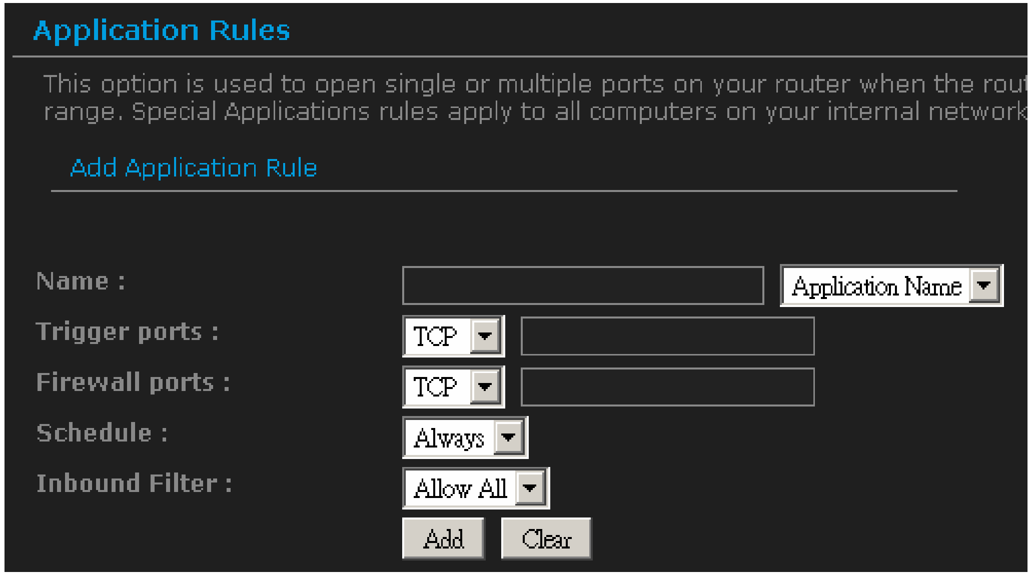
- **Public Port**: Specify the public port number.
- **Private Port**: Specify the private port number.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- **Inbound Filter**: Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Add** button to insert the entry into the Virtual Server list.

6.3.3.Special Applications

An application rule is used to open single or multiple ports on your router when the router senses data sent to the Internet on a trigger port or port range. An application rule applies to all computers on your internal network.



Application Rules

This option is used to open single or multiple ports on your router when the rout
range. Special Applications rules apply to all computers on your internal network

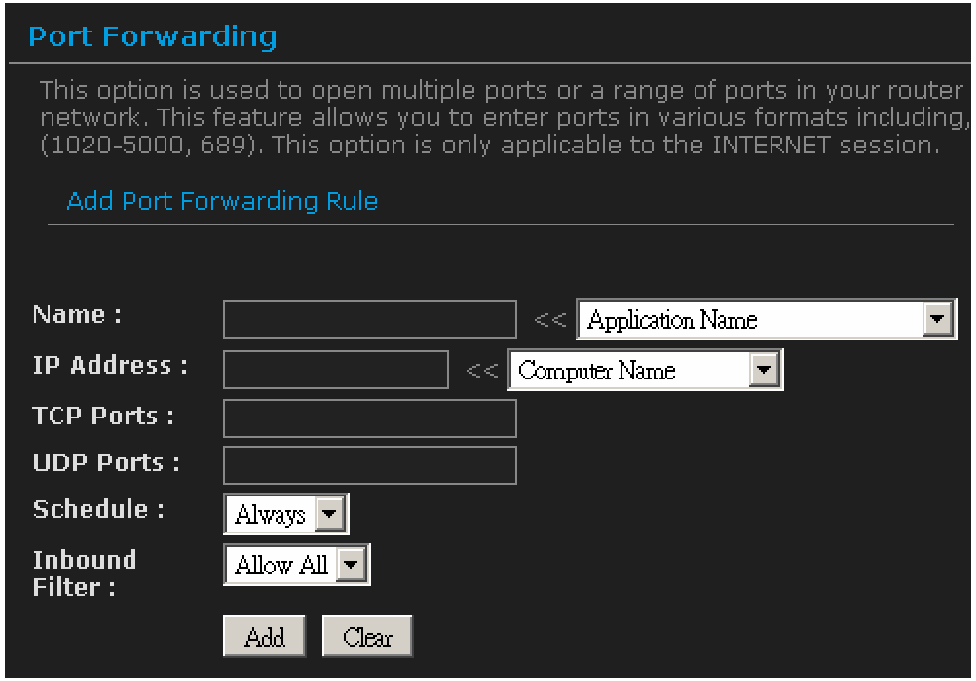
Add Application Rule

Name :		Application Name
Trigger ports :	TCP	
Firewall ports :	TCP	
Schedule :	Always	
Inbound Filter :	Allow All	

- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the **Application Name** drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **Triggering Ports**: Specify the outgoing port range that is used by the application.
- **Firewall Ports**: Specify the port range that you would like to open for Internet traffic.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- Click on the **Add** button to insert the entry into the Special Applications list.

6.3.4.Port Forwarding

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.



Port Forwarding

This option is used to open multiple ports or a range of ports in your router network. This feature allows you to enter ports in various formats including, (1020-5000, 689). This option is only applicable to the INTERNET session.

Add Port Forwarding Rule

Name : << Application Name

IP Address : << Computer Name

TCP Ports :

UDP Ports :

Schedule : Always

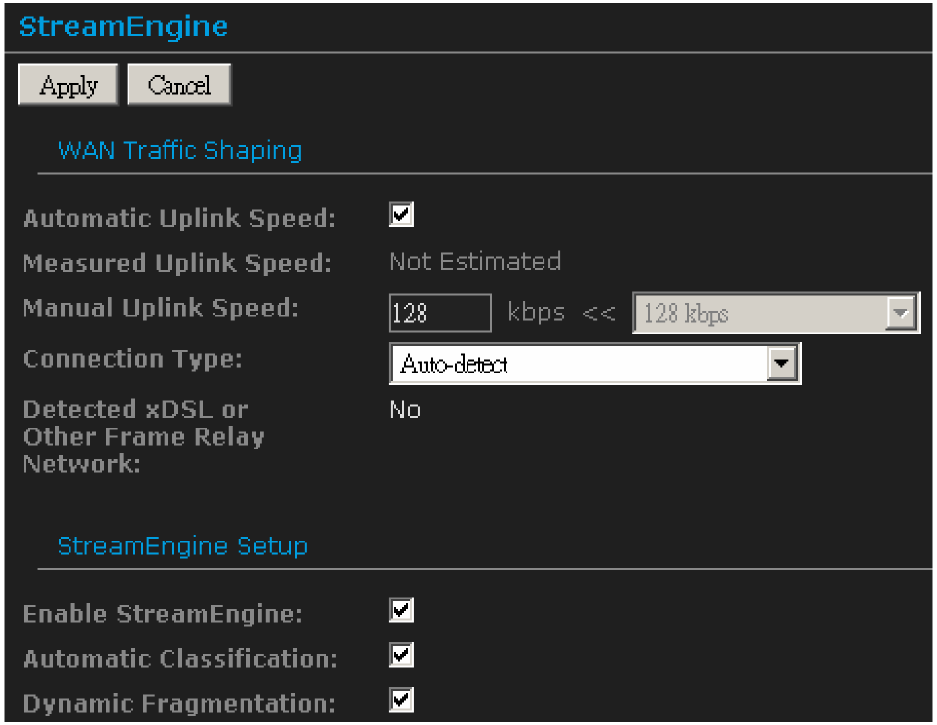
Inbound Filter : Allow All

- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the Application Name drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address**: Specify the IP address for the virtual server entry.
- **TCP/UDP Ports**: Specify the TCP or UDP port numbers.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.

- **Inbound Filter**: Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Add** button to insert the entry into the Port Forwarding list.

6.3.5.StreamEngine

The StreamEngine feature helps improve the network performance by prioritizing applications.



StreamEngine

WAN Traffic Shaping

Automatic Uplink Speed: ☑

Measured Uplink Speed: Not Estimated

Manual Uplink Speed: 128 kbps << 128 kbps

Connection Type: Auto-detect

Detected xDSL or Other Frame Relay Network: No

StreamEngine Setup

Enable StreamEngine: ☑

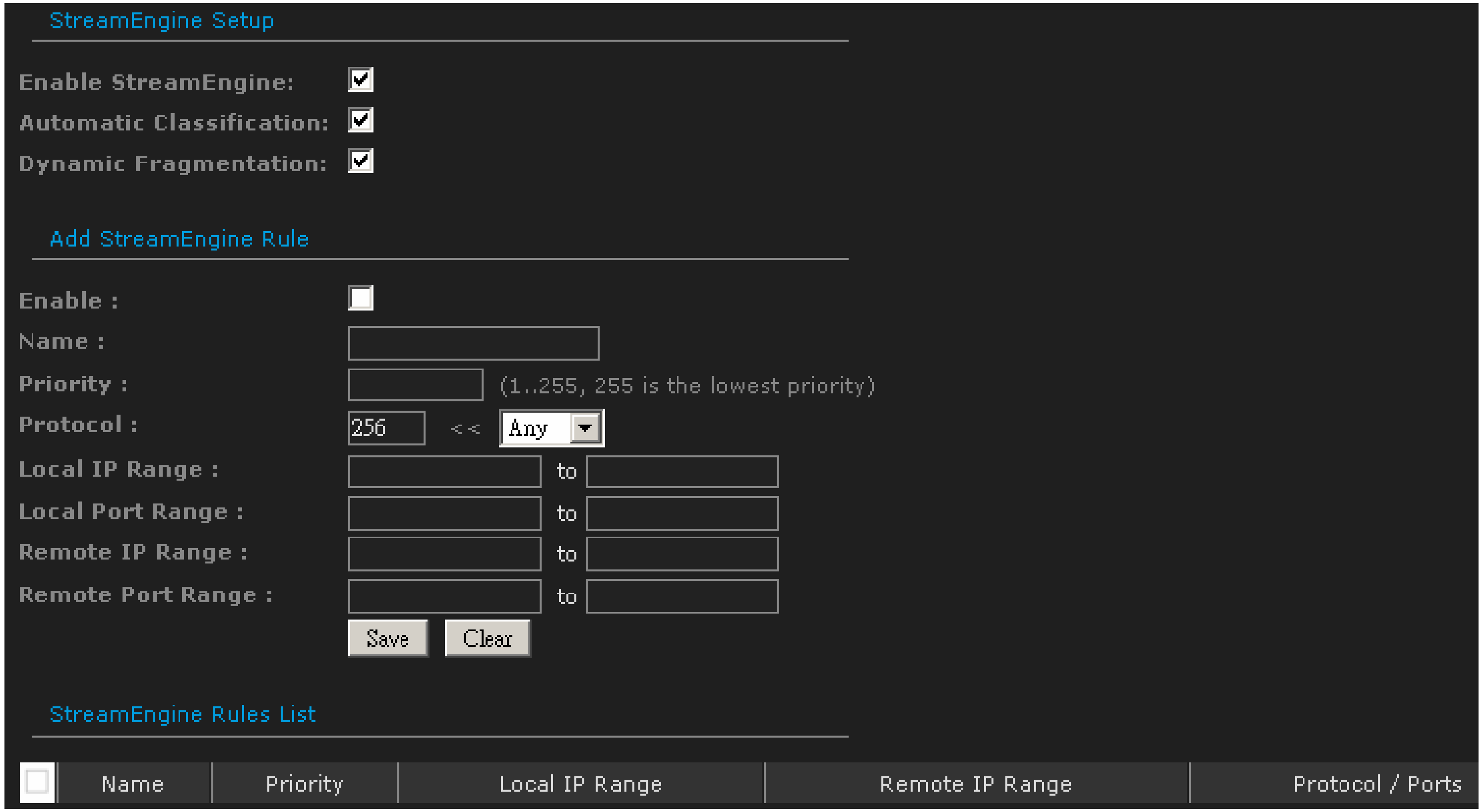
Automatic Classification: ☑

Dynamic Fragmentation: ☑

- **Enable Traffic Shaping**: Place a check in the box to enable traffic shaping. When this option is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.
- **Automatic Uplink Speed**. Place a check in this box to enable automatic uplink speed. When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).
- **Measured Uplink Speed**: Displays the uplink speed. This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads

associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.

