

## Firewall

This section is for configuration settings of the Router's firewall function.

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but 3Com recommends that you leave the firewall enabled whenever possible.

**SPI** Stateful Packet Inspection (SPI) - The Intrusion Detection Feature of the Router limits access for incoming traffic at the WAN port.

This feature is called a "stateful" packet inspection, because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

**Figure 55** Firewall Screen

The screenshot displays the Firewall configuration page for a 3Com Cable/DSL Wireless 11n Firewall Router. The page is titled "Firewall" and includes a navigation menu on the left with options like "Welcome", "LAN Settings", "Wireless Settings", "Internet Settings", "Firewall", "Advanced", "VPN", "System Tools", "Status and Logs", and "Support/Feedback". The main content area is divided into several sections:

- Protection Level:** Firewall level is set to "High".
- Alert by e-mail:** Fields for "Your E-mail Address", "SMTP Server Address", "User name", and "Password".
- Connection Policy:** A table of timeout settings:
 

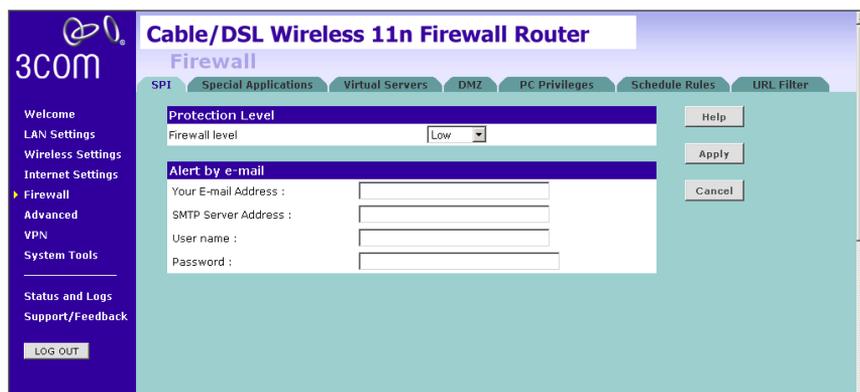
Fragmentation half-open wait :	10	secs
TCP SYN wait :	30	secs
TCP FIN wait :	5	secs
TCP connection idle timeout :	3600	secs
UDP session idle timeout :	30	secs
H.323 data channel idle timeout :	180	secs
- DoS Detect Criteria:** Total incomplete TCP/UDP sessions HIGH is set to 300 session.

Buttons for "Help", "Apply", and "Cancel" are visible on the right side. The status at the bottom is "Status : Ready".

To enable the firewall function:

- 1 Select the level of protection (High, Medium, or Low) that you desire from the *Firewall level* drop-down menu.
- 2 Click *Apply*.
  - For low and medium levels of firewall protection, refer to [Figure 56](#).
  - For high level of firewall protection, refer to [Figure 57](#).

**Figure 56** Low and Medium Level Firewall Protection Screen



When abnormal network activity occurs, an alerting email will be sent out to you. Enter the following information to receive the email:

- Your E-mail Address
- SMTP Server Address
- User name
- Password

**Figure 57** High Level Firewall Protection Screen

**3COM**

Welcome  
LAN Settings  
Wireless Settings  
Internet Settings  
▶ Firewall  
Advanced  
VPN  
System Tools  
Status and Logs  
Support/Feedback  
LOG OUT

**Protection Level**  
Firewall level: High

**Alert by e-mail**  
Your E-mail Address :  
SMTP Server Address :  
User name :  
Password :

**Connection Policy**  
Fragmentation half-open wait : 10 secs  
TCP SYN wait : 30 secs  
TCP FIN wait : 5 secs  
TCP connection idle timeout : 3600 secs  
UDP session idle timeout : 30 secs  
H.323 data channel idle timeout : 180 secs

**DoS Detect Criteria**  
Total incomplete TCP/UDP sessions HIGH : 300 session  
Total incomplete TCP/UDP sessions LOW : 250 session  
Incomplete TCP/UDP sessions (per min) HIGH : 250 session  
Incomplete TCP/UDP sessions (per min) LOW : 200 session  
Maximum incomplete TCP/UDP sessions number from same host : 10 session  
Incomplete TCP/UDP sessions detect sensitive time period : 300 msec

Status : Ready

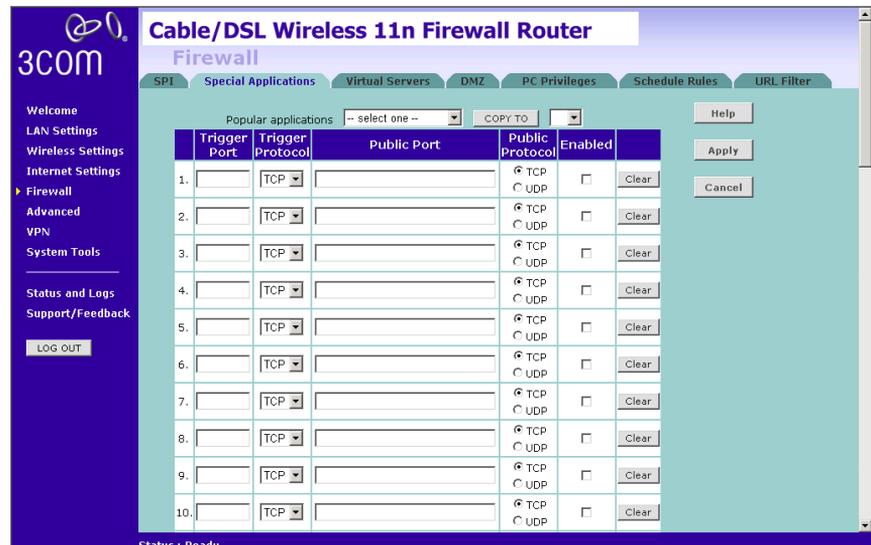
If you select high level of protection, you will need to configure additional parameters for the firewall.

- Fragmentation half-open wait - Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the Router drops the un-assembled packet, freeing that structure for use by another packet.
- TCP SYN wait - Defines how long the software will wait for a TCP session to synchronize before dropping the session.
- TCP FIN wait - Specifies how long a TCP session will be maintained after the firewall detects a FIN packet.
- TCP connection idle timeout - The length of time for which a TCP session will be managed if there is no activity.
- UDP session idle timeout - The length of time for which a UDP session will be managed if there is no activity.
- H.323 data channel idle timeout - The length of time for which an H.323 session will be managed if there is no activity.

- Total incomplete TCP/UDP sessions HIGH - Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
- Total incomplete TCP/UDP sessions LOW - Defines the rate of new unestablished sessions that will cause the software to stop deleting half-open sessions.
- Incomplete TCP/UDP sessions (per min) HIGH - Maximum number of allowed incomplete TCP/UDP sessions per minute.
- Incomplete TCP/UDP sessions (per min) LOW - Minimum number of allowed incomplete TCP/UDP sessions per minute.
- Maximum incomplete TCP/UDP sessions number from same host - Maximum number of incomplete TCP/UDP sessions from the same host.
- Incomplete TCP/UDP sessions detect sensitive time period - Length of time before an incomplete TCP/UDP session is detected as incomplete.
- Maximum half-open fragmentation packet number from same host - Maximum number of half-open fragmentation packets from the same host.
- Half-open fragmentation detect sensitive time period - Length of time before a half-open fragmentation session is detected as half-open.
- Flooding cracker block time - Length of time from detecting a flood attack to blocking the attack.

**Special Applications** Special Applications let you choose specific ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router.

**Figure 58** Special Applications Screen



A list of popular applications has been included to choose from. Select the application from the *Popular Applications* drop-down menu. Then select the row that you want to copy the settings to from the *Copy To* drop-down menu, and click *Copy To*. The settings will be transferred to the row that you specified. Click *Apply* to save the setting for that application.

If your application is not listed, you will need to check with the application vendor to determine which ports need to be configured. You can manually enter the port information into the Router. To manually enter the port information:

- 1 Specify the trigger port (the one used by the application when it is initialized) in the *Trigger Port* column, and specify whether the trigger is TCP or UDP.
- 2 Specify the Public Ports used by the application, that will need to be opened up in the firewall for the application to work properly. Also specify whether these ports are TCP or UDP.
- 3 Check the *Enabled* checkbox, then click *Apply*.

**Virtual Servers** The Virtual servers feature allows you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be 'seen'.

If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

The maximum number of virtual servers that can be configured is 20.

**Figure 59** Virtual Servers Screen

The screenshot shows the 'Virtual Servers' configuration page of a 3COM Cable/DSL Wireless 11n Firewall Router. The page has a navigation menu on the left and a main configuration area. The main area contains a table for adding virtual servers. At the top of the table, there is a 'Popular servers' drop-down menu and a 'COPY TO' button. The table has the following columns: LAN IP Address, Description, Protocol Type, LAN Port, Public Port, and Enabled. There are 11 rows in the table, each with a 'Clear' button. The 'Enabled' column has checkboxes, all of which are currently unchecked. The 'Apply' and 'Cancel' buttons are located to the right of the table.

	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enabled	
1	192.168.1.		TCP			<input type="checkbox"/>	Clear
2	192.168.1.		TCP			<input type="checkbox"/>	Clear
3	192.168.1.		TCP			<input type="checkbox"/>	Clear
4	192.168.1.		TCP			<input type="checkbox"/>	Clear
5	192.168.1.		TCP			<input type="checkbox"/>	Clear
6	192.168.1.		TCP			<input type="checkbox"/>	Clear
7	192.168.1.		TCP			<input type="checkbox"/>	Clear
8	192.168.1.		TCP			<input type="checkbox"/>	Clear
9	192.168.1.		TCP			<input type="checkbox"/>	Clear
10	192.168.1.		TCP			<input type="checkbox"/>	Clear
11	192.168.1.		TCP			<input type="checkbox"/>	Clear

A list of popular servers has been included to choose from. Select the server from the *Popular servers* drop-down menu. Then click *Add*, your selection will be added to the table.

If the server that you want to use is not listed in the drop-down menu, you can manually add the virtual server to the table. To manually configure your virtual servers:

- 1 Enter the IP address, and the description in the spaces provided for the internal machine.
- 2 Select the protocol type (TCP, UDP, or both TCP and UDP) from the drop-down menu.

- 3 Specify the public port that will be seen by clients on the Internet, and the LAN port which the traffic will be routed to.
- 4 You can enable or disable each Virtual Server entry by checking or unchecking the appropriate *Enabled* checkbox.
- 5 Click *Apply* to save the changes for each Virtual Server entry.

