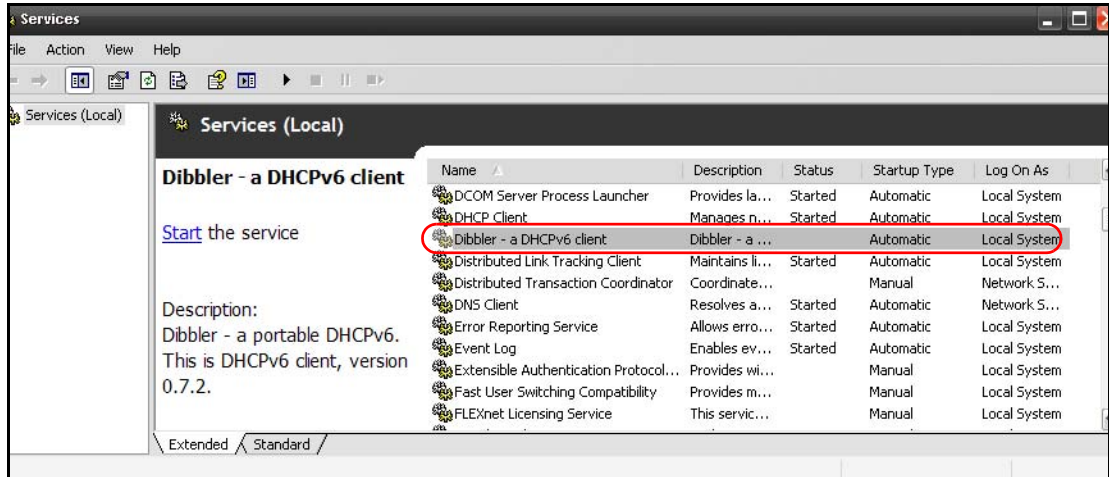
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

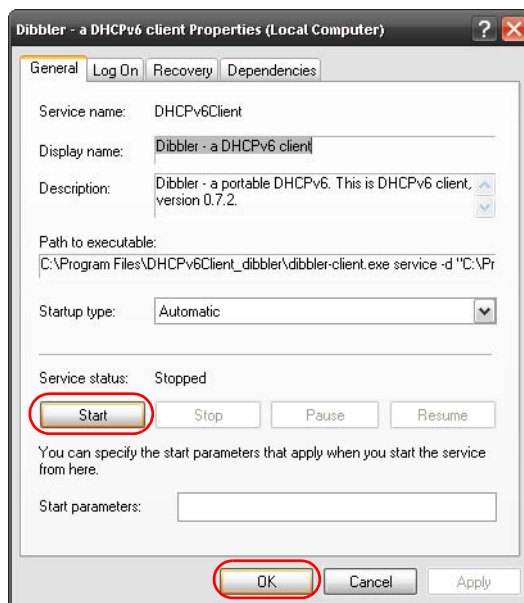
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click **Dibbler - a DHCPv6 client**.



- 5 Click **Start** and then **OK**.



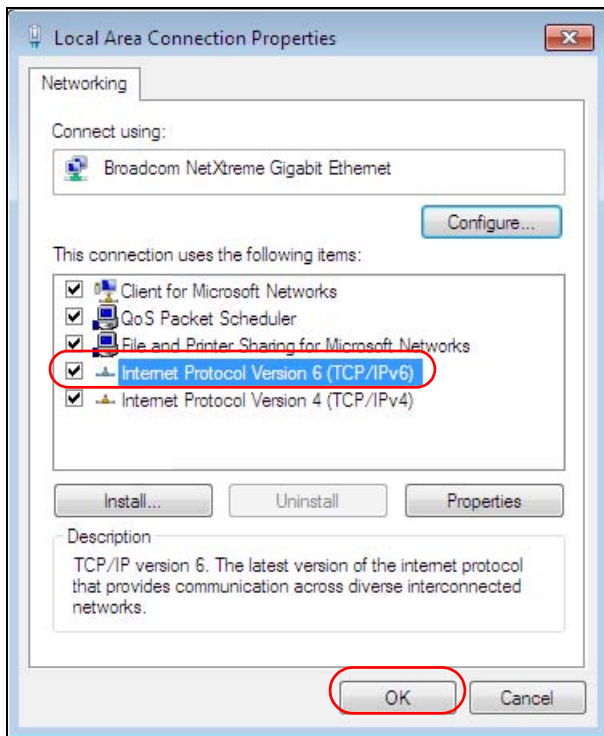
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
  
```

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 134 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.

Table 134 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).

Table 134 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

Legal Information

Copyright

Copyright © 2014 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.

- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

This Class [*] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [*] est conforme à la norme NMB-003 du Canada.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the

warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- This product is for indoor use only (utilisation intérieure exclusivement).
- The screen of the coaxial cable is intended to be connected to earth in the building installation.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



A

ACL rule [218](#)
 ACS [263](#)
 activation
 firewalls [215](#)
 media server [211](#)
 SIP ALG [190](#)
 SSID [110](#)
 adding a printer example [62](#)
 Address Resolution Protocol [249](#)
 administrator password [26](#)
 alternative subnet mask notation [317](#)
 antenna
 directional [343](#)
 gain [342](#)
 omni-directional [343](#)
 AP (access point) [333](#)
 applications
 Internet access [18](#)
 media server [210](#)
 activation [211](#)
 iTunes server [210](#)
 applications, NAT [194](#)
 ARP Table [249, 251](#)
 authentication [120, 121](#)
 RADIUS server [121](#)
 Auto Configuration Server, see ACS [263](#)

B

backup
 configuration [279](#)
 Basic Service Set, See BSS [331](#)
 Basic Service Set, see BSS
 blinking LEDs [21](#)
 Broadband [75](#)
 broadcast [99](#)
 BSS [123, 331](#)

example [123](#)

C

CA [233, 337](#)
 Canonical Format Indicator See CFI
 CCMs [282](#)
 certificate
 factory default [234](#)
 Certificate Authority
 See CA.
 certificates [233](#)
 authentication [233](#)
 CA
 creating [234](#)
 public key [233](#)
 replacing [234](#)
 storage space [234](#)
 Certification Authority [233](#)
 Certification Authority. see CA
 certifications [357](#)
 notices [358](#)
 CFI [99](#)
 CFM [282](#)
 CCMs [282](#)
 link trace test [282](#)
 loopback test [282](#)
 MA [282](#)
 MD [282](#)
 MEP [282](#)
 MIP [282](#)
 channel [333](#)
 interference [333](#)
 channel, wireless LAN [119](#)
 client list [138](#)
 compatibility, WDS [114](#)
 configuration
 backup [279](#)
 firewalls [215](#)
 reset [280](#)

restoring [280](#)
static route [96, 158, 198](#)

Connectivity Check Messages, see CCMs

copyright [357](#)

CoS [176](#)

CoS technologies [164](#)

creating certificates [234](#)

CTS (Clear to Send) [334](#)

CTS threshold [117, 120](#)

D

data fragment threshold [117, 120](#)

DDoS [214](#)

default server address [189](#)

Denials of Service, see DoS

DHCP [134, 153](#)

Differentiated Services, see DiffServ [176](#)

DiffServ [176](#)
marking rule [177](#)

digital IDs [233](#)

disclaimer [357](#)

DLNA [210](#)

DMZ [189](#)

DNS [134, 154](#)

DNS server address assignment [99](#)

Domain Name [195](#)

Domain Name System, see DNS

Domain Name System. See DNS.

DoS [214](#)

DS field [176](#)

DS, dee differentiated services

DSCP [176](#)

dynamic DNS [197](#)
wildcard [198](#)

Dynamic Host Configuration Protocol, see DHCP

dynamic WEP key exchange [338](#)

DYNDNS wildcard [198](#)

E

EAP Authentication [337](#)

ECHO [195](#)

e-mail
log example [274](#)

Encapsulation [96](#)
MER [97](#)
PPP over Ethernet [97](#)

encapsulation [76](#)

encryption [122, 339](#)

ESS [332](#)

Extended Service Set IDentification [104, 111](#)

Extended Service Set, See ESS [332](#)

F

FCC interference statement [357](#)

File Sharing [208](#)

file sharing [20](#)

filters
MAC address [111, 121](#)

Finger [195](#)

firewalls [213](#)
add protocols [215](#)
configuration [215](#)
DDoS [214](#)
DoS [214](#)
LAND attack [214](#)
Ping of Death [214](#)
SYN attack [214](#)

firmware [277](#)
version [73](#)

forwarding ports [182](#)

fragmentation threshold [117, 120, 334](#)