- **Manual Uplink Speed**: Specify an uplink speed or select it from the drop-down list. If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP.
- **Connection Type**: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either Static or DHCP in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.
- Click on the **Apply** button to store these settings.



StreamEngine Setup

Enable StreamEngine: ☑

Automatic Classification: ☑

Dynamic Fragmentation: ☑

Add StreamEngine Rule

Enable : □

Name :

Priority : (1..255, 255 is the lowest priority)

Protocol : 256 << Any

Local IP Range : to

Local Port Range : to

Remote IP Range : to

Remote Port Range : to

Save Clear

StreamEngine Rules List

□	Name	Priority	Local IP Range	Remote IP Range	Protocol / Ports

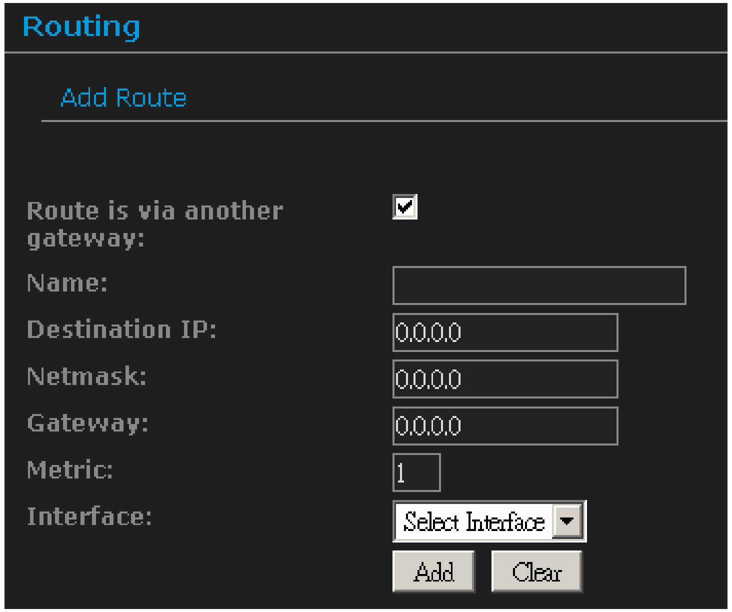
- **Enable StreamEngine**: Place a check in this box to enable this option. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.
- **Automatic Classification**: Place a check in this box to enable this option. This option is enabled by default so that your router will automatically determine which programs should have network priority.
- **Dynamic Fragmentation**: Place a check in this box to enable this option. This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

- **Add StreamEngine Rule**: A StreamEngine Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific StreamEngine Rules will not be required. StreamEngine supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.

- **Enable**: Place a check in this box to enable the StreamEngine rule.
- **Name**: Specify a name for the rule.
- **Priority**: Specify a priority for the rule. Being with 1 which is the highest and 255 the lowest priority.
- **Protocol**: Specify a protocol or select one from the drop-down list.
- **Local IP Range**: Specify the local (LAN) IP address range.
- **Local Port Range**: Specify the local (LAN) port range.
- **Remote IP Range**: Specify the remote (WAN) IP address range.
- **Remote Port Range**: Specify the remote (WAN) port range.
- Click on the **Save** button to insert the entry into the StreamEngine list.

6.3.6.Routing

This section adds a new entry into the routing table.



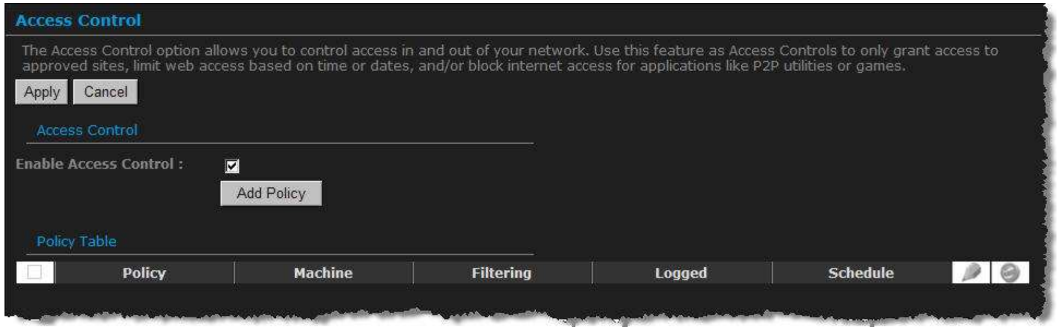
Route is via another gateway:	☑
Name:	
Destination IP:	0.0.0.0
Netmask:	0.0.0.0
Gateway:	0.0.0.0
Metric:	1
Interface:	Select Interface

- **Name**: Specify a name for the rule.
- **Destination IP**: Specify the destination IP address.
- **Netmask**: Specify the subnet mask for the IP address.
- **Gateway**: Specify the IP address of the gateway.
- **Metric**: Specify the number of routing hops. The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.
- **Interface**: Select the interface from the drop-down list.
- Click on the **Add** button to insert the entry into the Routing table.

6.3.7.Access Control

The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.

When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.



Access Control

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

Access Control

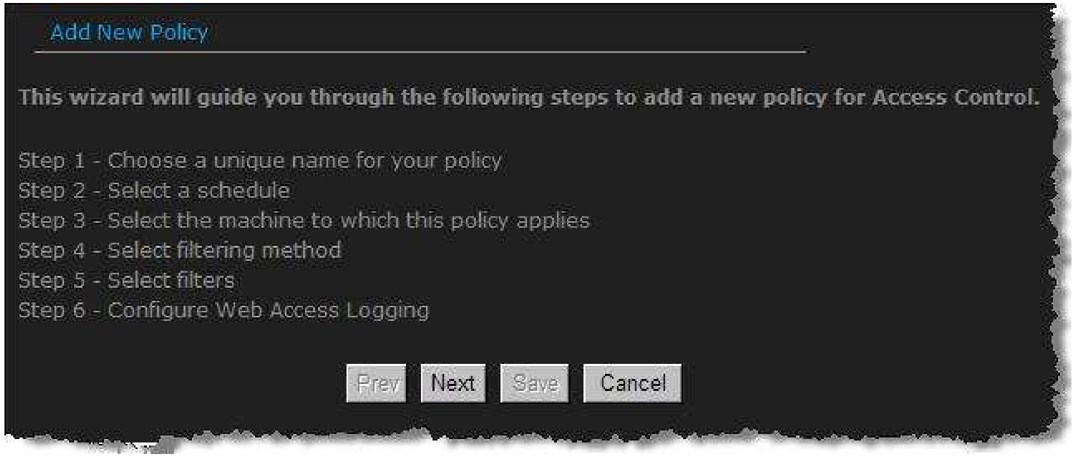
Enable Access Control : ☑

Policy Table

□	Policy	Machine	Filtering	Logged	Schedule

- Place a check in the **Enable Access Control** check box and then click on the **Add Policy** button. This will bring up the **Add New Policy** wizard.
- The wireless wizard will inform you that there are six major steps in the process.
- Choose a unique name for your policy
- Select a schedule
- Select the machine to which the policy applies
- Select filtering method
- Configure web access logging

- Click on the **Next** button to continue.

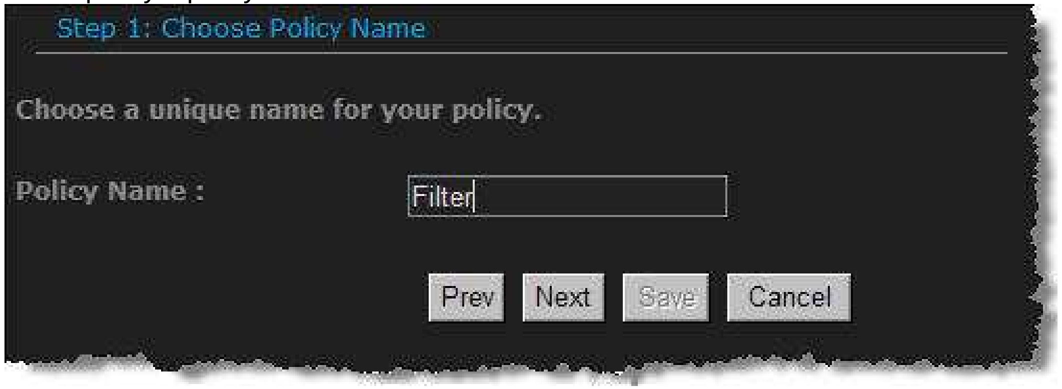


Add New Policy

This wizard will guide you through the following steps to add a new policy for Access Control.

Step 1 - Choose a unique name for your policy
Step 2 - Select a schedule
Step 3 - Select the machine to which this policy applies
Step 4 - Select filtering method
Step 5 - Select filters
Step 6 - Configure Web Access Logging

- Specify a policy name and then click on the **Next** button to continue.

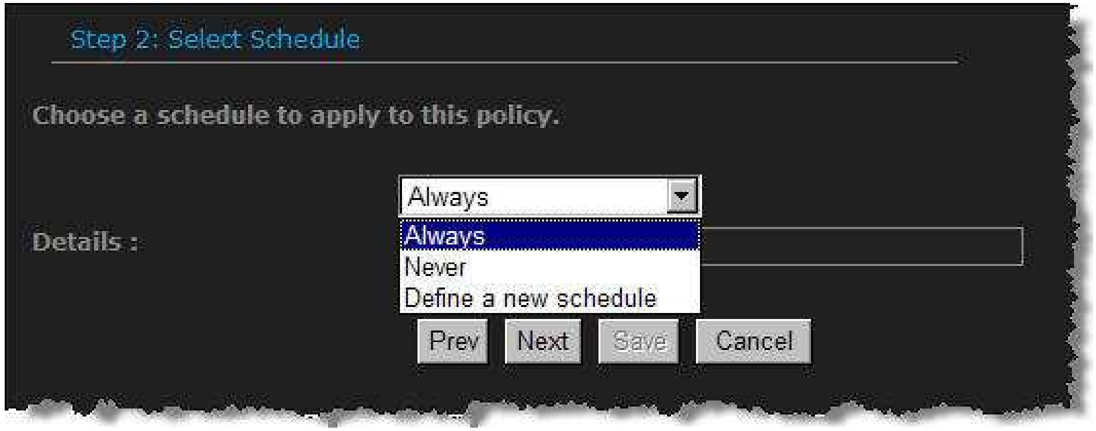


Step 1: Choose Policy Name

Choose a unique name for your policy.

Policy Name : Filter

- Select a schedule from the drop-down list: **Always** or **Never**, or you may define a new schedule. Click on the **Next** button to continue.

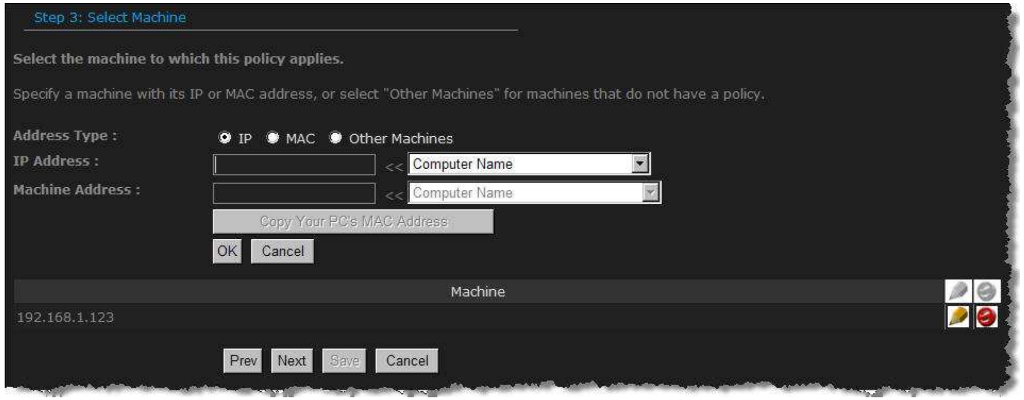


Step 2: Select Schedule

Choose a schedule to apply to this policy.