**DMZ** If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application.

**Figure 60** DMZ Screen



Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

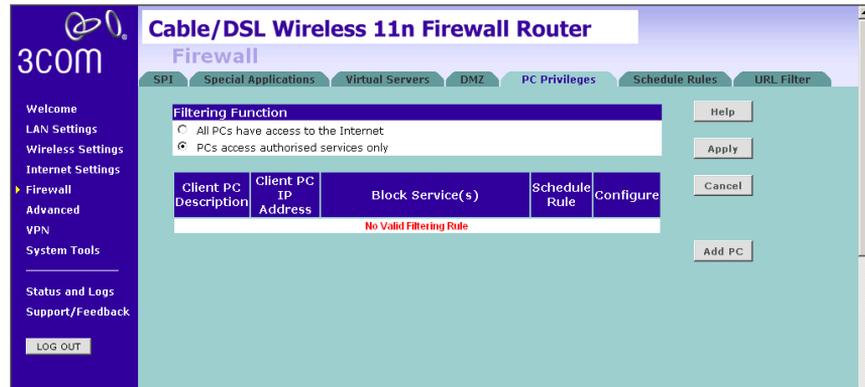
Check the *Enable DMZ* box, the IP Address of Virtual DMZ Host will appear.

- 1 Enter the last digits of the LAN IP address in the *Client PC IP Address* field. Enter the IP address (if known) that will be accessing the DMZ PC into the *Public IP Address* field, so that only the computer on the Internet at this address can access the DMZ PC without firewall protection. If the IP address is not known, or if more than one PC on the Internet will need to access the DMZ PC, then set the *Public IP Address* to *0.0.0.0*.
- 2 Click *Apply*.

**PC Privileges** The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

You can define the traffic type permitted or not-permitted to the Internet.

**Figure 61** PC Privileges Screen



- 1 Select one option from filtering function:
  - All PCs have access to the Internet: selecting this mode means that all clients have full access to Internet.
  - PCs access authorised services only:
- 2 Click *Add PC* (refer to [Figure 62](#)).

To edit or delete specific existing filtering rules, click on *Edit* or *Delete* for the appropriate filtering rule.

Figure 62 PC Privileges Add PC Screen

**Restricted Client PC**

Client PC Description

Client PC IP Address 192.168.1.  ~

Service Name	Detail Description	Bypass
Bypass URL Filter	HTTP (Ref. URL Filter Page)	<input type="checkbox"/>

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>

- 1 Enter a description in the *Client PC Description* field, and the IP address or IP address range into the *Client PC IP Address* fields.
- 2 To bypass the URL Filter and Content Filter, check the corresponding *Bypass* checkbox.

If you check the two options: *Bypass URL Filter*, and *Bypass Content Filter*, then the Web sites and keywords defined in this screen will not be filtered out.

- 3 Select the services to be blocked. A list of popular services is listed on this screen, to block a particular service, check the appropriate *Blocking* checkbox.

If the service to be restricted is not listed here, you can enter a custom range of ports at the bottom of the screen, under *User Defined Blocked Ports*.

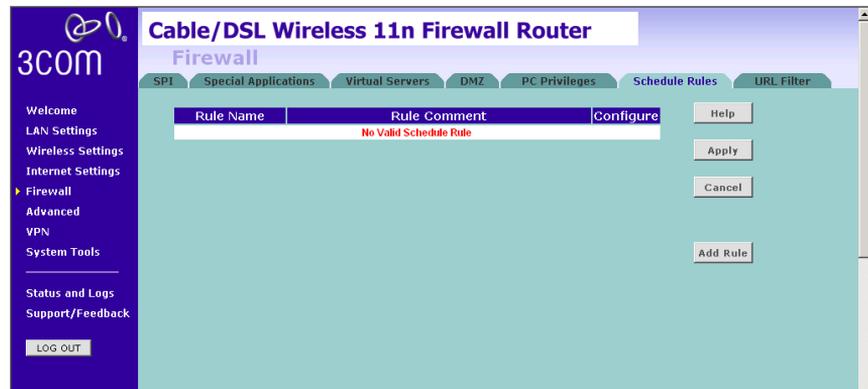
- 4 If you want the restriction to apply only at certain times, select the schedule rule to apply from the *Schedule Rule* drop-down menu.

Note that schedule rules are defined on the Schedule Rules screen (see [page 78](#)).

- 5 Click *Apply* to add the settings.

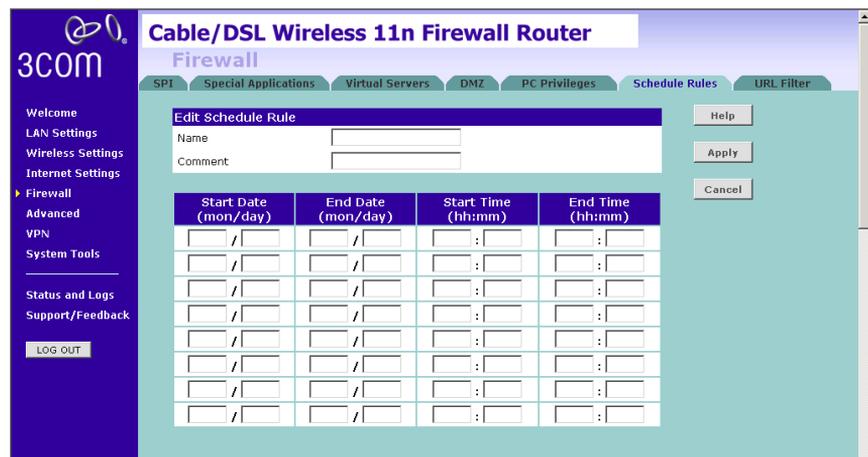
**Schedule Rule** The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Define the time in this screen, and define the rules in the *PC Privileges* screen (see [page 76](#)).

**Figure 63** Schedule Rule Screen



- 1 Click *Add Rule* to add a schedule rule (refer to [Figure 64](#)).

**Figure 64** Add Schedule Rule Screen



- 2 Enter a name and comment for the schedule rule in the *Name* and *Comment* fields.
- 3 Specify the schedule rules for the required days and times - note that all times should be in 24 hour format.
- 4 Click *Apply*.

**URL Filter** To configure the URL filter feature, use the table on the URL Filter screen to specify the Web sites (www.somesite.com) and/or keywords you want to filter on your network.

For example, entering a keyword of **xxx** would block access to any URL that contains the string **xxx**.

**Figure 65** URL Filter Screen

The screenshot shows the 'URL Filtering Function' configuration page. At the top, there's a header for 'OfficeConnect ADSL Wireless 11g Firewall Router' with a 'Firewall' sub-header. Below the header are several tabs: SPI, Special Applications, Virtual Servers, DMZ, Schedule Rules, PC Privileges, URL Filter, Content Filter, and Server Control. The 'URL Filter' tab is active. The main content area is titled 'URL Filtering Function' and contains a checkbox labeled 'Enable URL Filtering Function' which is checked. Below the checkbox is a table with 12 rows. The table has three columns: 'Rule Number', 'URL / Keyword', and 'Mode'. The 'Rule Number' column contains numbers 1 through 12. The 'URL / Keyword' column contains empty text input fields. The 'Mode' column contains dropdown menus, all of which are currently set to 'Denied'. To the right of the table are four buttons: 'Help', 'Apply', 'Cancel', and 'Clear All'. On the left side of the screen is a dark blue sidebar with the '3COM' logo and a list of navigation options: Welcome, LAN Settings, Wireless Settings, Internet Settings, Firewall (highlighted), QoS, Advanced, System Tools, Status and Logs, and Support/Feedback. At the bottom of the sidebar is a 'LOG OUT' button.

Rule Number	URL / Keyword	Mode
1		Denied
2		Denied
3		Denied
4		Denied
5		Denied
6		Denied
7		Denied
8		Denied
9		Denied
10		Denied
11		Denied
12		Denied

- 1 Check the *Enable URL Filtering Function* checkbox. The rule table will appear.
- 2 Enter the URL address or keywords in the *URL/Keyword* field.
- 3 Select *Denied* or *Allowed* from the *Mode* drop-down menu.

To complete this configuration, you will need to create or modify the filtering rule in the PC Privileges screen (see [page 76](#)).

From the *PC Privileges Add PC* screen ([Figure 62](#)), if you check the two options: *Bypass URL Filter*, and *Bypass Content Filter*, then the Web sites and keywords defined in this screen will not be filtered out.

## Advanced

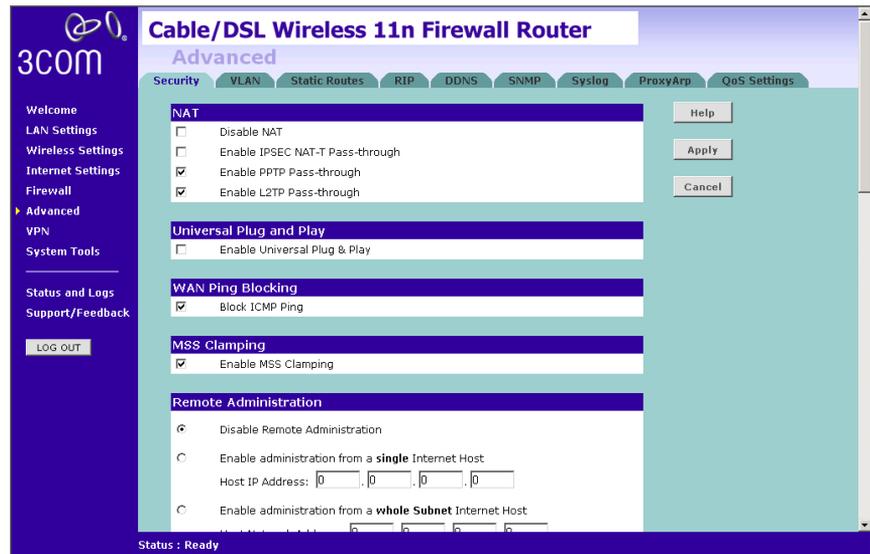
The Advanced section allows you to set additional parameter details for the Router. You can configure:

- Security
- VLAN
- Static Routes
- RIP
- DDNS
- SNMP
- Syslog
- Proxy Arp
- QoS Settings

## Security

Use the Security screen to set the advanced security settings for the Router.

**Figure 66** Security Screen



- **NAT** — Before you enable NAT (Network Address Translation), make sure you have changed the administrator password. NAT is the method by which the Router shares the single IP address assigned by your ISP with the computers on your network.

This function should only be disabled by advanced users, and if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur.

- **IPSEC NAT-T Pass-through** — NAT-T (NAT Traversal) is an Internet Draft proposed to IETF in order to help the problems associated with passing IPsec traffic through NAT Routers. For NAT-T to work, both ends of the connection need to support this function. Ensure that you select NAT-T only if it is needed as it will reduce LAN-WAN throughput. This Router supports NAT-T draft 2 implementation.
- **Universal Plug and Play** — This is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are Universal Plug and Play compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is Universal Plug and Play compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the Universal Plug and Play feature disabled. If you are using any applications that are Universal Plug and Play compliant, and want to take advantage of the Universal Plug and Play features, you can enable this feature. Simply check the *Enable Universal Plug and Play* checkbox. Click *Apply* to save the change.
- **WAN Ping Blocking** — Computer hackers use what is known as "Pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an Internet Control Message Protocol (ICMP) Ping from the outside. This heightens the level of security of your Router. To turn off the ping response, check *Block ICMP Ping* and click *Apply*; the Router will not respond to an ICMP ping from the Internet.