FTP [182, 195](#)

G

General wireless LAN screen [102](#)

Hhidden node [333](#)HTTP [195](#)**I**IANA [322](#)Internet Assigned Numbers Authority
see IANAIBSS [331](#)IEEE 802.11g [335](#)IEEE 802.1Q [98](#)IGA [193](#)IGMP [99](#)multicast group list [253](#)
version [99](#)ILA [193](#)

Independent Basic Service Set

See IBSS [331](#)initialization vector (IV) [339](#)

Inside Global Address, see IGA

Inside Local Address, see ILA

interface group [201](#)

Internet

wizard setup [33](#)Internet access [18](#)wizard setup [33](#)Internet Protocol version 6 [77](#)

Internet Protocol version 6, see IPv6

Internet Service Provider, see ISP

IP address [134, 154](#)ping [283](#)private [155](#)WAN [76](#)IP Address Assignment [98](#)

IP alias

NAT applications [195](#)IPv6 [77, 345](#)addressing [77, 100, 345](#)EUI-64 [347](#)global address [346](#)interface ID [347](#)link-local address [345](#)Neighbor Discovery Protocol [345](#)ping [345](#)prefix [77, 100, 345](#)prefix delegation [79](#)prefix length [77, 100, 345](#)unspecified address [346](#)ISP [76](#)iTunes server [210](#)**L**LAN [133](#)client list [138](#)DHCP [134, 153](#)DNS [134, 154](#)IP address [134, 135, 154](#)MAC address [139](#)status [73](#)subnet mask [134, 135, 154](#)LAND attack [214](#)LAN-Side DSL CPE Configuration [265](#)LBR [282](#)

limitations

wireless LAN [122](#)WPS [130](#)link trace [282](#)

Link Trace Message, see LTM

Link Trace Response, see LTR

login [25](#)passwords [25, 26](#)logs [241, 245, 253, 273](#)

Loop Back Response, see LBR

loopback [282](#)LTM [282](#)LTR [282](#)**M**MA [282](#)MAC address [112, 139](#)filter [111, 121](#)MAC authentication [111](#)Mac filter [224](#)

Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
managing the device
 good habits [17](#)
MBSSID [123](#)
MD [282](#)
media server [210](#)
 activation [211](#)
 iTunes server [210](#)
MEP [282](#)
MoCA [151](#)
MTU (Multi-Tenant Unit) [98](#)
multicast [99](#)
Multiple BSS, see MBSSID

N

NAT [181](#), [183](#), [192](#), [193](#), [321](#)
 applications [194](#)
 IP alias [195](#)
 example [194](#)
 global [193](#)
 IGA [193](#)
 ILA [193](#)
 inside [193](#)
 local [193](#)
 outside [193](#)
 port forwarding [182](#)
 port number [195](#)
 services [195](#)
 SIP ALG [190](#)
 activation [190](#)
NAT example [196](#)
Network Address Translation
 see NAT
Network Address Translation, see NAT
Network Map [71](#)
network map [29](#)
NNTP [195](#)

P

Pairwise Master Key (PMK) [339](#), [341](#)
passwords [25](#), [26](#)
PBC [125](#)
Per-Hop Behavior, see PHB [177](#)
PHB [177](#)
PIN, WPS [125](#)
 example [127](#)
Ping of Death [214](#)
Point-to-Point Tunneling Protocol [195](#)
POP3 [195](#)
port forwarding [182](#)
ports [21](#)
PPP over Ethernet, see PPPoE
PPPoE [76](#), [97](#)
 Benefits [97](#)
PPTP [195](#)
preamble [117](#), [120](#)
preamble mode [124](#)
prefix delegation [79](#)
Printer Server [211](#)
printer sharing [62](#)
 configuration [62](#)
 requirements [211](#)
private IP address [155](#)
product registration [359](#)
protocol [76](#)
PSK [339](#)
push button [23](#)
Push Button Configuration, see PBC
push button, WPS [125](#)

Q

QoS [163](#), [176](#)
 marking [164](#)
 setup [163](#)
 tagging [164](#)
 versus CoS [164](#)
Quality of Service, see QoS

R

RADIUS [336](#)
 message types [336](#)
 messages [336](#)
 shared secret key [337](#)
 RADIUS server [121](#)
 registration
 product [359](#)
 related documentation [2](#)
 remote management
 TR-069 [263](#)
 Remote Procedure Calls, see RPCs [263](#)
 reset [22, 280](#)
 restart [281](#)
 restoring configuration [280](#)
 RFC 1058. See RIP.
 RFC 1389. See RIP.