Details :

- Select a machine to which the policy applies.
- **Address Type**: Select the IP address or MAC address radio button.
- **IP Address**: If you selected IP address above, then specify the IP address here.
- **MAC Address**: If you need to change the MAC address of the rounter's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PCs MAC Address**.
- Click on the **OK** button to insert the entry into the table.
- Click on the **Next** button to continue.



Step 3: Select Machine

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

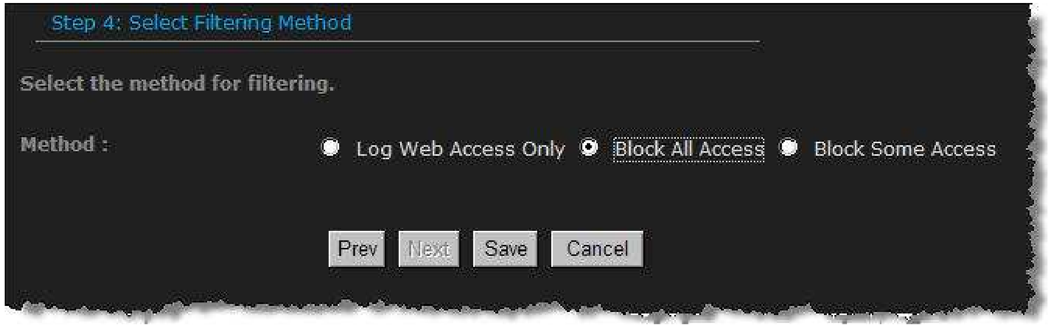
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : << Computer Name

Machine Address : << Computer Name

Machine
192.168.1.123

- Select a filtering method:
- **Log Web Access Only**: Select this radio but in order to log web access.
- **Block All Access**: Select this radio but in order to block all web access.
- **Block Some Access**: Select this radio but in order to block some web access.
- Click on the **Save** button to store the changes.



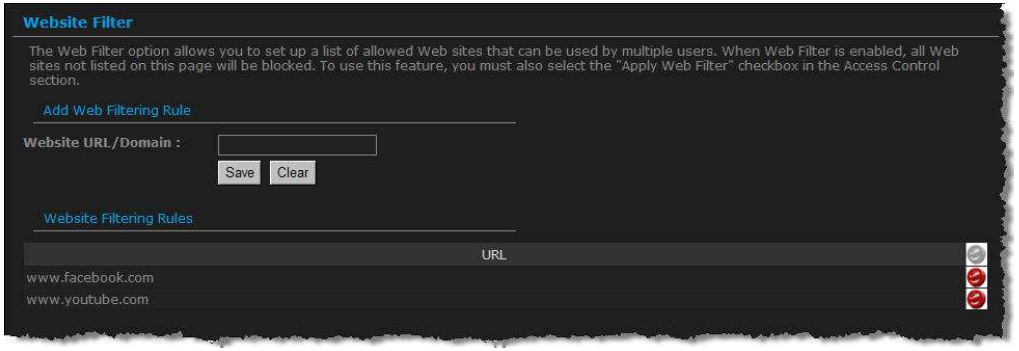
Step 4: Select Filtering Method

Select the method for filtering.

Method : ○ Log Web Access Only ● Block All Access ○ Block Some Access

6.3.8.Web Filter

This is a type of parental control feature used to restrict certain websites form being accessed through your network. These filters can be used for securing and restricting your network.



Website Filter

The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

Add Web Filtering Rule

Website URL/Domain :

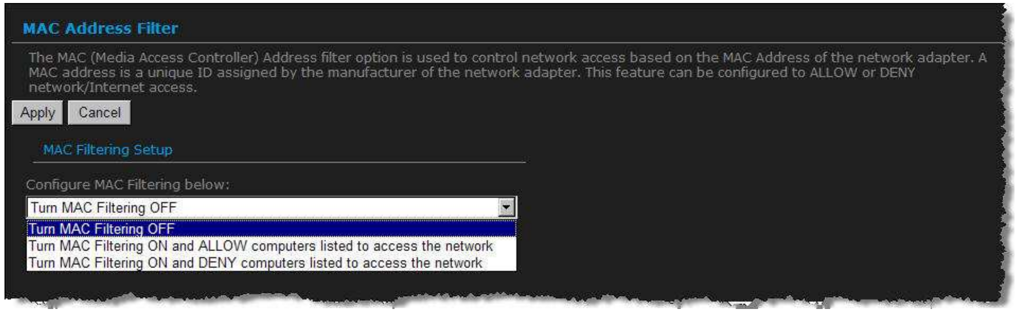
Website Filtering Rules

URL
www.facebook.com
www.youtube.com

Website/URL/Domain: Specify the web address that you would like to filter. **Do not use "http://"**
Click on the **Save** button to store the changes.

6.3.9.MAC Address Filter

This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.



MAC Address Filter

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Apply
Cancel
MAC Filtering Setup

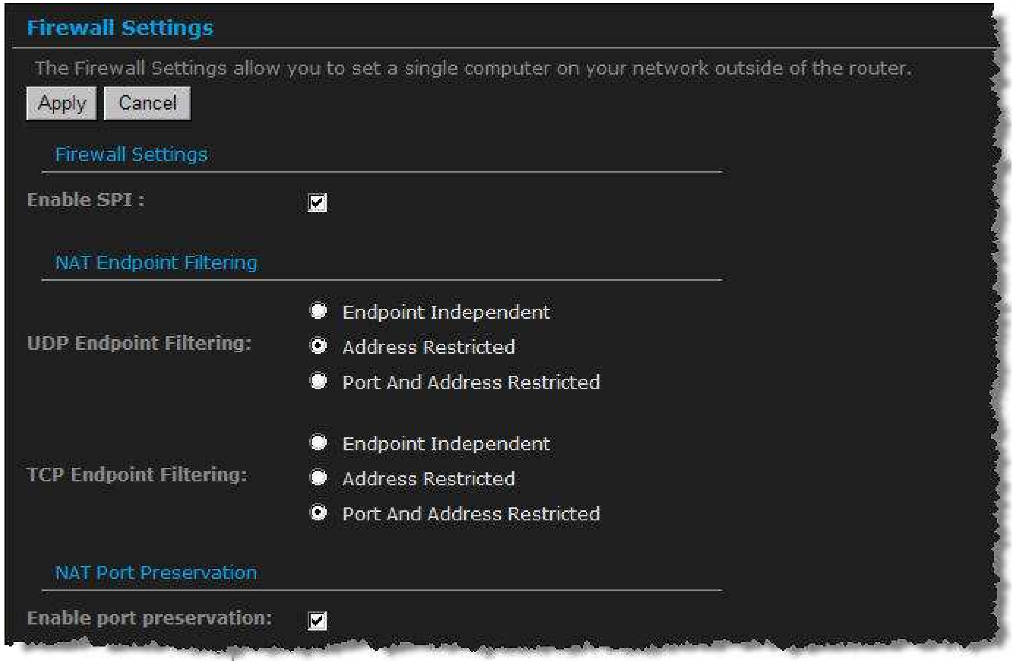
Configure MAC Filtering below: Turn MAC Filtering OFF

Turn MAC Filtering OFF
Turn MAC Filtering ON and ALLOW computers listed to access the network
Turn MAC Filtering ON and DENY computers listed to access the network

- **Configure MAC Filtering**: Select one of the options from the drop-down list.
- **Turn MAC Filtering OFF:** When "OFF" is selected, MAC addresses are not used to control network access.
- **Turn MAC Filtering ON and ALLOW computers listed to access the network:** When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Filtering Rules list are granted network access.
- **Turn MAC Filtering ON and DENY computers listed to access the network:** When "DENY" is selected, any computer with a MAC address listed in the MAC Filtering Rules list is refused access to the network.
- **MAC Address**: Specify that MAC address that you would like to filter.
- Click on the **Save** button to store the changes.

6.3.10. Firewall

The device provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.



Firewall Settings

The Firewall Settings allow you to set a single computer on your network outside of the router.

Firewall Settings

Enable SPI : ☑

NAT Endpoint Filtering

UDP Endpoint Filtering:
○ Endpoint Independent
● Address Restricted
○ Port And Address Restricted

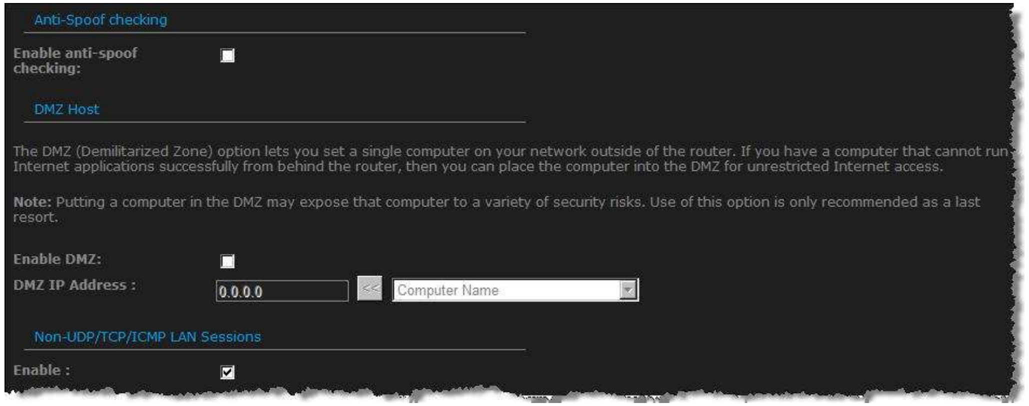
TCP Endpoint Filtering:
○ Endpoint Independent
○ Address Restricted
● Port And Address Restricted

NAT Port Preservation

Enable port preservation: ☑

- **Enable SPI**: Place a check in this box to enable SPI. SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol. When the protocol is TCP, SPI checks that packet sequence numbers are within the valid range for the session, discarding those packets that do not have valid sequence numbers. Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.

- **TCP / UDP NAT Endpoint Filtering** options control how the router's NAT manages incoming connection requests to ports that are already being used. Select one of the radio buttons.
- **End Point Independent** Once a LAN-side application has created a connection through a specific port, the NAT will forward any incoming connection requests with the same port to the LAN-side application regardless of their origin. This is the least restrictive option, giving the best connectivity and allowing some applications (P2P applications in particular) to behave almost as if they are directly connected to the Internet.
- **Address Restricted** The NAT forwards incoming connection requests to a LAN-side host only when they come from the same IP address with which a connection was established. This allows the remote application to send data back through a port different from the one used when the outgoing session was created.
- **Port And Address Restricted** The NAT does not forward any incoming connection requests with the same port address as an already establish connection.
- **Note**: Some of these options can interact with other port restrictions. Endpoint Independent Filtering takes priority over inbound filters or schedules, so it is possible for an incoming session request related to an outgoing session to enter through a port in spite of an active inbound filter on that port. However, packets will be rejected as expected when sent to blocked ports (whether blocked by schedule or by inbound filter) for which there are no active sessions. Port and Address Restricted Filtering ensures that inbound filters and schedules work precisely, but prevents some level of connectivity, and therefore might require the use of port triggers, virtual servers, or port forwarding to open the ports needed by the application. Address Restricted Filtering gives a compromise position, which avoids problems when communicating with certain other types of NAT router (symmetric NATs in particular) but leaves inbound filters and scheduled access working as expected.
- **Enable Port Preservation**: Place a check in this box to enable Port Preservation. NAT Port preservation (on by default) tries to ensure that, when a LAN host makes an Internet connection, the same LAN port is also used as the Internet visible port. This ensures best compatibility for internet communications. Under some circumstances it may be desirable to turn off this feature.