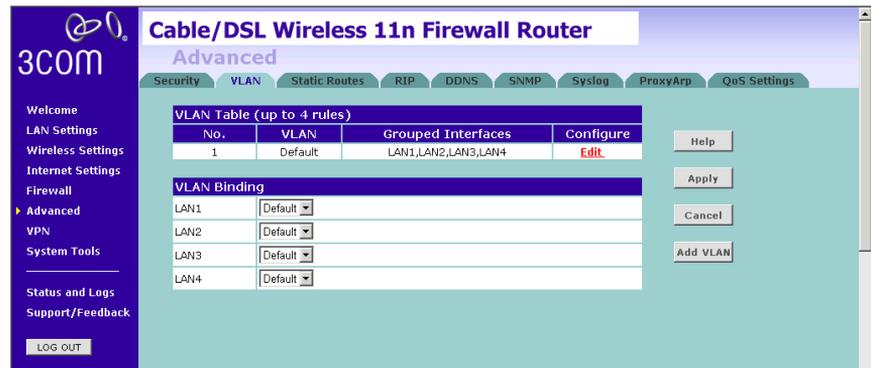
- **MSS Clamping** — You might not be able to browse some Web sites or to send email messages that contain attachments from an Internet Connection Sharing client computer if your outbound connection is through a Windows XP-based Internet Connection Sharing host computer that uses Point-to-Point Protocol over Ethernet (PPPoE). This issue may occur if the Windows XP-based Internet Connection Sharing host computer uses a smaller Maximum Transmission Unit (MTU) size on the WAN interface (the PPPoE connection to the Internet) than it uses on the private interface (the Ethernet connection to the Internet Connection Sharing client). If a packet is larger than the MTU size on the WAN interface, the client sends an Internet Control Message Protocol (ICMP) error to the external server to request that the server negotiate the TCP Maximum Segment Size (MSS). However, this message may be blocked by some firewalls. When this occurs, the packet is dropped. To allow the message to go through the firewall, enable MSS Clamping. MSS clamping will make Internet Connection Sharing set the MSS value low enough to match the external interface.
- **Remote Administration** — This feature allows you to make changes to your Router's settings from anywhere on the Internet. Four options are available:
  - If you do not want to use this feature, select *Disable Remote Administration*.
  - Select *Enable administration from a single Internet Host*, and enter the IP address, to allow only one computer to use the remote administration. This is more secure, as only the specified IP address will be able to manage the Router.
  - Select *Enable administration from a whole Subnet Internet Host*, and enter the IP address and subnet mask, to allow PCs from that specific subnet group to use the remote administration.
  - Select *Enable administration from any Internet Host*, this allows any computer to access the Router remotely.



*Before you enable this function, ensure that you have set the Administration Password.*

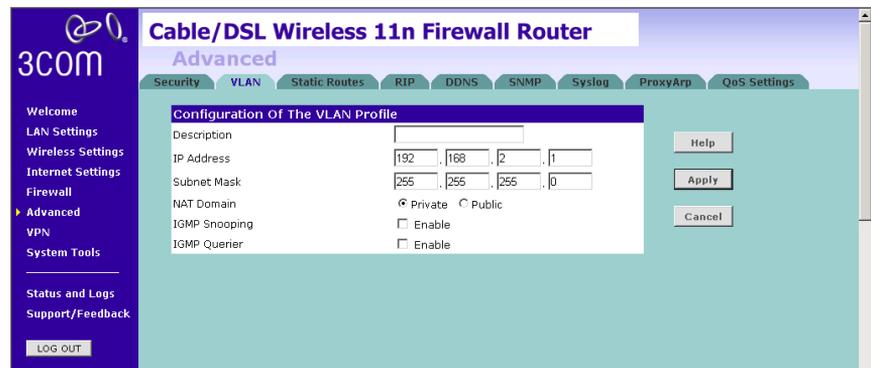
**VLAN** The VLAN screen allows you to setup VLAN groups.

**Figure 67** VLAN Screen



Click *Add VLAN* to create a new entry (see [Figure 68](#)).

**Figure 68** VLAN Profile Screen

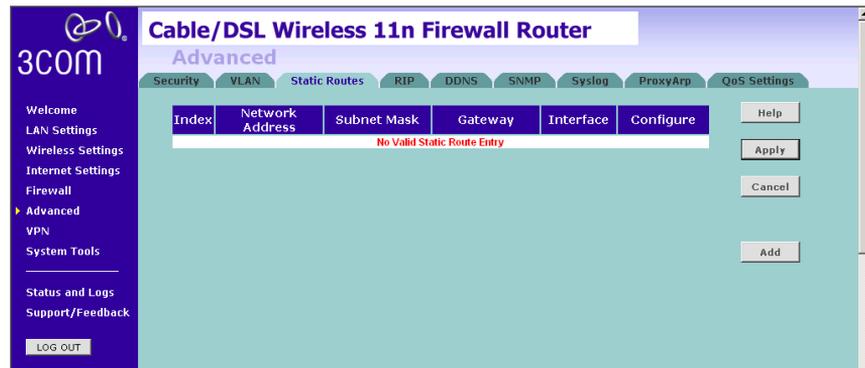


- Enter a description for your VLAN in the *Description* field.
- Enter the IP Address and subnet mask in the corresponding fields.
- Select to set the *NAT Domain* as public or private.
- IGMP Snooping: enabling it will turn on the feature that allows an Ethernet switch to “listen in” on the IGMP conversation between hosts and routers.
- IGMP Querier: enabling this function will send out periodic IGMP queries.

Click *Apply*.

**Static Routes** You can configure static routes in this screen.

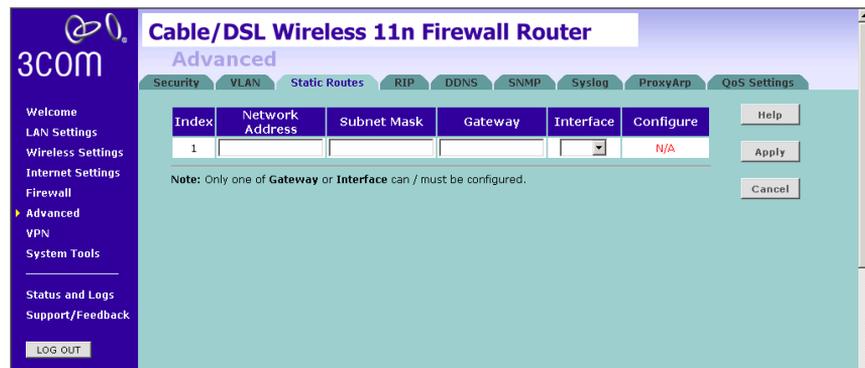
**Figure 69** Static Routes Screen



To add a static route entry to the table, click *Add* (see [Figure 70](#)).

To change an existing entry, click *Edit*. To delete an entry, click *Delete*.

**Figure 70** Add Static Route Screen



Enter the following information:

- *Network Address* — the network address of the static route.
- *Subnet Mask* — the subnet mask of the route.



*A network address of 0.0.0.0 and a subnet mask of 0.0.0.0 indicates the default route.*

- *Gateway* — the router used to route data to the network specified by the network address.

- Interface — select the interface.

After you have finished making changes to the table, click *Apply*.

**RIP** RIP (Routing Information Protocol) - RIP allows the network administrator to set up routing information on one RIP-enabled device and send that information to all RIP-enabled devices on the network.

**Figure 71** RIP Parameter Screen

The screenshot shows the configuration page for the RIP parameter on a 3COM router. The page title is 'Cable/DSL Wireless 11n Firewall Router' and the sub-section is 'Advanced'. The navigation tabs include Security, VLAN, Static Routes, RIP, DDNS, SNMP, Syslog, ProxyArp, and QoS Settings. The left sidebar contains various configuration options like Welcome, LAN Settings, Wireless Settings, Internet Settings, Firewall, Advanced (selected), VPN, System Tools, Status and Logs, and Support/Feedback. The main content area is titled 'General RIP parameter' and contains two checked checkboxes: 'Enable RIP' and 'Enable Auto summary'. Below this is a table titled 'Table of current interface RIP parameter' with the following data:

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Password
LAN1	Disable	1	Disable	None	
WLAN	Disable	1	Disable	None	
WAN	Disable	1	Disable	None	

You can set up RIP independently on both LAN and WAN interfaces.

- 1 Check the *Enable RIP* checkbox.
- 2 Check the *Enable Auto summary* checkbox. Auto summarization sends simplified routing data to other RIP-enabled devices rather than full routing data.
- 3 Select the *Operation Mode*:
  - *Disable* — RIP is not enabled for the WAN or LAN interface.
  - *Enable* — RIP is enabled for the WAN or LAN interface. The router will transmit RIP update information to other RIP-enabled devices.
  - *Silent* — RIP is enabled, however the Router only receives RIP update messages, it will not transmit any messages itself.
- 4 In the *Version* field, select 1 or 2.



*3Com recommends that you only use RIPv1 if there is an existing RIP-enabled device on your network that does not support RIPv2. In all other cases, you should use RIPv2.*

- 5 Use the *Poison Reverse* drop-down menu to enable or disable *Poison Reverse* on the Router. Enabling *Poison Reverse* on your Router allows it to indicate to other RIP-enabled devices that they have both routes that point to each other, preventing data loops.
- 6 Use the *Authentication Required* field to choose the mode of authentication:
  - *None* — Switches off authentication on the specified interface.
  - *Password* — An unencrypted text password that needs to be set on all RIP-enabled devices connected to this Router. RIP information is not shared between devices whose passwords do not match.
- 7 In the *Password* field, enter the required password.
- 8 Click *Apply*.

**DDNS** The Router provides a list of dynamic DNS providers for you to choose from. Dynamic Domain Name Server (DDNS) enables you to map a static domain name to a dynamic IP address.

Before you set up DDNS, you must obtain an account, password or key and static domain name from your DDNS provider.

The Router supports five DDNS providers:

- DynDNS.org
- TZO.com
- Dt DNS.com
- No-IP.com
- Zoneedit.com

**Figure 72** Dynamic Domain Name Server (DDNS) Screen

The screenshot shows the web interface of a 3COM Cable/DSL Wireless 11n Firewall Router. The main title is 'Cable/DSL Wireless 11n Firewall Router' with 'Advanced' below it. A navigation bar includes 'Security', 'VLAN', 'Static Routes', 'RIP', 'DDNS', 'SNMP', 'Syslog', 'ProxyApp', and 'QoS Settings'. The 'DDNS' tab is active. On the left is a sidebar with 'Welcome', 'LAN Settings', 'Wireless Settings', 'Internet Settings', 'Firewall', 'Advanced' (selected), 'VPN', 'System Tools', 'Status and Logs', and 'Support/Feedback'. A 'LOG OUT' button is at the bottom of the sidebar. The main content area is titled 'DDNS Configuration' and contains a 'Help' button, a checked 'Enable DDNS' checkbox, a 'Provider' dropdown menu (set to 'DynDNS.org'), and three text input fields for 'Domain Name', 'Account', and 'Password'. 'Apply' and 'Cancel' buttons are on the right.