 RFC 3164 [241](#)
 RIP [161](#)
 router features [18](#)
 Routing Information Protocol. See RIP
 RPPCs [263](#)
 RTS (Request To Send) [334](#)
 threshold [333, 334](#)
 RTS threshold [117, 120](#)

S

security
 wireless LAN [120](#)
 Security Log [243](#)
 Security Parameter Index, see SPI
 service access control [261](#)
 Service Set [104, 111](#)
 Services [195](#)
 setup
 firewalls [215](#)
 static route [96, 158, 198](#)
 Single Rate Three Color Marker, see srTCM
 SIP ALG [190](#)
 activation [190](#)
 SMTP [195](#)

SNMP [195](#)
 SNMP trap [195](#)
 SPI [214](#)
 srTCM [178](#)
 SSID [121](#)
 activation [110](#)
 MBSSID [123](#)
 static route [157, 271](#)
 configuration [96, 158, 198](#)
 example [157](#)
 static VLAN
 status [71](#)
 firmware version [73](#)
 LAN [73](#)
 WAN [73](#)
 wireless LAN [73](#)
 status indicators [21](#)
 subnet [315](#)
 subnet mask [134, 154, 316](#)
 subnetting [318](#)
 SYN attack [214](#)
 syslog
 protocol [241](#)
 severity levels [241](#)
 system
 firmware [277](#)
 version [73](#)
 passwords [25, 26](#)
 reset [22](#)
 status [71](#)
 LAN [73](#)
 WAN [73](#)
 wireless LAN [73](#)
 time [267](#)

T

Tag Control Information See TCI
 Tag Protocol Identifier See TPID
 TCI
 TFTP [152](#)
 The [76](#)
 thresholds
 data fragment [117, 120](#)
 RTS/CTS [117, 120](#)

- time [267](#)
 - TPID [98](#)
 - TR-064 [265](#)
 - TR-069 [263](#)
 - ACS setup [263](#)
 - authentication [264](#)
 - trTCM [179](#)
 - Two Rate Three Color Marker, see trTCM
- ## U
- unicast [99](#)
 - Universal Plug and Play, see UPnP
 - upgrading firmware [277](#)
 - UPnP [140](#)
 - cautions [135](#)
 - example [141](#)
 - installation [141](#)
 - NAT traversal [134](#)
 - USB features [20](#)
- ## V
- VID
 - Virtual Local Area Network See VLAN
 - VLAN [98](#)
 - Introduction [98](#)
 - number of possible VIDs
 - priority frame
 - static
 - VLAN ID [98](#)
 - VLAN Identifier See VID
 - VLAN tag [98](#)
- ## W
- WAN
 - status [73](#)
 - Wide Area Network, see WAN [75](#)
 - warranty
 - note [359](#)
 - WDS [114, 124](#)
 - compatibility [114](#)
 - example [124](#)
 - web configurator [25](#)
 - login [25](#)
 - passwords [25, 26](#)
 - WEP [122](#)
 - WEP Encryption [106, 107](#)
 - WEP encryption [105](#)
 - WEP key [105](#)
 - Wi-Fi Protected Access [338](#)
 - wireless client WPA supplicants [340](#)
 - Wireless Distribution System, see WDS
 - wireless LAN [101, 118](#)
 - authentication [120, 121](#)
 - BSS [123](#)
 - example [123](#)
 - channel [119](#)
 - encryption [122](#)
 - example [119](#)
 - fragmentation threshold [117, 120](#)
 - limitations [122](#)
 - MAC address filter [111, 121](#)
 - MBSSID [123](#)
 - preamble [117, 120](#)
 - RADIUS server [121](#)
 - RTS/CTS threshold [117, 120](#)
 - security [120](#)
 - SSID [121](#)
 - activation [110](#)
 - status [73](#)
 - WDS [114, 124](#)
 - compatibility [114](#)
 - example [124](#)
 - WEP [122](#)
 - WPA [122](#)
 - WPA-PSK [122](#)
 - WPS [124, 127](#)
 - example [128](#)
 - limitations [130](#)
 - PIN [125](#)
 - push button [23, 125](#)
 - wireless security [335](#)
 - Wireless tutorial [40](#)
 - wizard setup
 - Internet [33](#)
 - WLAN
 - interference [333](#)
 - security parameters [342](#)

- WPA [122](#), [338](#)
 - key caching [340](#)
 - pre-authentication [340](#)
 - user authentication [339](#)
 - vs WPA-PSK [339](#)
 - wireless client supplicant [340](#)
 - with RADIUS application example [340](#)
- WPA2 [338](#)
 - user authentication [339](#)
 - vs WPA2-PSK [339](#)
 - wireless client supplicant [340](#)
 - with RADIUS application example [340](#)
- WPA2-Pre-Shared Key [339](#)
- WPA2-PSK [339](#)
 - application example [341](#)
- WPA-PSK [122](#), [339](#)
 - application example [341](#)
- WPS [124](#), [127](#)
 - example [128](#)
 - limitations [130](#)
 - PIN [125](#)
 - example [127](#)
 - push button [23](#), [125](#)