Anti-Spoof checking

Enable anti-spoof checking: □

DMZ Host

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

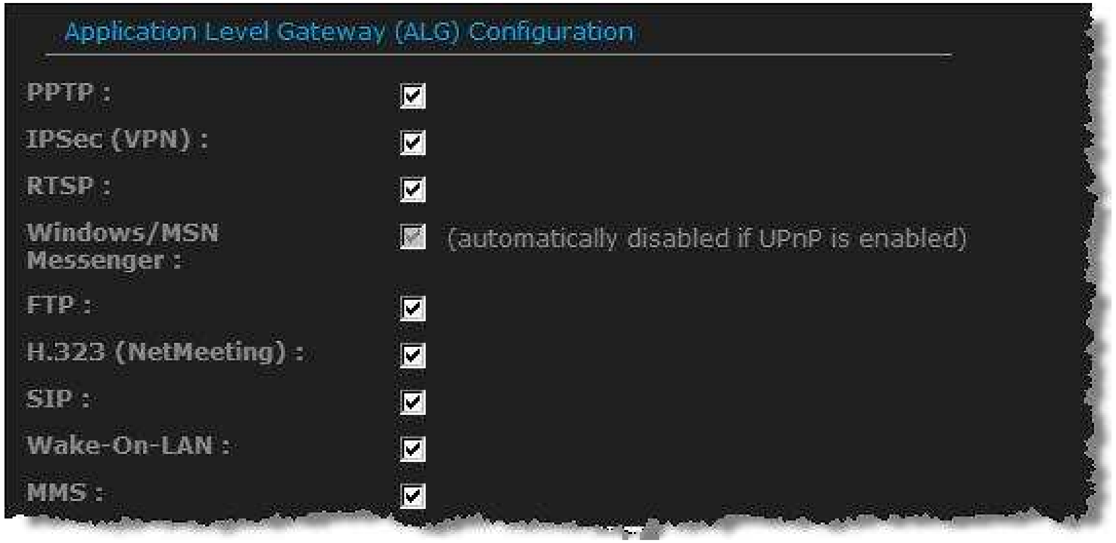
Enable DMZ: □

DMZ IP Address : 0.0.0.0 << Computer Name

Non-UDP/TCP/ICMP LAN Sessions

Enable : ☑

- **Enable anti-spoof checking**: Place a check in this box to enable anti-spoof checking. Enabling this option can provide protection from certain kinds of "spoofing" attacks. However, enble this option with care. With some modems, the WAN connection may be lost when this option is enabled. In that case, it may be necessary to change the LAN subnet to something other than 192.168.0.x (192.168.2.x, for example), to re-establish the WAN connection.
- **Enable DMZ Host**: Place check in this box to enable DMZ host. DMZ host is a demilitarized zone used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web, FTP, email and DNS servers.
- **DMZ IP Address**: Specify the IP address of the DMZ host.
- **Non-UDP/TCP/ICMP LAN Sessions**: Place a check in this box to enable this feature. When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol. This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an ALG.
- **Note**: This feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions.
- Enabling this option (the default setting) enables single VPN connections to a remote host. (But, for multiple VPN connections, the appropriate VPN ALG must be used.) Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled.



Application Level Gateway (ALG) Configuration

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

Windows/MSN Messenger : ☑ (automatically disabled if UPnP is enabled)

FTP : ☑

H.323 (NetMeeting) : ☑

SIP : ☑

Wake-On-LAN : ☑

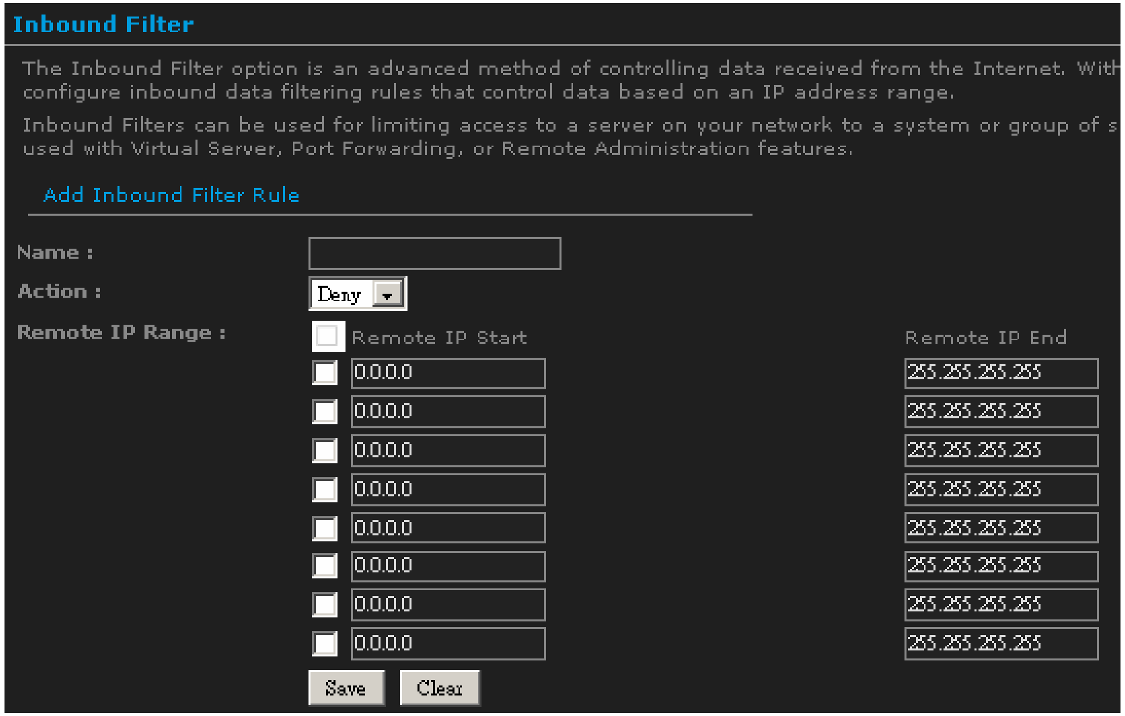
MMS : ☑

- **Application Layer Gateway (ALG)** Configuration: Place a check in appropriate feature boxes to enable them. . Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.
- **PPTP**: Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to Advanced → Virtual Server).
- **IPSec**: (VPN) Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option. Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.
- **RTSP**: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.
- **Windows/MSN Messenger**: Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) and MSN Messenger. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled.
- **FTP**: Allows FTP clients and servers to transfer data across NAT.
- **H.323 (Netmeeting)**: Allows H.323 (specifically Microsoft Netmeeting) clients to communicate across NAT server.
- **SIP**: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.
- **Wake-On-LAN**: This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable.
- **MMS**: Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet.
- Click on the **Apply** button to store these settings.

6.3.11. Inbound Filter

When you use the Virtual Server, Port Forwarding, or Remote Administration features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyber attacks from the Internet. In these cases, you can use Inbound Filters to limit that exposure by specifying the IP addresses of internet hosts that you trust to access your LAN through the ports that you have opened.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features.



Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With
configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of s
used with Virtual Server, Port Forwarding, or Remote Administration features.

Add Inbound Filter Rule

Name :

Action : Deny

Remote IP Range :

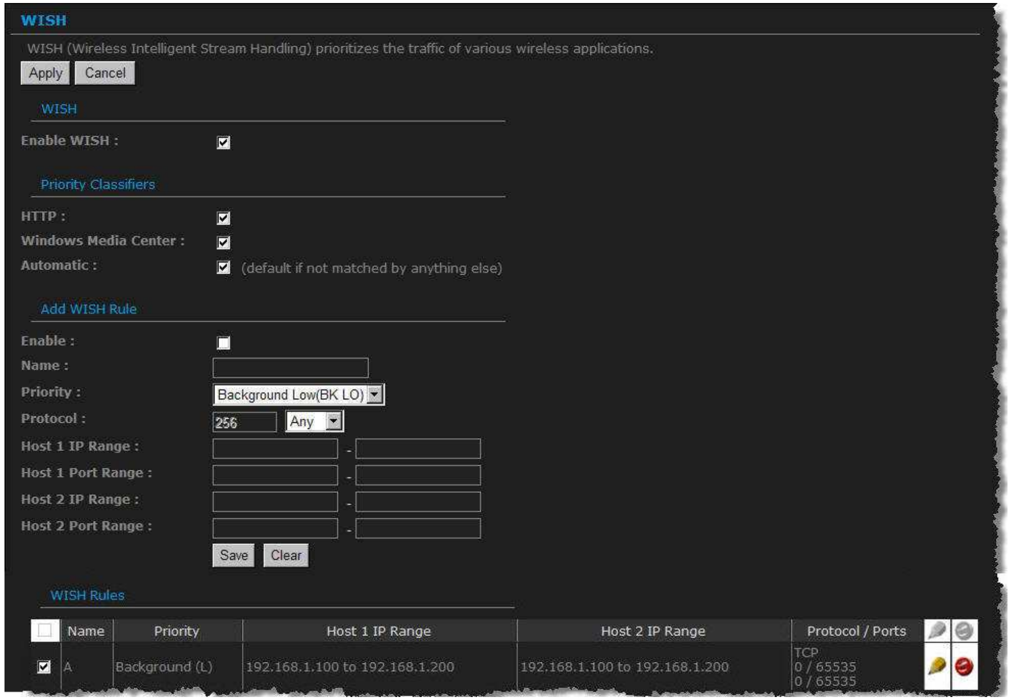
□	Remote IP Start	Remote IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255

- **Name** Specify a name for the inbound filter.

- **Action:** Select Allow or Deny from the drop-down list. This will apply the inbound filter rule on the WAN interface.
- **Remote IP Range:** Specify the remote IP address range and then click in the check box to enable the range.
- Click on the **Save** button to store the changes.

6.3.12. WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.



WISH

WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.

WISH

Enable WISH : ☑

Priority Classifiers

HTTP : ☑
Windows Media Center : ☑
Automatic : ☑ (default if not matched by anything else)

Add WISH Rule

Enable : ☐
Name :
Priority : Background Low(BK LO)
Protocol : 256 Any
Host 1 IP Range : -
Host 1 Port Range : -
Host 2 IP Range : -
Host 2 Port Range : -

WISH Rules

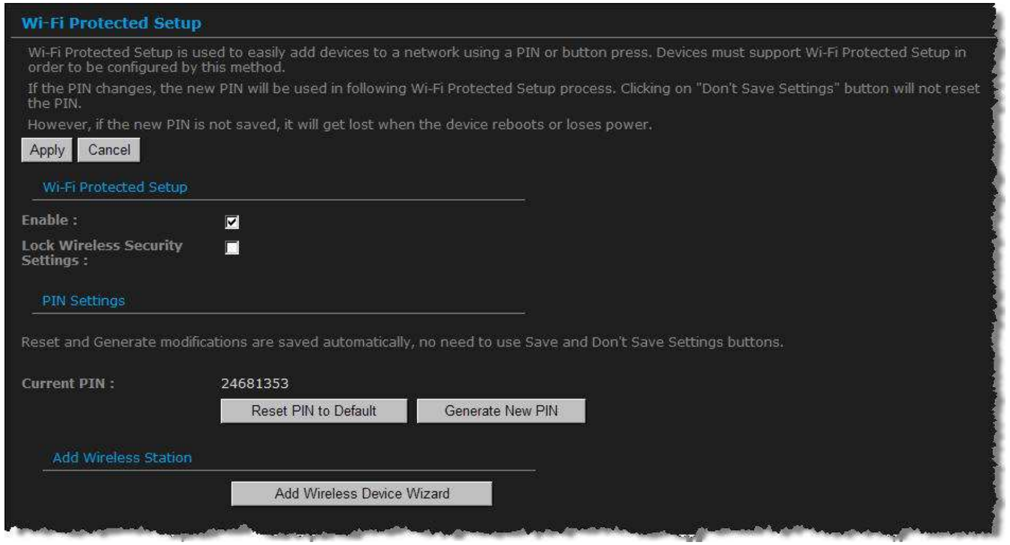
☐	Name	Priority	Host 1 IP Range	Host 2 IP Range	Protocol / Ports	✎	⊘
☑	A	Background (L)	192.168.1.100 to 192.168.1.200	192.168.1.100 to 192.168.1.200	TCP 0 / 65535 0 / 65535	✎	⊘

- **Enable WISH**: Place a check in this box to enable the WISH feature.