- 1 Check *Enable DDNS*.
- 2 Select the provider, and then enter the necessary information provided by your DDNS provider.
- 3 Click *Apply*.

**SNMP** SNMP (Simple Network Management Protocol) allows remote management of your Router by a PC that has an SNMP management agent installed.

Check the *Enable SNMP* box, the table will appear.

**Figure 73** SNMP Screen

**Cable/DSL Wireless 11n Firewall Router**  
Advanced

Security VLAN Static Routes RIP DDNS **SNMP** Syslog ProxyArp QoS Settings

**SNMP Configuration**

Enable SNMP

Please enter the SNMP Community parameters in the following table.

No.	Community	Access	Valid
1	public	Read	<input checked="" type="checkbox"/>
2	private	Write	<input checked="" type="checkbox"/>
3		Read	<input type="checkbox"/>
4		Read	<input type="checkbox"/>
5		Read	<input type="checkbox"/>

Please enter the SNMP Trap parameters in the following table.

No.	IP Address	Community	Version
1	0 . 0 . 0 . 0		Disabled
2	0 . 0 . 0 . 0		Disabled
3	0 . 0 . 0 . 0		Disabled
4	0 . 0 . 0 . 0		Disabled
5	0 . 0 . 0 . 0		Disabled

Help  
Apply  
Cancel

Status : Ready

To Configure SNMP Community:

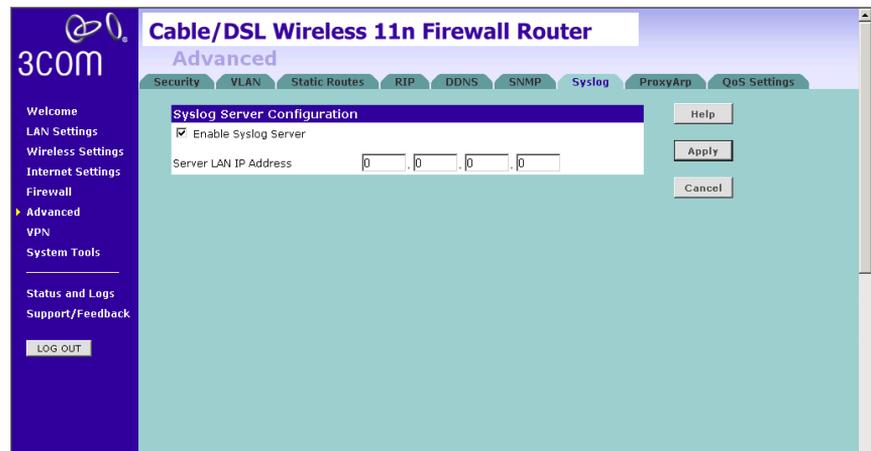
- 1 In the *Community* column, enter the name of the SNMP communication channel. Your SNMP management agent needs to be configured with this name so that it can communicate with your Router.
- 2 In the *Access* column, select *Read* to allow the management agent to collect data (for example, bandwidth usage) from your Router. Select *Write* to allow the management agent to change the configuration of your Router.
- 3 Check the appropriate *Valid* checkbox to enable the communication channel.

You can configure your Router to send status messages to the SNMP management agent if a problem occurs on the network. To configure SNMP traps:

- 1 In the *IP Address* field, enter the IP address of the PC to which you want your Router to send status messages.
- 2 In the *Community* field, enter the name of the SNMP communication channel to which you want your Router to send status messages.
- 3 Set the *Version* field to match the version of trap messaging that your SNMP management agent supports. The Router supports V1 and V2c trap messaging.

**Syslog** Using third party syslog software, this Syslog Server tool will automatically download the Router log to the specified server IP address.

**Figure 74** Syslog Server Screen



- 1 Check the *Enable Syslog Server* checkbox.
- 2 Enter the *Server LAN IP Address* in the space provided.
- 3 Click *Apply*.

**Proxy ARP** Proxy ARP is the technique in which one host, usually a Router, answers ARP requests intended for another machine. By “faking” its identity, the Router accepts responsibility for routing packets to the “real” or intended destination. This heightens the security for your network.

**Figure 75** Proxy ARP Screen

The screenshot shows the configuration page for Proxy ARP on a 3COM router. The interface includes a sidebar with navigation options like 'Welcome', 'LAN Settings', 'Wireless Settings', 'Internet Settings', 'Firewall', 'Advanced', 'VPN', 'System Tools', 'Status and Logs', and 'Support/Feedback'. The main content area is titled 'Cable/DSL Wireless 11n Firewall Router' and 'Advanced'. It features a 'Proxy ARP' tab and a section for 'Enable ProxyARP' with a checked checkbox and a 'Help' button. Below this is a table for 'IP Ranges of Public Hosts In LAN' with columns for 'IP Address From' and 'IP Address To', and rows numbered 1 through 13. At the bottom, there are 'Apply' and 'Cancel' buttons, and a 'Status: Ready' indicator.

	IP Address From	IP Address To
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

- 1 Check the *Enable ProxyARP* box.
- 2 Enter the corresponding IP address in the *IP Address From* and *IP Address To* fields.
- 3 Click *Apply*.

**QoS Settings** The QoS (Quality of Service) function allows you to differentiate your network traffic and provide it with high-priority forwarding service.

The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. This QoS function allows you to classify traffic of applications and provides them with differentiated services (Diffserv).

**Figure 76** QoS Settings Screen

**QoS Settings**

Enable QoS

WAN Out Bandwidth :  kbps

Name	Description	Priority	Bandwidth Allocation	
			Minimum	Allow More
BE	Best Effort forwarding	Lowest	<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>
AF1x	Assured Forwarding, provides delivery of packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedens.	Low ↑ ↓ High	<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>
AF2x			<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>
AF3x			<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>
AF4x			<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.	Highest	<input type="text" value="0"/> kbps	<input checked="" type="checkbox"/>

Buttons: Help, Apply, Cancel

- 1 Check the *Enable QoS* box.
- 2 Enter the value for *WAN Out Bandwidth*.
- 3 Define the minimum percentage of bandwidth for each type of traffic.
- 4 Check the corresponding box to allow more bandwidth allocation.
- 5 Click *Apply*.

---

**VPN**

The Router has a Virtual Private Network (VPN) feature that provides a secure link between remote users and the corporate network by establishing an authenticated and encrypted tunnel for passing secure data over the Internet. The Router supports three modes of VPN operation:

- IPsec (IP Security) — provides IP network-layer encryption. IPsec can support large encryption networks (such as the Internet) by using digital certificates for device authentication. When setting up an IPsec connection between two devices, make sure that they support the same encryption method.

*Note: Enabling IPsec VPN disables pass-through to IPsec and L2TP over IPsec Virtual Servers on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.*

- PPTP (Point-to-Point Tunneling Protocol) — provides a secure tunnel for remote client access to a PPTP security gateway. It is not as secure as IPsec but is easy to administer. PPTP does not support gateway to gateway connections and is only suitable for connecting remote users. Check that your ISP's routers support this protocol before you use it.

*Note: Enabling the PPTP Server disables PPTP pass-through to a Virtual Server on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.*

- L2TP over IPsec — this is a combination of two protocols. L2TP is used to authenticate a user, and IPsec is used to encrypt data. L2TP over IPsec does not support gateway to gateway connections and is only suitable for connecting remote users. Check that your ISP's routers support this protocol before you use it.

*Note: Enabling L2TP over IPsec disables pass-through to IPsec and L2TP over IPsec Virtual Servers on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.*

Using the VPN Tunnel Configuration screen, you can add new IPsec, L2TP over IPsec and PPTP connections, and to edit existing connections. When adding or editing values on this screen remember that both ends of the connection must contain the same information.

- 1 Check the *Enable IPsec* box.

**Figure 77** VPN Screen

- 2 Enter the *Local ID Name* of your VPN.
- 3 Click *Add* to create a new entry.

**Figure 78** Add New VPN Tunnel Configuration Screen

On the VPN Tunnel Configuration screen,

- 1 Select *IPSec* as the *VPN Tunnel Type*.
- 2 Enter a descriptive name for the tunnel in the *Tunnel Name* field.
- 3 Remote VPN Gateway - select *IP address*, and then enter the IP address in the *IP Address/Host Name* field. If you select *ANY*, then it would be no need to enter the IP address, as any remote server can be used.
- 4 At the *Remote Party ID* drop-down list, select either *IP\_IPV4\_ADDR* or *ID\_USER\_FQDN*. This information must be entered identically on the IPSec software installed on the client's machine.

Note that if you select *IKE Main Mode* from the *Key Management* drop-down menu (see step 00xx), you must enter *IP\_IPV4\_ADDR* here.

- 5 Type a name for the Remote Party ID in the text box area next to the drop-down menu. This must be unique for each connection rule that you create.

Enter the following Remote Secure Group information:

- Remote Party ID - select the ID, and then enter the ID in the corresponding fields.
  - If *ID\_IPV4\_ADDR* is selected, then enter the ID in the *Remote Party ID* field. Enter the IP address and subnet mask in the *Remote Network Address* and *Remote Subnet Mask* fields.
  - If *ID\_USER\_FQDN* is selected, then enter the ID in the *Remote Party ID* field. Enter the IP address and subnet mask in the *Remote Network Address* and *Remote Subnet Mask* fields.

Enter the following Local Secure Group information:

- Local Party ID -
- Network Address
- Subnet Mask

Enter the following Phase I IKE (Internet Key Exchange) parameters:

- Key Management
- SA attribute
- Enter the *Pre-shared Key* in the field.

Enter the following Phase II IPsec Parameters:

- Authentication Algorithm
- Encrypt Algorithm
- Key lifetime
- PFS
- Diffie-Hellman Group
- IKE Keep Alive -

## System Tools

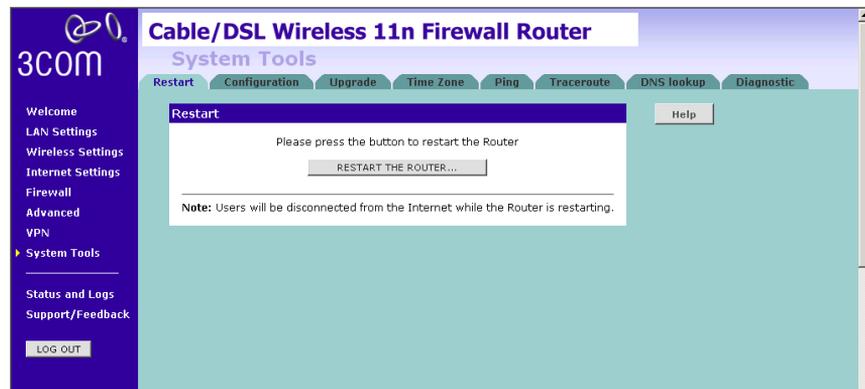
These screens allow you to manage different parameters of the Router and perform certain administrative functions.

### Restart Router

Sometimes it may be necessary to restart (or reboot) the Router. Restarting the Router from this screen will not delete any of your configuration settings.