- **HTTP**: Place a check in this box to add HTTP as a classifier. This allows the device to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.
- **Windows Media Center**: Place a check in this box to add HTTP as a classifier. This enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.
- **Automatic**: Place a check in this box for the device to automatically configure the classifiers. When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.
- **Enable**: Place a check in this box to enable the WISH rule. A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.
- **Name**: Assign a meaningful name to the WISH rule.
- **Priority**: Select a priority from the drop-down list. The four priority message flows are:
- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).
- **Protocol**: Select a protocol from the drop-down list.
- **Hos1 IP Range**: Specify the IP range for the rule.
- **Host 1 Port Range**: Specify the port range for the rule.
- **Host 2 IP Range**: Specify the IP range for the rule.
- **Host 2 Port Range**: Specify the port range for the rule.
- Click on the **Save** button to insert the entry into the WISH rules list.

6.3.13. Wi-Fi Protected Setup

Wi-Fi Protected Setup is a feature that locks the wireless security settings and prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup.



Wi-Fi Protected Setup

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

Wi-Fi Protected Setup

Enable : ☑

Lock Wireless Security Settings : □

PIN Settings

Reset and Generate modifications are saved automatically, no need to use Save and Don't Save Settings buttons.

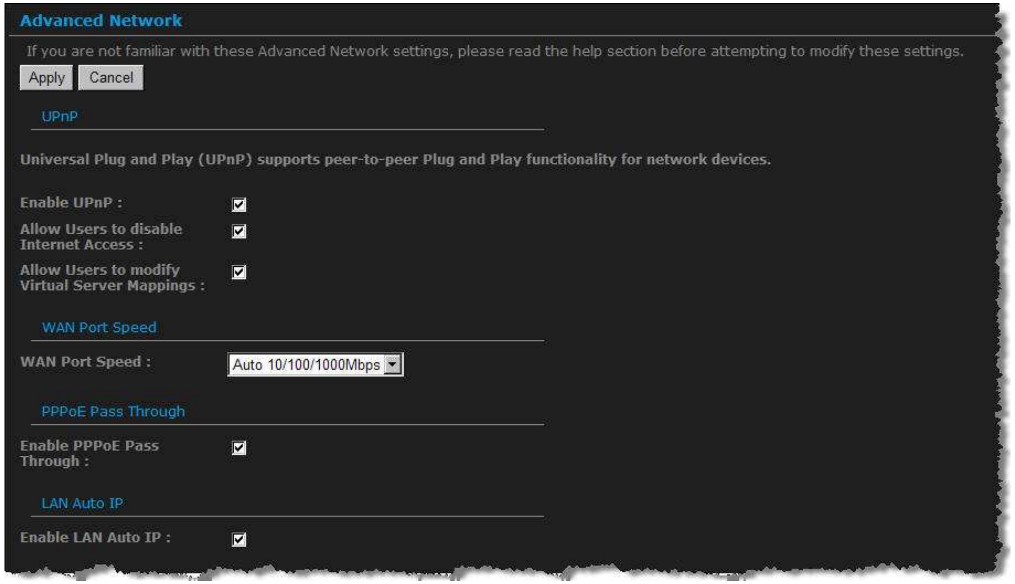
Current PIN : 24681353

Add Wireless Station

- **Enable**: Place a check in this box to enable this feature.
- **Lock**: Place a check in this box to lock the wireless security settings and prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup.
- **Reset PIN to Default**: Press this button to reset the PIN to it's default setting.
- **Generate NEW PIN**: Press this button to generate a new random PIN.
- **Add Wireless Device Wizard**: Please refer to Chapter 4 in order to configure Wi-Fi Protected Setup using the Wizard.
- Click on the **Apply** button to store these settings.

6.3.14. Advanced Network (UPNP, WAN Ping…)

In this section you can configure the UPNP, WAN Ping, WAN port speed, multicast streams, and PPPoE pass-through settings.



Advanced Network

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

UPnP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP : ☑

Allow Users to disable Internet Access : ☑

Allow Users to modify Virtual Server Mappings : ☑

WAN Port Speed

WAN Port Speed : Auto 10/100/1000Mbps

PPPoE Pass Through

Enable PPPoE Pass Through : ☑

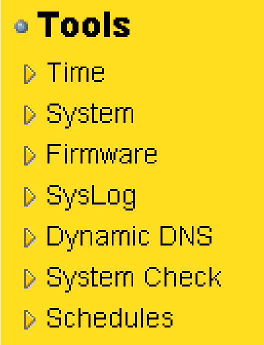
LAN Auto IP

Enable LAN Auto IP : ☑

- **Enable UPnP**: Place a check in this box to enable UPnP. UPnP stands for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software.
- **Allow Users to disable Internet Access**: Place a check in this box if you would like to allow to user to terminate the WAN session.
- **Allow Users to modify Virtual Server Mappings**: Place a check in this box if you would like the users to add, modify, or delete server mapping entries.
- **Enable WAN Ping Respond**: Place a check in this box if you would like this device to be pinged from the WAN side.
- **WAN Ping Inbound Filter**: You may select the computer that may ping this device from the WAN side.
- **WAN Port Speed**: You may select a WAN port speed from the drop-down list. It is recommended that you select **Auto**.

- **Enable Multicast Streams**: Place a check in this box to enable multicast streams. The router uses the IGMP protocol to support efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.
- **Enable PPPoE Pass Through**: Place a check in this box to enable PPPoE pass-through. This option controls whether LAN computers can act as PPPoE clients and negotiate the PPP sessions through the router over the WAN ethernet link. Enabling this option allows LAN computers to act as PPPoE clients. Disabling this option prevents LAN computers from establishing PPPoE pass-through connections.
- Click on the **Apply** button to store these settings.

6.4. Tools

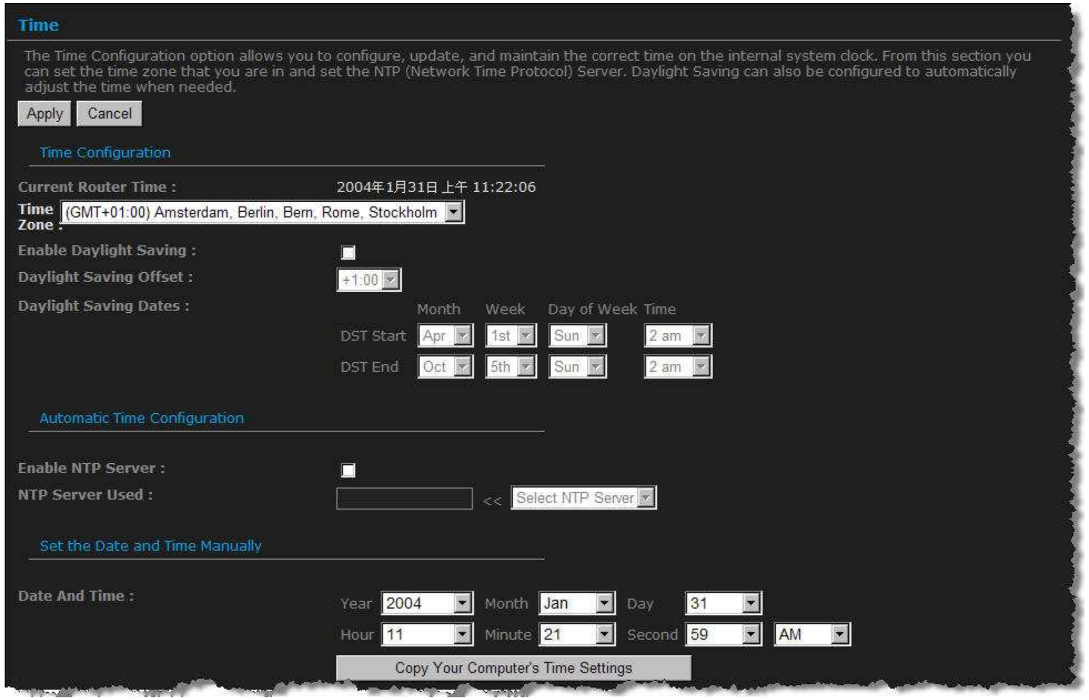


Click on the **Tools** link on the navigation drop-down menu. You will then see seven options: Time, System, Firmware, SysLog, Dynamic DNS, System Check, and Schedules. The configuration steps for each option are described below.

6.4.1.Time Zone Setting

Click on the **Time** link in the navigation menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

Note: If the device losses power for any reason, it will not be able to keep its time running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.



Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time Configuration

Current Router Time : 2004年1月31日 上午 11:22:06

Time Zone : (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm

Enable Daylight Saving : □

Daylight Saving Offset : +1:00

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Apr	1st	Sun	2 am
DST End	Oct	5th	Sun	2 am

Automatic Time Configuration

Enable NTP Server : □

NTP Server Used : << Select NTP Server

Set the Date and Time Manually

Date And Time :

Year 2004 Month Jan Day 31

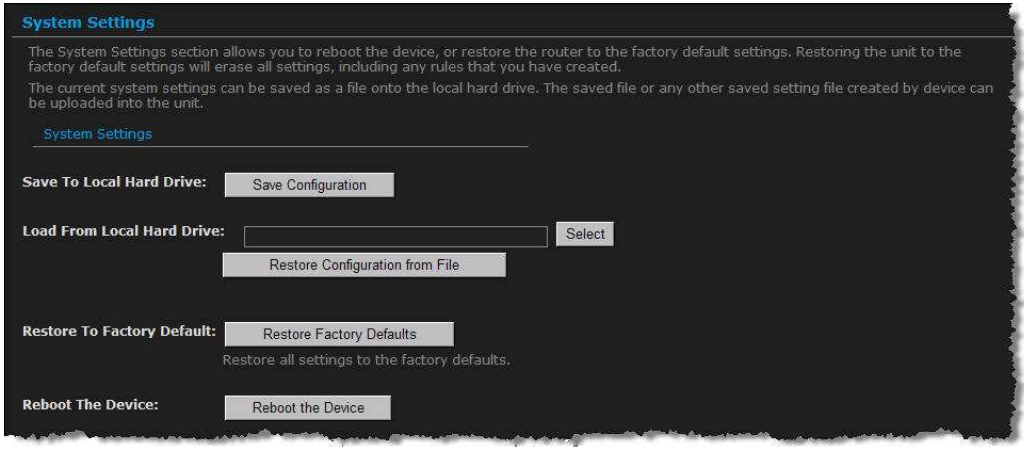
Hour 11 Minute 21 Second 59 AM

- **Current Router Time**: Displays the current time on the device.
- **Time Zone**: Select your time zone from the drop-down list.

- **Enable Daylight Saving**: Place a check in this box to enable daylight savings time.
- **Daylight Saving Offset**: Select the offset from the drop-down list.
- **Daylight Saving Date**: Select the daylight savings date from the drop-down list. Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."
- **Enable NTP Server**: Place a check in this box if you would like to synchronize the device's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.
- **NTP Server Used**: Specify the NTP server or select one from the drop-down list.
- **Set the Date and Time**: Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Apply** button once you have modified the settings.

6.4.2.System

Click on the **System** link in the navigation menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.