Click the *Restart the Router* button to restart the Router.

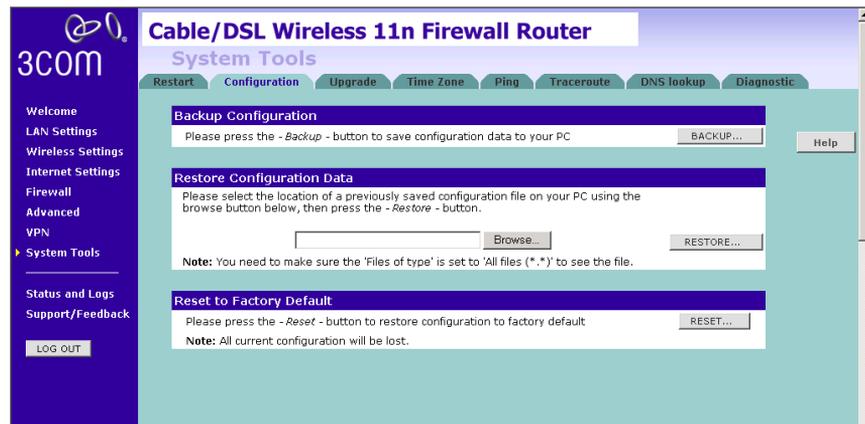
**Figure 79** Restart Router Screen



### Configuration

Use this configuration screen to backup, restore or reset the configuration details of the Router.

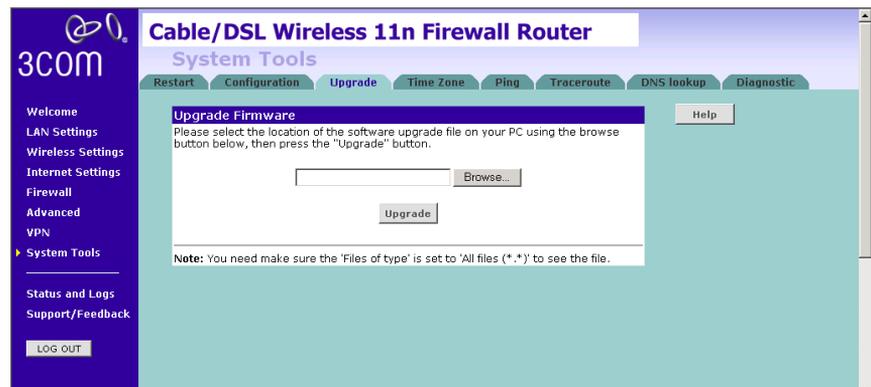
**Figure 80** Configuration Screen



- Backup Configuration — You can save your current configuration by clicking the *Backup* button. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- Restore Configuration Data — The Restore Settings option will allow you to restore a previously saved configuration. Please select the configuration file using the *Browse* button and click *Restore*.
- Reset to Factory Default — Using this option will reset all of the settings in the Router to the factory default settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click *Reset*. Note that all of your current configuration will be lost.

**Upgrade** From time to time 3Com may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

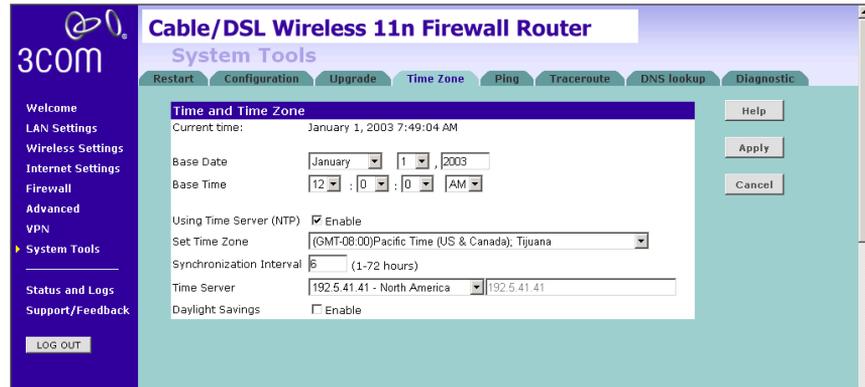
**Figure 81** Upgrade Screen



Please download the firmware file to your PC first, and then click *Browse* to locate the file, and select the firmware file. Click *Upgrade* to upload the firmware to the Router.

**Time Zone** You can set the time settings for the Router on this screen.

**Figure 82** Time Zone Screen



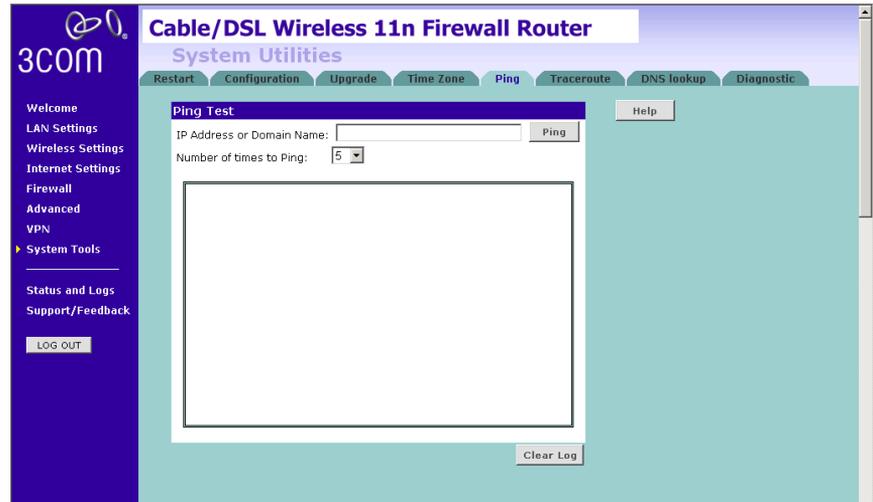
The Router keeps time by connecting to a Network Time Protocol (NTP) server. This allows the Router to synchronize the system clock to the Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in.

If you reside in an area that observes Daylight Saving, then check the *Enable Daylight Savings* box. The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

You can specify which NTP servers the Router will use to update the system clock, although doing this should only be necessary if you are experiencing difficulty.

**Ping** The ping tool is used to test if the network is working properly.

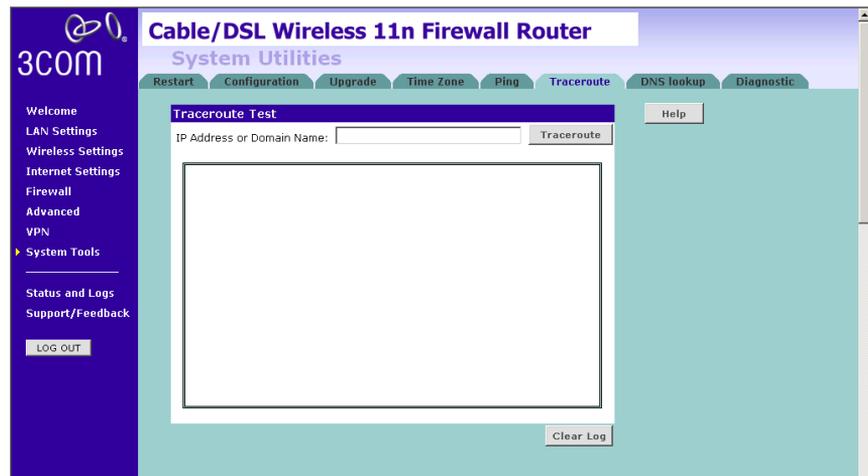
**Figure 83** Ping Screen



- 1 Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Ping*.
- 2 Select from the *Number of times to Ping* drop-down menu.
- 3 The Router keeps a log of the ping test, click *Clear Log* to delete the records.

**Traceroute** Traceroute is the program that shows you the route over the network between two systems, listing all the intermediate routers a connection must pass through to get to its destination. It can help you determine why your connections to a given server might be poor, and can often help you figure out where exactly the problem is. It also shows you how systems are connected to each other, letting you see how your ISP connects to the Internet as well as how the target system is connected.

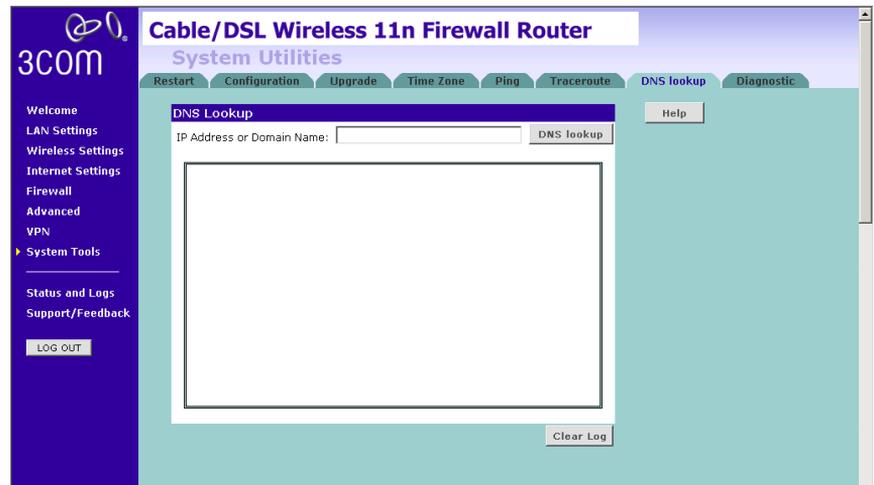
**Figure 84** Traceroute Screen



- 1 Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Traceroute*.
- 2 The Router keeps a log of the traceroute test, click *Clear Log* to delete the records.

**DNS Lookup** DNS Lookup is the process of resolving an IP address (i.e. 192.168.11.137) to a host name (i.e. xxxcompany.net).

**Figure 85** DNS Lookup Screen



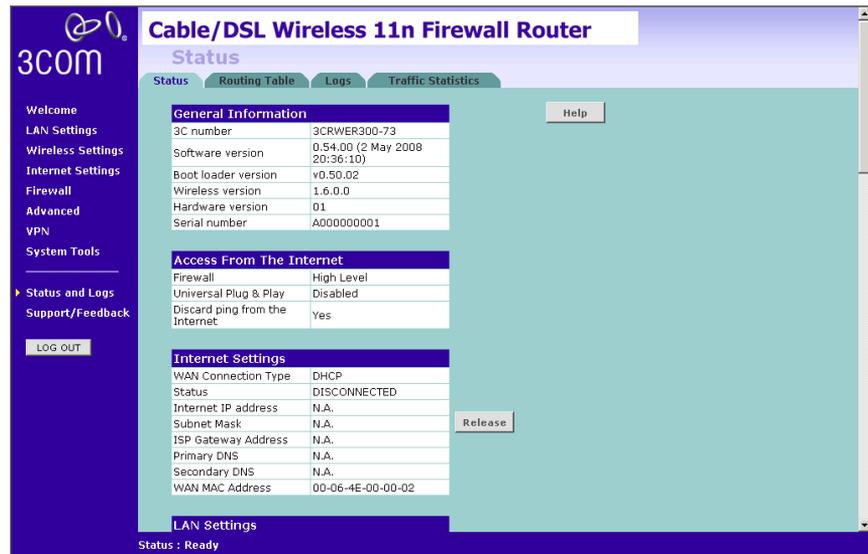
- 1 Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Dns lookup*.
- 2 The Router keeps a log of the DNS lookup test, click *Clear Log* to delete the records.

## Status and Logs

You can use the Status Screen to view version numbers for your Router's software and hardware and check the status of connections to WAN, LAN and WLAN interfaces.

**Status** This screen shows Router status and statistics.

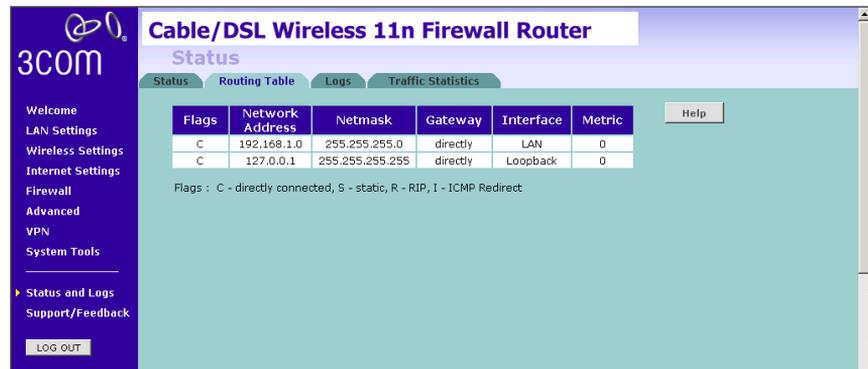
**Figure 86** Status Screen



## Routing Table

This screen displays details for the default routing used by your Router and any routing created using Static Routing or RIP.

**Figure 87** Routing Table Screen



**Logs** This screen shows any attempts that have been made to gain access to your network as well as the system activities.

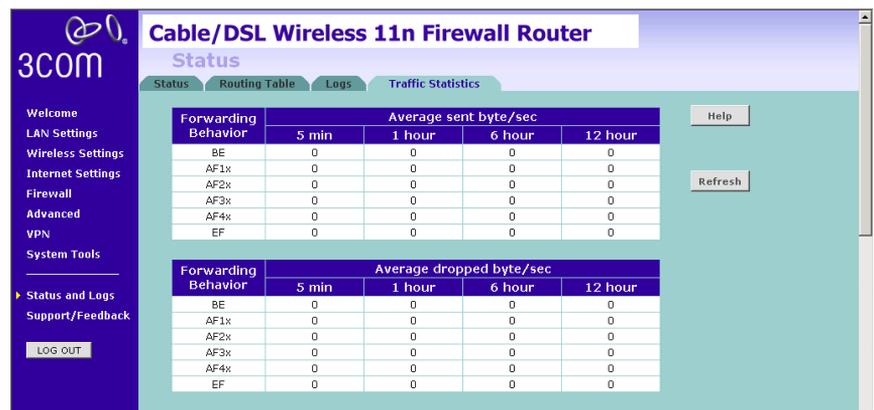
**Figure 88** Logs Screen



- Click *Help* to view the help file.
- Click *Save* to save the log to the hard disk as a text file. When prompted for a location to save the file to, specify a filename and location, and then click *OK*.
- Click *Clear* to clear the log (note that all current entries will be erased).
- Click *Refresh* to update the record.

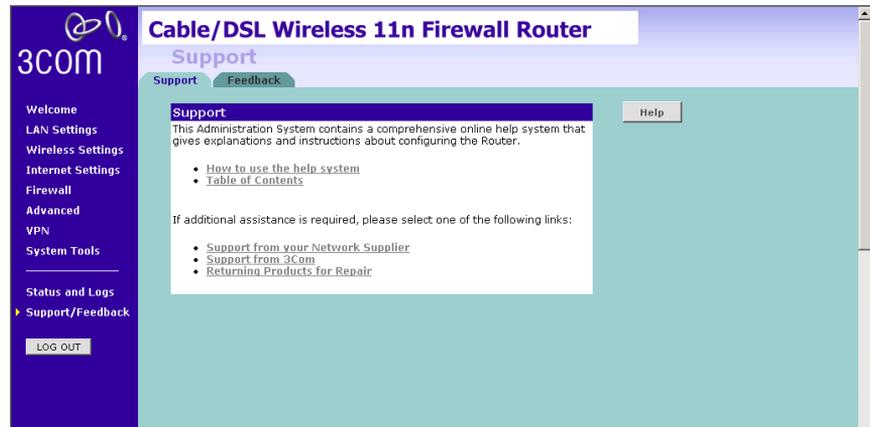
**Traffic Statistics** This screen shows the traffic statistics.

**Figure 89** Traffic Statistics Screen



**Support/Feedback**

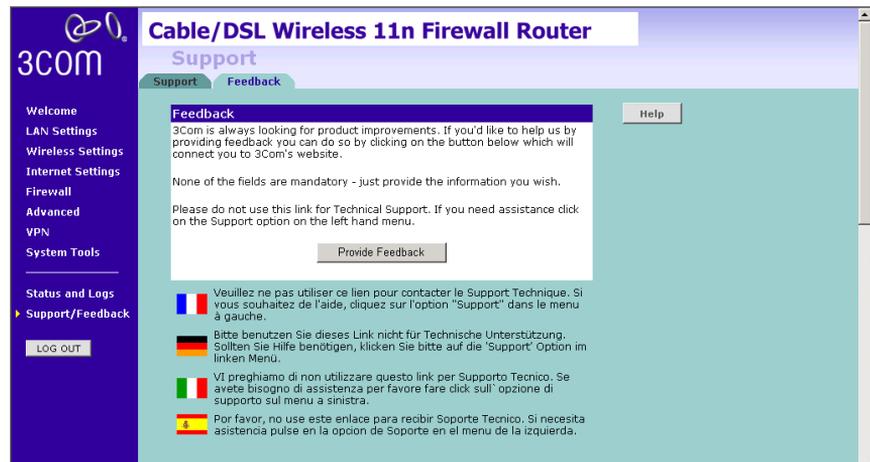
You can use the Support/Feedback screen to obtain support and help, and also provide feedback to 3Com.

**Support** **Figure 90** Support Screen

This screen shows support information.

**Feedback**

To provide feedback to 3Com, please click *Provide Feedback*, and this will connect you to the 3Com Web site.

**Figure 91** Feedback Screen

This screen shows feedback information.

# 6

## TROUBLESHOOTING

---

### Basic Connection Checks

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the LAN Status and SYNC LEDs on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

---

### Browsing to the Router Configuration Screens

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Router and network adapter are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in [Chapter 3](#). Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.
- When entering the address of the Router into your web browser, ensure that you use the full URL including the http:// prefix (e.g. **http://192.168.1.1**).
- Ensure that you do not have a Web proxy enabled on your computer. Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click on the *LAN Settings* button at the bottom. Make sure that the *Proxy Server* option is unchecked.

- If you cannot browse to the Router, use the *winiipcfg* utility in Windows 98/ME to verify that your computer has received the correct address information from the Router. From the *Start* menu, choose *Run* and then enter **winiipcfg**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Router). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Router. Under Windows 2000 and Windows XP, use the *ipconfig* command-line utility to perform the same functions.

---

## Connecting to the Internet

If you can browse to the Router configuration screens but cannot access Web sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the telephone line is OK, and that the DSL LED on the Router is illuminated.
- Ensure that you have entered the correct information into the Router configuration screens as required by your Internet Service Provider. Use the Internet Settings screen to verify this.
- Check that the PPPoE or PPPoA user name and password are correct.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel > Internet Options > Connections*.

---

## Forgotten Password and Reset to Factory Defaults

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to its factory default configuration.



**CAUTION:** *All your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.*

- 1 Power off the Router.
- 2 Disconnect all your computers and the telephone line from the Router.
- 3 Re-apply power to the Router, and wait for it to finish booting up.

- 4 Press and hold the *Reset* button on the rear panel (see [Figure 4](#) on [page 16](#)) for 5 seconds.
- 5 The Router will restart, and when the start-up sequence has completed, browse to:  
  
`http://192.168.1.1`  
and run the configuration wizard. You may need to restart your computer before you attempt this.
- 6 When the configuration wizard has completed, you may reconnect your network as it was before.

---

## Wireless Networking

- Ensure that you have an 802.11b or 802.11g or 802.11n wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each wireless computer has either Windows 98 or higher or MAC OS 8.5 or higher.
- Verify that your wireless computers are configured to work in Infrastructure mode and not Ad Hoc mode. The Router contains an Access Point that is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Router.
- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the WLAN LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to [Wireless Settings](#) on [page 47](#) and enable wireless networking.
- Ensure that the TCP/IP settings for all devices are correct.
- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive.
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router cannot simultaneously support WPA and WEP encryption.
- Ensure that you have the wireless computer enabled in the list of allowed MAC addresses if you are using MAC Address Filtering on the Router.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router. For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage.

Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the wireless computer or the Router, or trying a different channel on the Router.

- Sources of interference: The 2.4Ghz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices, like microwave ovens for example, close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.
- Most wireless computer adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your wireless computer adapter documentation and vendor to do this.
- Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network with wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

---

## Recovering from Corrupted Software

If the system software has become corrupted, the Router will enter a “recovery” state; DHCP is enabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Router unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.



*Check your ISP for the latest version firmware.*

- 1 Remove power from the Router and disconnect the telephone line and all your computers, except for the one computer with the software image.
- 2 You will need to reconfigure this computer to obtain an IP address automatically (see [Obtaining an IP Address Automatically](#) on [page 23](#)).
- 3 Restart the computer, and re-apply power to the Router.
- 4 Using the Web browser on the computer, enter the following URL in the location bar:  
**http://192.168.1.1.**  
This will connect you to the Recovery utility in the Router.
- 5 Follow the on-screen instructions. Enter the path and filename of the software image file.
- 6 When the upload has completed, the Router will restart, run the self-test and, if successful, resume normal operation.
- 7 Refer to the Installation Guide to reconnect your Router to the telephone line and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Router does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

---

**Frequently Asked Questions****How do I reset the Router to Factory Defaults?**

See [Forgotten Password and Reset to Factory Defaults](#) on [page 106](#).

**How many computers on the LAN does the Router support?**

A maximum of 253 computers on the LAN are supported.

**How many wireless clients does the Router support?**

A maximum of 128 wireless clients are supported.

**There are only 4 LAN ports on the Router. How are additional computers connected?**

You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. 3Com wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

<http://www.3com.com/>

**Does the Router support virtual private networks (VPNs)?**

The Router supports VPN passthrough, which allows VPN clients on the LAN to communicate with VPN hosts on the Internet. It is also possible to set up VPN hosts on your LAN that clients elsewhere on the Internet can connect to, but this is not a recommended configuration.

# A

## IP ADDRESSING

---

### **The Internet Protocol Suite**

The Internet Protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

---

### **Managing the Router over the Network**

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

### **IP Addresses and Subnet Masks**

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.