System Settings

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

System Settings

Save To Local Hard Drive:

Load From Local Hard Drive:

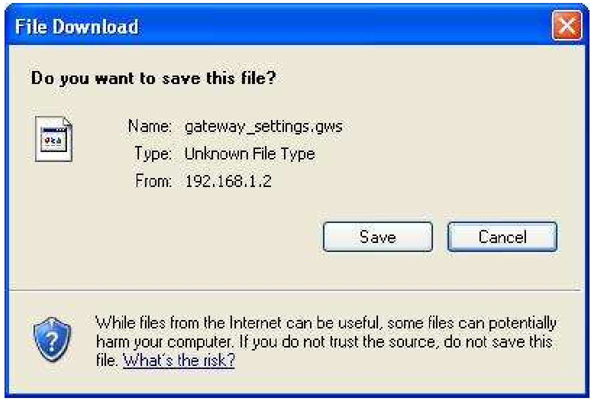
Restore To Factory Default:

Restore all settings to the factory defaults.

Reboot The Device:

6.4.2.1. Save To Local Hard Drive

This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



File Download

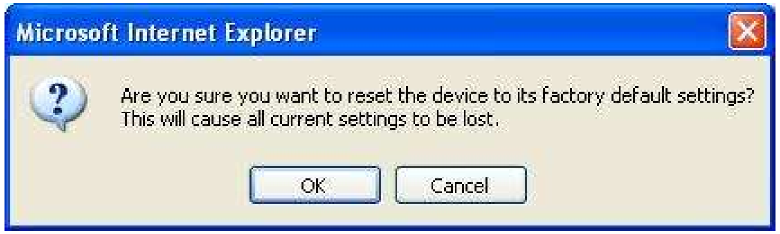
Do you want to save this file?

Name: gateway_settings.gws
Type: Unknown File Type
From: 192.168.1.2

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

6.4.2.2. Load From Local Hard Drive

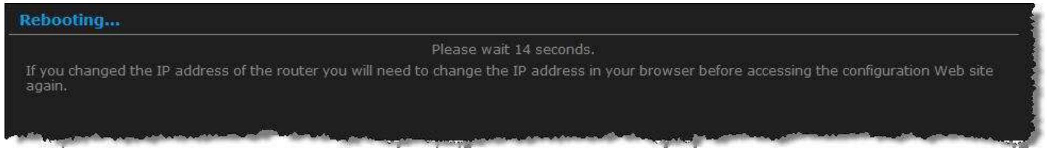
This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
The system then prompts you to reboot the device.



Microsoft Internet Explorer

Are you sure you want to reset the device to its factory default settings?
This will cause all current settings to be lost.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.



Rebooting...

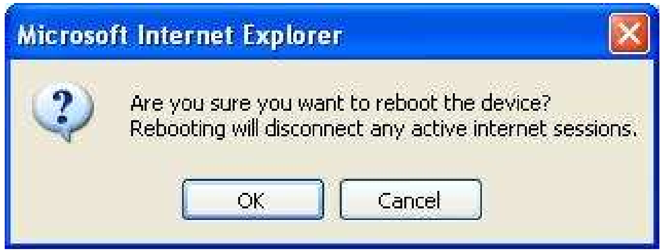
Please wait 14 seconds.

If you changed the IP address of the router you will need to change the IP address in your browser before accessing the configuration Web site again.

Please wait while the system is rebooting.
Note: Do no un-plug the device during this process as this may cause permanent damage.

6.4.2.3. Restore To Factory Default

Click on the **Restore all Settings to Factory Defaults** button. This option restores all configuration settings back to the settings that were in effect at the time when the device was shipped from the factory.

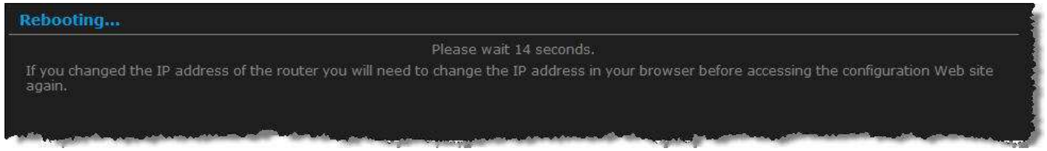


Microsoft Internet Explorer

Are you sure you want to reboot the device?
Rebooting will disconnect any active internet sessions.

Once the dialog box appears, click on the **OK** button to confirm the action.
Note: The current settings will be lost.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.



Rebooting...

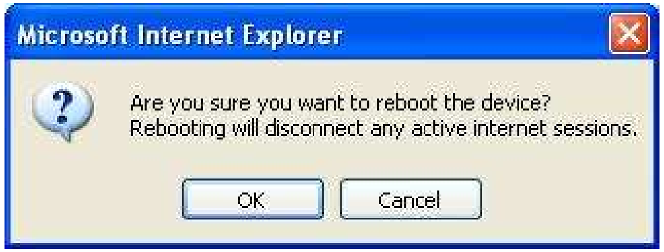
Please wait 14 seconds.

If you changed the IP address of the router you will need to change the IP address in your browser before accessing the configuration Web site again.

Please wait while the system is rebooting.
Note: Do no un-plug the device during this process as this may cause permanent damage.

6.4.2.4. Reboot the device

- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.



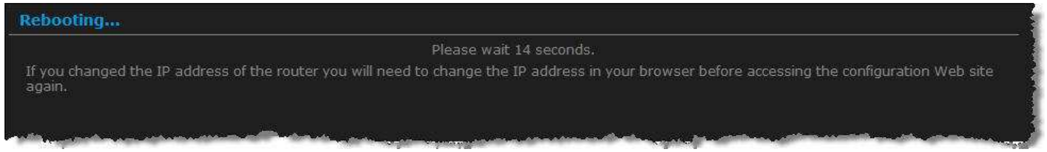
Microsoft Internet Explorer

Are you sure you want to reboot the device?
Rebooting will disconnect any active internet sessions.

- Once the dialog box appears, click on the **OK** button to confirm the action.

Note: The current settings will be lost.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.



Rebooting...

Please wait 14 seconds.

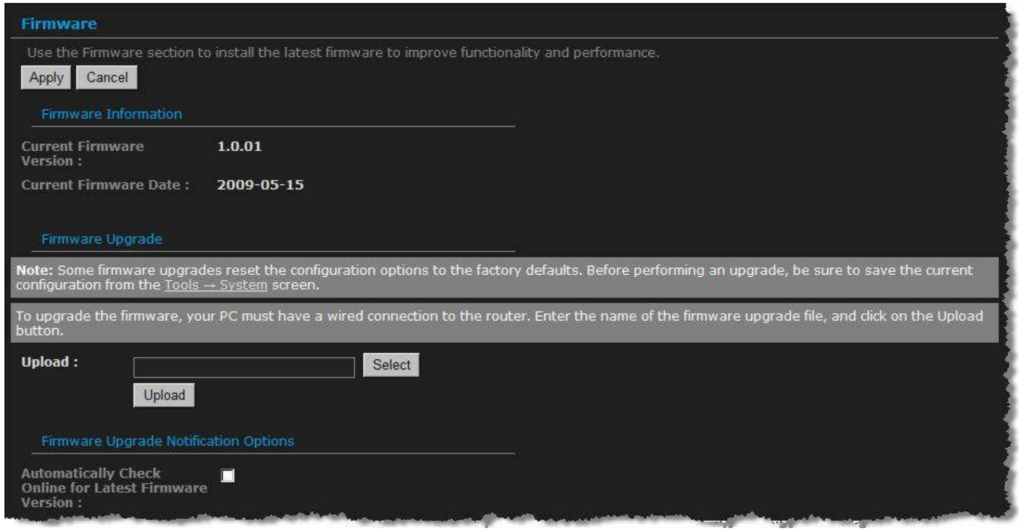
If you changed the IP address of the router you will need to change the IP address in your browser before accessing the configuration Web site again.

Please wait while the system is rebooting.

Note: Do no un-plug the device during this process as this may cause permanent damage.

6.4.3.Firmware Upgrade

- Click on the **Firmware** link in the navigation menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.



Firmware

Use the Firmware section to install the latest firmware to improve functionality and performance.

Firmware Information

Current Firmware Version : 1.0.01

Current Firmware Date : 2009-05-15

Firmware Upgrade

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

Firmware Upgrade Notification Options

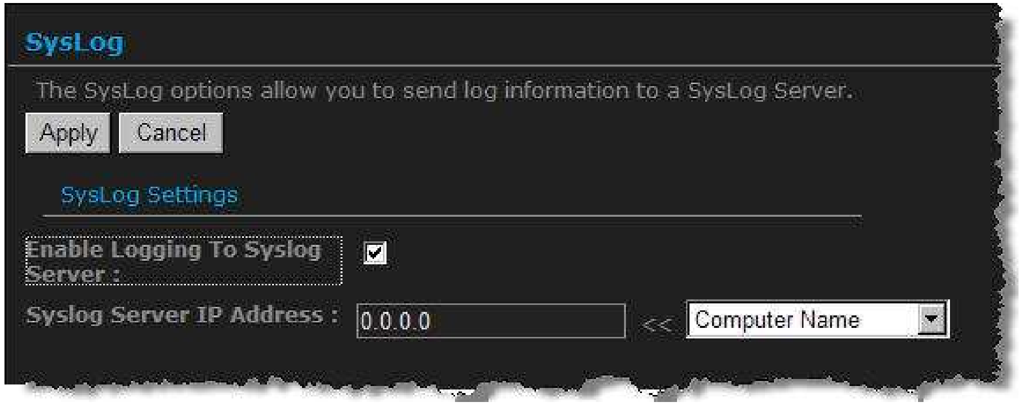
Automatically Check Online for Latest Firmware Version : □

Ensure that you have downloaded the appropriate firmware from the vendor’s website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.

- Click on the **Browse** button to select the firmware and then click on the **Upload** button.

6.4.4.System Logs

Logs display a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes



SysLog

The SysLog options allow you to send log information to a SysLog Server.

SysLog Settings

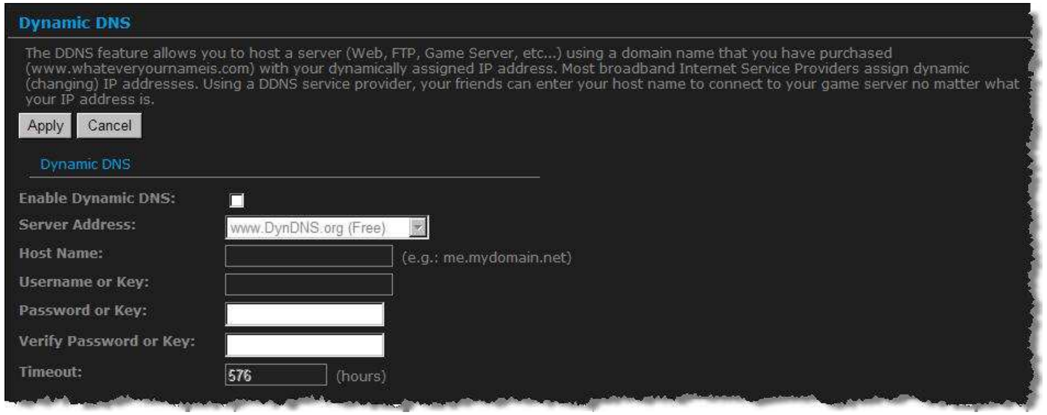
Enable Logging To Syslog Server : ☑

Syslog Server IP Address : 0.0.0.0 << Computer Name

- **Enable Logging to a Syslog Server:** Place a check in this box to enable syslog logging.
- **Syslog Server IP Address:** Specify the IP address of the syslog server.
- Click on the **Apply** button once you have modified the settings.

6.4.5.Dynamic DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your host name to connect to your server, no matter what your IP address is.



Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Dynamic DNS

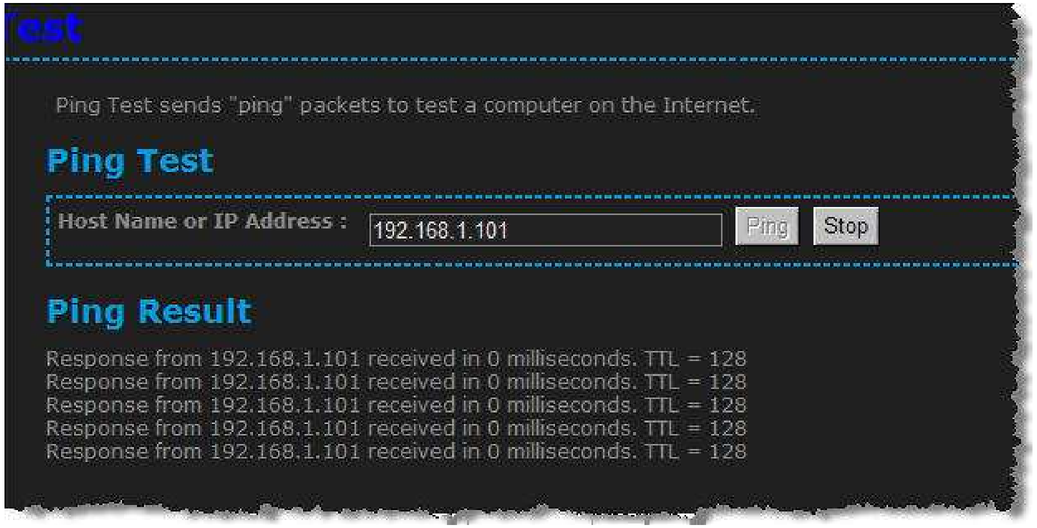
Enable Dynamic DNS: □
Server Address: www.DynDNS.org (Free)
Host Name: (e.g.: me.mydomain.net)
Username or Key:
Password or Key:
Verify Password or Key:
Timeout: 576 (hours)

- **Enable Dynamic DNS**: Place a check in this box to enable the DDNS feature.
- **Service Address**: Select a DDNS service provider from the drop-down list. DynDNS is a free service while TZO offers a 30 day free trial.
- **Host Name**: Specify the website URL.
- **User Name**: Specify the user name for the DDNS service.
- **Password**: Specify the password for the DDNS service and verify it once again in the next field.
- **Timeout**: Specify the time between periodic updates to the Dynamic DNS, if the dynamic IP address has not changed. The timeout period is entered in hours.

Click on the **Apply** button once you have modified the settings.

6.4.6.System Check

Click on the **System Check** link in the navigation menu. This page allows you to ping a host name or IP address.



Ping Test sends "ping" packets to test a computer on the Internet.

Ping Test

Host Name or IP Address : 192.168.1.101

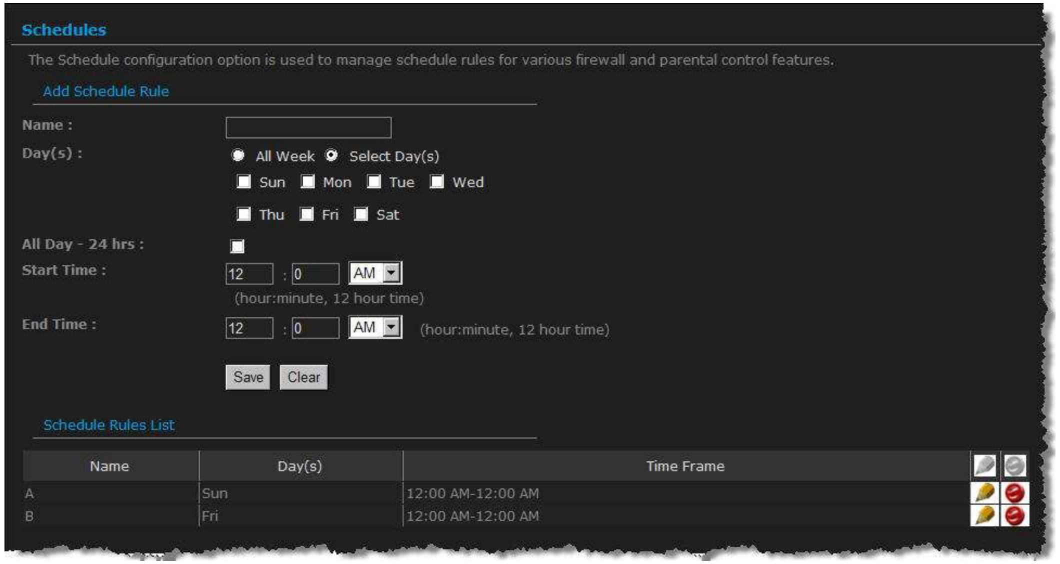
Ping Result

```
Response from 192.168.1.101 received in 0 milliseconds. TTL = 128
Response from 192.168.1.101 received in 0 milliseconds. TTL = 128
Response from 192.168.1.101 received in 0 milliseconds. TTL = 128
Response from 192.168.1.101 received in 0 milliseconds. TTL = 128
Response from 192.168.1.101 received in 0 milliseconds. TTL = 128
```

Host Name or IP address: Specify the host name or IP address and then click on the **Ping** button.

6.4.7.Schedules

Click on the **Schedules** link in the navigation menu. Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.



Schedules

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

Add Schedule Rule

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : 12 : 0 AM (hour:minute, 12 hour time)

End Time : 12 : 0 AM (hour:minute, 12 hour time)

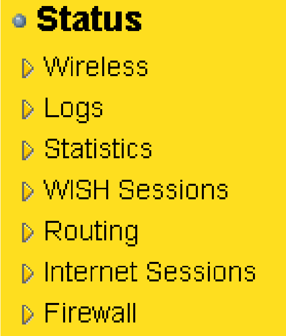
Save Clear

Schedule Rules List

Name	Day(s)	Time Frame
A	Sun	12:00 AM-12:00 AM
B	Fri	12:00 AM-12:00 AM

- **Name**: Specify a name for the schedule.
- **Day(s)**: Select the days at which you would like the schedule to be effective.
- **All Day – 24 hrs**: Place a check in this box if you would like the schedule to be active for 24 hours.
- **Start Time**: If you do not use the 24 hours option, you may specify a start time.
- **End Time**: If you do not use the 24 hours option, you may specify an end time.
- Click on the **Save** button to add this schedule into the list.

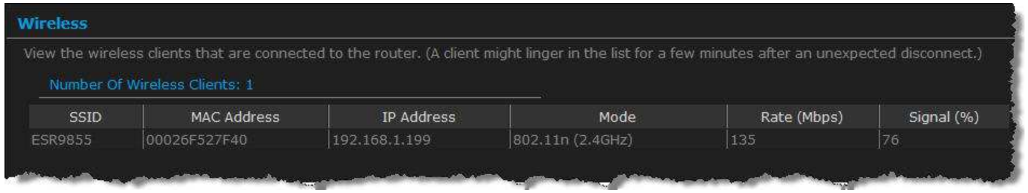
6.5. Status



Click on the **Status** link on the navigation tree menu. You will then see six options: Wireless, Logs, Statistics, WISH Sessions, Routing, and Internet Sessions. The configuration steps for each option are described below.

6.5.1.Wireless Status

Click on the **Wireless** link in the navigation menu. The wireless section allows you to view the wireless clients that are connected to the device.



Wireless

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

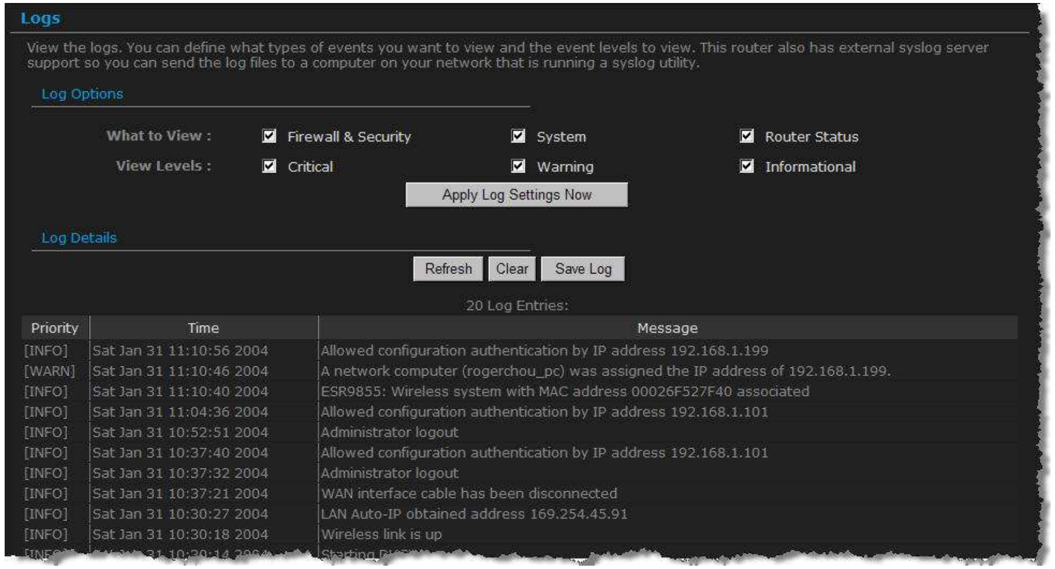
Number Of Wireless Clients: 1

SSID	MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)
ESR9855	00026F527F40	192.168.1.199	802.11n (2.4GHz)	135	76

- **MAC Address**: The Ethernet ID (MAC address) of the wireless client.
- **IP Address**: The LAN-side IP address of the client.
- **Mode**: The transmission standard being used by the client. Values are 11a, 11b, 11g, or 11n for 802.11a, 802.11b, 802.11g, or 802.11n respectively.
- **Rate**: The actual transmission rate of the client in megabits per second.
- **Signal**: This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

6.5.2.Logs Status

Click on the **Logs** link in the navigation menu. The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.



Logs

View the logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

Log Options

What to View : ☑ Firewall & Security ☑ System ☑ Router Status

View Levels : ☑ Critical ☑ Warning ☑ Informational

Log Details

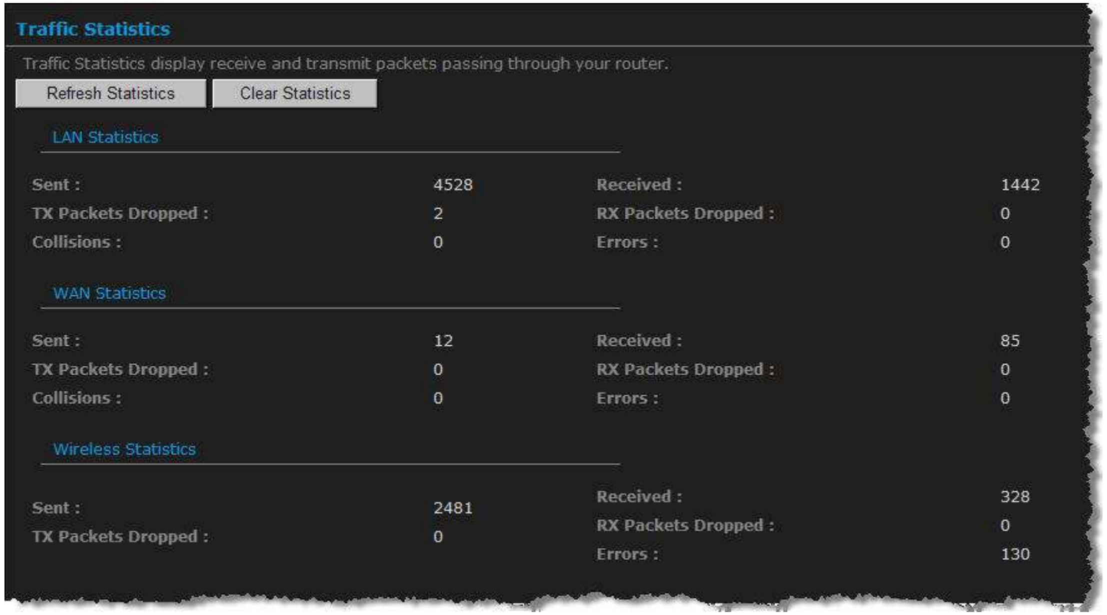
20 Log Entries:

Priority	Time	Message
[INFO]	Sat Jan 31 11:10:56 2004	Allowed configuration authentication by IP address 192.168.1.199
[WARN]	Sat Jan 31 11:10:46 2004	A network computer (rogerchou_pc) was assigned the IP address of 192.168.1.199.
[INFO]	Sat Jan 31 11:10:40 2004	ESR9855: Wireless system with MAC address 00026F527F40 associated
[INFO]	Sat Jan 31 11:04:36 2004	Allowed configuration authentication by IP address 192.168.1.101
[INFO]	Sat Jan 31 10:52:51 2004	Administrator logout
[INFO]	Sat Jan 31 10:37:40 2004	Allowed configuration authentication by IP address 192.168.1.101
[INFO]	Sat Jan 31 10:37:32 2004	Administrator logout
[INFO]	Sat Jan 31 10:37:21 2004	WAN interface cable has been disconnected
[INFO]	Sat Jan 31 10:30:27 2004	LAN Auto-IP obtained address 169.254.45.91
[INFO]	Sat Jan 31 10:30:18 2004	Wireless link is up
[INF	31 10:30:14 2004	Starting D

- **What to View**: Select the features of which you would like to view the logs: Firewall & Security, System, or Router Status.
- **View Levels**: Select the warning levels for the logs: Critical, Warning, or Informational.
- Click on the **Apply Log Settings Now** to make the new log effective.