*The only value that will be different is the specific host device number. This value must always be unique.*

An example IP address is '192.168.100.8'. However, the size of the network determines the structure of this IP address. In using the Router, you will probably only encounter two types of IP address and subnet mask structures.

### Type One

In a small network, the IP address of '192.168.100.8' is split into two parts:

- Part one ('192.168.100') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP address operates on a subnet mask of '255.255.255.0'.

See [Table 3](#) for an example about how a network with three computers and a Router might be configured.

**Table 3** IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Router	192.168.100.72	255.255.255.0

### Type Two

In larger networks, where there are more devices, the IP address of '192.168.100.8' is, again, split into two parts but is structured differently:

- Part one ('192.168') identifies the network on which the device resides.
- Part two ('.100.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.0.0'.

See [Table 4](#) for an example about how a network (only four computers represented) and a Router might be configured.

**Table 4** IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Router	192.168.002.72	255.255.0.0

## How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

### DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows 98, Windows NT 4.0, Windows 2000, Windows XP, and Windows Vista. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

### Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

### Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves

an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000 and Windows XP.

# B

## TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the 3Com Wireless 11n Cable/DSL Firewall Router.

---

### 3Com Wireless 11n Cable/DSL Firewall Router

#### Interfaces

WAN connection

LAN connection — four 10 Mbps/100 Mbps dual speed Ethernet ports (10BASE-T/100BASE-TX)

#### WLAN Interfaces

IEEE draft 802.11n, Orthogonal Frequency Division Multiplexing (OFDM)  
Transmission rate: 802.11n 40MHz: 270Mbps, automatic fallback to 243, 216, 162, 135, 121.5, 108, 81, 54, 40.5, 27, 13.5Mbps

802.11n 20MHz: 130Mbps, automatic fallback to 117, 104, 78, 65, 58.5, 52, 39, 26, 19.5, 13, 6.5Mbps

Maximum channels: 13

Range up to 304.8m (1000ft)

Sensitivity: 11 Mbps: -82 dBm; 54 Mbps: -68 dBm;

MCS15 (20MHz): -65 dBm ; MCS15 (40MHz): -62 dBm

Modulation: CCK, BPSK, QPSK, OFDM

Encryption: 40/64 bit WEP, 128 bit WEP, WPA/WPA2

Maximum clients: 128

O/P Power: 14dBm

Standard IEEE 802.11g, Direct Sequence Spread Spectrum (DSSS)

Transmission rate: 54 Mbps, automatic fallback to 48, 36, 24, 18, 12, or 6 Mbps

Maximum channels: 13

Range up to 304.8m (1000ft)

Sensitivity: 6, 12, 18, 24, 36, 48 Mbps: -85 dBm;

54 Mbps -66 dBm typical

Modulation: CCK, BPSK, QPSK, OFDM  
Encryption: 40/64 bit WEP, 128 bit WEP, WPA/WPA2  
Maximum clients: 128  
O/P Power: 14dBm

Standard IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)  
Transmission rate: 11Mbps, automatic fallback to 5.5, 2, or 1 Mbps  
Maximum channels: 13  
Range up to 304.8m (1000ft)  
Sensitivity: 1, 2, 5.5 Mbps: -85 dBm; 11 Mbps -82 dBm typical  
Modulation: CCK, BPSK, QPSK  
Encryption: 40/64 bit WEP, 128 bit WEP, WPA/WPA2  
Maximum clients: 128  
O/P Power 18dBm

**Operating Temperature**

0 °C to 40 °C (32 °F to 105 °F)

**Power**

12V1A/15V1A

**Humidity**

0% to 90% (non-condensing) humidity

**Dimensions**

- Width = 178 mm (7.0 in.)
- Depth = 160 mm (6.1 in.)
- Height = 39 mm (1.5 in.)

**Weight**

Approximately 285 g

<b>Standards</b>	Functional:	ISO 8802/3 IEEE 802.3 IEEE 802.11b, 802.11g
	Safety:	EN 60950-1: 2001 UL 60950-1 IEC 60950-1: 2001

EMC: FCC Part15 B  
EN 55022  
EN 55024  
EN 61000  
EN 301 489-1  
ICES-003

Radio FCC Part 15 C  
RSS-210  
EN 300 328

Environmental: EN 60068 (IEC 68)

\*See "[Regulatory Notices](#)" for conditions of operation.

**System Requirements    Operating Systems**

The Router will support the following Operating Systems:

- Windows 98Se
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Windows Vista
- Mac OS 8.5 or higher
- Unix

**Ethernet Performance**    The Router complies to the IEEE 802.3i, u and x specifications.

**Cable Specifications**    The Router supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).

# C

## SAFETY INFORMATION

---

### Important Safety Information



**WARNING:** Warnings contain directions that you must follow for your personal safety. Follow all directions carefully. You must read the following safety information carefully before you install or remove the unit:



**WARNING:** The Router generates and uses radio frequency (rf) energy. In some environments, the use of rf energy is not permitted. The user should seek local advice on whether or not rf energy is permitted within the area of intended use.



**WARNING:** Exceptional care must be taken during installation and removal of the unit.



**WARNING:** To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.



**WARNING:** The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.



**WARNING:** This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.



**WARNING:** There are no user-replaceable fuses or user-serviceable parts inside the Router. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.



**WARNING:** Disconnect the power adapter before moving the unit.



**WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.

## Wichtige Sicherheitshinweise



**VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.

Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerat installieren oder ausbauen:



**VORSICHT:** Der Router erzeugt und verwendet Funkfrequenz (RF). In manchen Umgebungen ist die Verwendung von Funkfrequenz nicht gestattet. Erkundigen Sie sich bei den zustandigen Stellen, ob die Verwendung von Funkfrequenz in dem Bereich, in dem der Bluetooth Access Point eingesetzt werden soll, erlaubt ist.



**VORSICHT:** Bei der Installation und beim Ausbau des Gerats ist mit hochster Vorsicht vorzugehen.



**VORSICHT:** Aufgrund von internationalen Sicherheitsnormen darf das Gerat nur mit dem mitgelieferten Netzadapter verwendet werden.



**VORSICHT:** Die Netzsteckdose mu in der Nahе des Gerats und leicht zuganglich sein. Die Stromversorgung des Gerats kann nur durch Herausziehen des Geratenetzkabels aus der Netzsteckdose unterbrochen werden.



**VORSICHT:** Der Betrieb dieses Gerats erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gema IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerat angeschlossenen Gerate unter SELV-Bedingungen betrieben werden.



**VORSICHT:** Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Router haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.



**VORSICHT:** Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.



**VORSICHT: RJ-45-Anschlüsse.** Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.

## Consignes importantes de sécurité



**AVERTISSEMENT:** Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes. Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:



**AVERTISSEMENT:** La Router fournit et utilise de l'énergie radioélectrique (radio fréquence -rf). L'utilisation de l'énergie radioélectrique est interdite dans certains environnements. L'utilisateur devra se renseigner sur l'autorisation de cette énergie dans la zone prévue.



**AVERTISSEMENT:** Faites très attention lors de l'installation et de la dépose du groupe.



**AVERTISSEMENT:** Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.



**AVERTISSEMENT:** La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.



**AVERTISSEMENT:** L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces

*conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*



**AVERTISSEMENT:** *Il n'y a pas de parties remplaçables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.*



**AVERTISSEMENT:** *Débranchez l'adaptateur électrique avant de retirer cet appareil.*



**AVERTISSEMENT: Ports RJ-45.** *Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.*



# END USER SOFTWARE LICENSE AGREEMENT

---

## 3Com Corporation END USER SOFTWARE LICENSE AGREEMENT

**YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.**

**LICENSE:** 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

**ASSIGNMENT; NO REVERSE ENGINEERING:** You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

**EXPORT RESTRICTIONS:** The Software, including the Documentation and all related technical data (and any copies thereof) (collectively "Technical Data"), is subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data.

In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department's Table of Denial Orders or the U.S. Treasury Department's list of Specially Designated Nationals.

**TRADE SECRETS; TITLE:** You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

**UNITED STATES GOVERNMENT LEGENDS:** The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFARS 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

**TERM AND TERMINATION:** The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

**LIMITED WARRANTIES AND LIMITATION OF LIABILITY:** All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software; however, this End User Software License Agreement amends such Limited Warranty Card or product manual as follows: 3Com's warranty and warranty disclaimers for the materials runs from 3Com to the purchasing Internet Service Provider only (not the end user of the materials), and such warranty is only for a total of fifteen (15) months from the date of manufacture. Such warranties and limitations of liability are incorporated herein in their entirety by this reference. THERE ARE NO IMPLIED WARRANTIES. THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXCLUDED.

**GOVERNING LAW:** This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**SEVERABILITY:** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

**ENTIRE AGREEMENT:** This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concern this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

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

# E

## OBTAINING SUPPORT FOR YOUR PRODUCT

---

To obtain support for your product, please contact the ISP that supplied this product.



# GLOSSARY

- 802.11b** The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.
- 802.11g** The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.
- 10BASE-T** The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.
- 100BASE-TX** The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
- Access Point** An access point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.
- Ad Hoc mode** Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the router uses. (see also Infrastructure mode.)

- Auto-negotiation** Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.
- Bandwidth** The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.
- Category 3 Cables** One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.
- Category 5 Cables** One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.
- Channel** Similar to any radio device, the Wireless Cable/DSL router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.
- Client** The term used to describe the desktop PC that is connected to your network.
- DHCP** Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

- DNS Server Address** DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.
- DSL modem** DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.
- Encryption** A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.
- ESSID** Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the Router and each of its wireless clients.
- Ethernet** A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.
- Ethernet Address** See MAC address.
- Fast Ethernet** An Ethernet system that is designed to operate at 100 Mbps.
- Firewall** Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.
- Full Duplex** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
- Half Duplex** A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

**Hub** A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

**IEEE** Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

**IETF** Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

**Infrastructure mode** Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)

**IP** Internet Protocol. IP is a Layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

**IP Address** Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

**IPsec** IP Security. Provides IP network-layer encryption. IPsec can support large encryption networks (such as the Internet) by using digital certificates for device authentication. When setting up an IPsec connection between two devices, make sure that they support the same encryption method.

**ISP** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

- LAN** Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).
- MAC** Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.
- MAC Address** Media Access Control Address. Also called the hardware or physical address. A Layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.
- NAT** Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
- Network** A network is a collection of computers and other computer equipment that is connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.
- Network Interface Card (NIC)** A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.
- Protocol** A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.
- PPPoE** Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.
- PPTP** Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the Internet.