6.5.3.Statistics

Click on the **Statistics** link in the navigation drop-down menu. This page displays the transmitted and received packet statistics of the wired (LAN & WAN) and wireless interface. Click on the Refresh button to refresh the statistics.



Traffic Statistics

Traffic Statistics display receive and transmit packets passing through your router.

LAN Statistics

Sent :	4528	Received :	1442
TX Packets Dropped :	2	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WAN Statistics

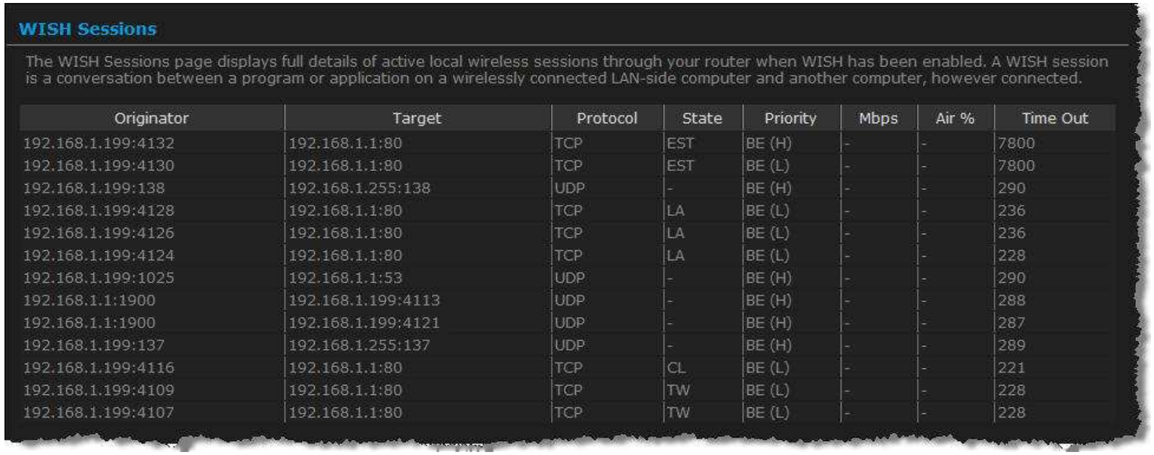
Sent :	12	Received :	85
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

Wireless Statistics

		Received :	328
Sent :	2481	RX Packets Dropped :	0
TX Packets Dropped :	0	Errors :	130

6.5.4.WISH Session Status

Click on the **WISH Sessions** link in the navigation drop-down menu. The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.



WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

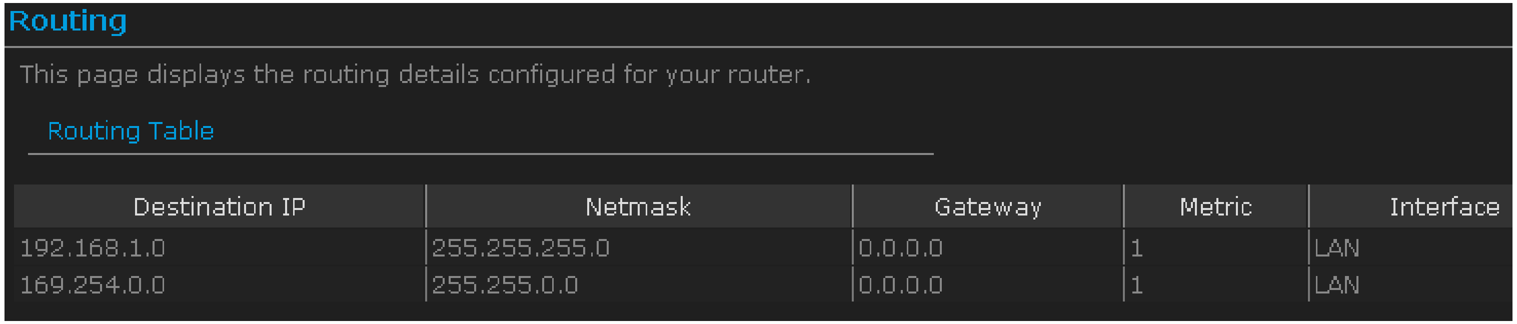
Originator	Target	Protocol	State	Priority	Mbps	Air %	Time Out
192.168.1.199:4132	192.168.1.1:80	TCP	EST	BE (H)	-	-	7800
192.168.1.199:4130	192.168.1.1:80	TCP	EST	BE (L)	-	-	7800
192.168.1.199:138	192.168.1.255:138	UDP	-	BE (H)	-	-	290
192.168.1.199:4128	192.168.1.1:80	TCP	LA	BE (L)	-	-	236
192.168.1.199:4126	192.168.1.1:80	TCP	LA	BE (L)	-	-	236
192.168.1.199:4124	192.168.1.1:80	TCP	LA	BE (L)	-	-	228
192.168.1.199:1025	192.168.1.1:53	UDP	-	BE (H)	-	-	290
192.168.1.1:1900	192.168.1.199:4113	UDP	-	BE (H)	-	-	288
192.168.1.1:1900	192.168.1.199:4121	UDP	-	BE (H)	-	-	287
192.168.1.199:137	192.168.1.255:137	UDP	-	BE (H)	-	-	289
192.168.1.199:4116	192.168.1.1:80	TCP	CL	BE (L)	-	-	221
192.168.1.199:4109	192.168.1.1:80	TCP	TW	BE (L)	-	-	228
192.168.1.199:4107	192.168.1.1:80	TCP	TW	BE (L)	-	-	228

- **Originator**: The IP address and, where appropriate, port number of the computer that originated a network connection.
- **Target**: The IP address and, where appropriate, port number of the computer to which a network connection has been made.
- **Protocol**: The communications protocol used for the conversation.
- **State**: State for sessions that use the TCP protocol.
- **NO**: None -- This entry is used as a placeholder for a future connection that may occur.
- **SS**: SYN Sent -- One of the systems is attempting to start a connection.
- **EST**: Established -- the connection is passing data.
- **FW**: FIN Wait -- The client system has requested that the connection be stopped.
- **CW**: Close Wait -- the server system has requested that the connection be stopped.
- **TW**: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- **LA**: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.

- **CL**: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.
- **Priority**: The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:
- **BK**: Background (least urgent).
- **BE**: Best Effort.
- **VI**: Video.
- **VO**: Voice (most urgent).
- **Time Out**: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.
- **300 seconds** - UDP connections.
- **240 seconds** - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- **7800 seconds** - Established or closing TCP connections.

6.5.5.Routing

This function shows current routing table



Routing

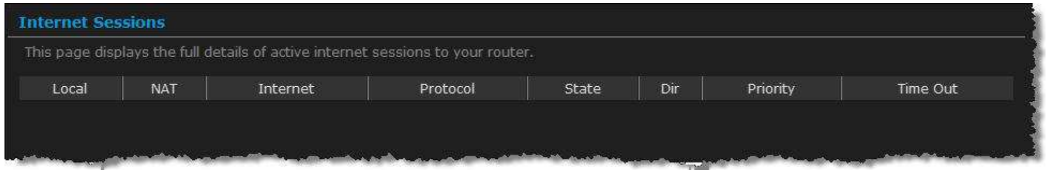
This page displays the routing details configured for your router.

Routing Table

Destination IP	Netmask	Gateway	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	1	LAN
169.254.0.0	255.255.0.0	0.0.0.0	1	LAN

6.5.6.Internet Session Status

Click on the **Internet Sessions** link in the navigation drop-down menu. The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.



Internet Sessions

This page displays the full details of active internet sessions to your router.

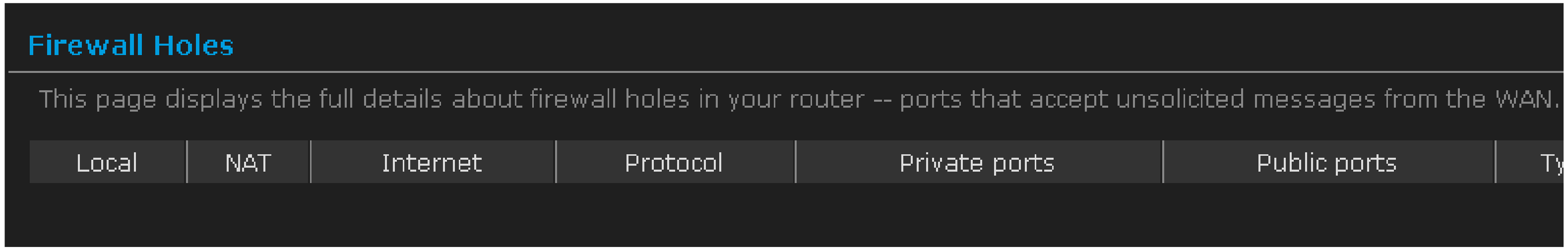
Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out

- **Local**: The IP address and, where appropriate, port number of the local application.
- **NAT**: The port number of the LAN-side application as viewed by the WAN-side application.
- **Internet**: The IP address and, where appropriate, port number of the application on the Internet.
- **Protocol**: The communications protocol used for the conversation.
- **State**: State for sessions that use the TCP protocol.
- **NO**: None -- This entry is used as a placeholder for a future connection that may occur.
- **SS**: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- **FW**: FIN Wait -- The client system has requested that the connection be stopped.
- **CW**: Close Wait -- the server system has requested that the connection be stopped.
- **TW**: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- **LA**: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- **CL**: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.
- **Priority**: The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:
- **BK**: Background (least urgent).
- **BE**: Best Effort.
- **VI**: Video.
- **VO**: Voice (most urgent).
- **Time Out**: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

- **300 seconds** - UDP connections.
- **240 seconds** - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- **7800 seconds** - Established or closing TCP connections.

6.5.7.Firewall

This page displays the full details about firewall holes in your router -- ports that accept unsolicited messages from the WAN.



Firewall Holes

This page displays the full details about firewall holes in your router -- ports that accept unsolicited messages from the WAN.

Local	NAT	Internet	Protocol	Private ports	Public ports	Ty

Appendix A – Glossary

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the sane time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

K

Kbps

Kilobits per second

Kbyte

Kilobyte

L

L2TP

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

M

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W

Wake on LAN

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

Appendix C – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment 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 equipment 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 equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.