- RJ-45** A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.
- Router** A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.
- Server** A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.
- SSID** Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.
- Subnet Address** An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.
- Subnet Mask** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).
- Subnets** A network that is a component of a larger network.
- Switch** A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.
- TCP/IP** Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.
- TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

<b>Traffic</b>	The movement of data packets on a network.
<b>Universal Plug and Play</b>	Universal Plug and Play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.
<b>URL Filter</b>	A URL Filter is a feature of a firewall that allows it to stop its clients from browsing inappropriate Web sites.
<b>WAN</b>	Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.
<b>WDS</b>	Wireless Distribution System. WDS enables one or more access points to rebroadcast received signals to extend range and reach, though this can affect the overall throughput of data.
<b>WECA</b>	Wireless Ethernet Compatibility Alliance. An industry group formed to certify cross vendor interoperability and compatibility of 802.11b and 802.11g wireless networking products and to promote the standard for enterprise, small business and home environments. (see also 802.11b, 802.11g, Wi-Fi)
<b>WEP</b>	Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.
<b>Wi-Fi</b>	Wireless Fidelity. This is the certification granted by WECA to products that meet their interoperability criteria. (see also 802.11b, WECA)
<b>Wireless Client</b>	The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network.
<b>Wireless LAN Service Area</b>	Another term for ESSID (Extended Service Set Identifier).
<b>Wizard</b>	A Windows application that automates a procedure such as installation or configuration.

**WLAN** Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

**WPA** Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.

## REGULATORY NOTICES

### For 3Com Wireless 11n Cable/DSL Firewall Router

---

#### GENERAL STATEMENTS

The 3Com Wireless 11n Cable/DSL Firewall Router (WL-602) must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

This product contains encryption. It is unlawful to export out of the U.S. without obtaining a U.S. Export License.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate 3Com's warranty and all applicable regulatory certifications and approvals.

This product can only be used with the supplied antenna(s).

---

#### EXPOSURE TO RADIO FREQUENCY RADIATION

This device generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency exposure guidelines for an uncontrolled environment, this equipment must be installed and operated while maintaining a minimum body to antenna distance of 20 cm (approximately 8 in.).

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's website [www.hc-sc.gc.ca/rpb](http://www.hc-sc.gc.ca/rpb).

This product must maintain a minimum body to antenna distance of 20 cm. Under these conditions this product will meet the Basic Restriction limits of 1999/519/EC [Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)].

---

#### US - RADIO FREQUENCY REQUIREMENTS

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

---

#### US FEDERAL COMMUNICATIONS COMMISSION (FCC) EMC COMPLIANCE

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.

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.

**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.

#### 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.

2.4GHz operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

The user may find the following booklet prepared by the Federal Communications Commission helpful: The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402.

Stock No. 004-000-0034504.

3Com is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this 3Com Wireless 11n Cable/DSL Firewall Router (WL-602), or the substitution or attachment of connecting cables and equipment other than specified by 3Com.

The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

---

**US MANUFACTURER'S FCC  
DECLARATION OF  
CONFORMITY**

3Com Corporation  
350 Campus Drive  
Marlborough, MA 01752-3064, USA  
(508) 323-5000  
Date: April 24, 2008

Declares that the Product:

Brand Name: 3Com Corporation  
Model Number: WL-602  
Equipment Type: 3Com Wireless 11n Cable/DSL Firewall Router

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.




---

**INDUSTRY CANADA - RF  
COMPLIANCE**

This device complies with RSS-210 of the Industry Canada Rules.

Operation is subject to the following two conditions:

1) this device may not cause interference and, 2) this device must accept any interference, including interference that may cause undesired operation of the device.

L' utilisation de ce dispositif est autorisee seulement aux conditions suivantes: (1) il ne doit pas produire de brouillage et (2) l' utilisateur du dispositif doit etre pret a accepter tout brouillage radioelectrique recu, meme si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numerique de la class B est conforme a la norme NMB-003 du Canada.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for uncontrolled environments. 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.

2.4GHz operation of this product in Canada is firmware-limited to channels 1 through 11.

---

**INDUSTRY CANADA -  
EMISSIONS COMPLIANCE  
STATEMENT**

This Class B digital apparatus complies with Canadian ICES-003.

---

**AVIS DE CONFORMITÉ À LA  
RÉGLEMENTATION  
D'INDUSTRIE CANADA**

Cet appareil numérique de la classe B est conform à la norme NMB-003 du Canada.

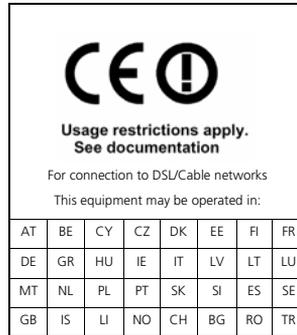
---

**SAFETY COMPLIANCE NOTICE**

This device has been tested and certified according to the following safety standards and is intended for use only in Information Technology Equipment which has been tested to these or other equivalent standards:

- UL Standard 60950-1
- CAN/CSA C22.2 No. 60950-1
- IEC 60950-1
- EN 60950-1

## EU COMPLIANCE



Intended use: DSL/Cable 802.11g/b/n Firewall Router

For connection to DSL/Cable networks

NOTE: To ensure product operation is in compliance with local regulations, select the country in which the product is installed. Refer to 3CRWER300-73 User Guide.

Česky [Czech]	3Com Coporation tímto prohlašuje, že tento <i>RLAN device</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede 3Com Coporation erklærer herved, at følgende udstyr <i>RLAN device</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt 3Com Coporation, dass sich das Gerät <i>RLAN device</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab 3Com Coporation seadme <i>RLAN device</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, 3Com Coporation, declares that this <i>RLAN device</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente 3Com Coporation declara que el <i>RLAN device</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ 3Com Coporation ΔΗΛΩΝΕΙ ΟΤΙ <i>RLAN device</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente <i>3Com Corporation</i> déclare que l'appareil <i>RLAN device</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente <i>3Com Corporation</i> dichiara che questo <i>RLAN device</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>3Com Corporation</i> deklarē, ka <i>RLAN device</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>3Com Corporation</i> deklaruoja, kad šis <i>RLAN device</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart <i>3Com Corporation</i> dat het toestel <i>RLAN device</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, <i>3Com Corporation</i> , jiddikjara li dan <i>RLAN device</i> jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, <i>3Com Corporation</i> nyilatkozik, hogy a <i>RLAN device</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym <i>3Com Corporation</i> oświadcza, że <i>RLAN device</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	<i>3Com Corporation</i> declara que este <i>RLAN device</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	<i>3Com Corporation</i> izjavlja, da je ta <i>RLAN device</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>3Com Corporation</i> týmto vyhlasuje, že <i>RLAN device</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	<i>3Com Corporation</i> vakuuttaa täten että <i>RLAN device</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

---

**EU - RESTRICTIONS FOR USE  
IN THE 2.4GHZ BAND**

This device can be operated in the EU without restrictions indoor. However, operated outdoors in France is restricted to 2400 ~ 2454 MHz : (Channel 1 ~ 7).

---

**BRAZIL RF COMPLIANCE**

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não causar interferência a sistema operando em caráter primário.

---

**DGT STATEMENT**

1. 經審驗合格之射頻電信終端設備，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。
2. 射頻電信終端設備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。所謂合法通信，係指依電信法規定作業之無線電信。
3. 輸入、製造射頻電信終端設備之公司、商號或其使用者違反本辦法規定，擅自使用或變更無線電頻率、電功率者，除依電信法規定處罰外，電信總局並得撤銷其審驗合格證明。
4. 本機限在不干擾合法電台與不受被干擾保障條件下於室內使用。
5. 為減少電磁波干擾，請妥適使用。

---

**SAFETY STATEMENT**

This product is intended to be supplied by a UL listed power unit marked "Class 2" or "LPS" rated 15V dc minimum 1A or 12V dc minimum 1A.

---

**PANASONIC LICENSED PATENT  
NUMBER**

Only for xDSL Product

Licensed under one or more of U.S. Patent Nos.6694470; 6735245; 6751254; 6765957; 6768772; 6873652; 6901547; 6917647; 6934326; 6950459; 6952442; 6987802; 6999506; 7012954; 7051258; 7058123; and 7272173



# INDEX

---

## Numbers

128-bit WEP 46  
128-bit WEP Screen 46  
1483 Bridge Mode 55  
64-bit WEP Screen 47

---

## A

Access Control Screen 62  
Add PC Screen 63  
Add Schedule Rule Screen 65  
Addresses  
    IP 85  
Admin Password Screen 75  
Advanced Screen 68  
Automatic Addressing 87

---

## B

Backup/Restore Settings Screen 74  
Bridge Mode for Single PC Screen 53  
Bridged Mode Configuration Screen 33

---

## C

Cable Specifications 91  
Channels 111  
Configuration Summary Screen 37  
Connection Type Screen 29, 50  
Conventions  
    notice icons, About This Guide 8  
    text, About This Guide 8

---

## D

DDNS 70  
DHCP 87  
DHCP Clients List 42  
DHCP server 25, 42  
disabling 26  
DMZ Screen 67  
DNS 24  
DNS Screen 55

DSL mode 29  
Dynamic Domain Server (DDNS) Screen 70  
Dynamic IP Address 34  
Dynamic/Fixed IP for Bridge Mode Screen 35, 55  
DYNDNS 70

---

## E

Editing DHCP Clients List Screen 42  
Encryption Screen 44  
Encryption, disabling 45

---

## F

Firewall Screen 59  
Forgotten Password 80

---

## H

Hostname  
    configuring 56  
Hostname and MAC Address Screen 56

---

## I

Internet  
    addresses 85  
Internet Properties Screen 26  
Internet Protocol (TCP/IP) Properties Screen 24  
IP Address 41, 85  
IPSEC 68

---

## L

LAN Settings Screen 41  
LED 14  
LEDs 14  
Local Area Properties Screen 24  
Logs Screen 77

---

## M

MAC Address 56  
    configuring 56

MAC Address Filtering Screen 66  
mode 30

---

## N

NAT (Network Address Translation) 68  
NAT-T (NAT Traversal) 68  
Network  
  addresses 85  
Networking  
  wireless 81  
NIC  
  wireless 14

---

## P

Password 27, 75  
Poison Reverse 58  
PPPoA 31  
PPPoA Screen 31  
PPPoA Settings Screen 52  
PPPoE 26, 30, 31  
PPPoE Screen 30  
PPPoE Settings Screen 51

---

## R

Remote Admin 68  
Reset to Factory Default Screen 73  
Reset to Factory Defaults 80  
Restart Router Screen 73  
RFC 1483 Bridged Mode 32, 53  
RFC 1483 Routed Mode 34  
RIP (Routing Information Protocol) 57  
RIP Parameter Screen 58  
Router Login Screen 28  
Routing Mode Screen 34  
Routing Table Screen 59

---

## S

Schedule Rule Screen 65  
Setup Wizard 27  
SNMP Community Screen 71  
SNMP Trap Screen 72  
Special Applications Screen 60  
Specifications  
  technical 89  
SSID 31, 32, 33, 35, 36, 43  
Static Addressing 87  
Static Route Parameters Screen 57  
Status Screen 28, 40  
Subnet Mask 85

---

---

## T

TCP/IP 23, 25, 85  
Technical  
  specifications 89  
  standards 89  
Time and Time Zone screen 76  
TZO.com 70

---

## U

Universal Plug and Play 68  
Upgrade Screen 74  
URL Blocking Screen 64

---

## V

Virtual Servers Screen 61  
VPI/VCI 30, 32, 33, 34, 36

---

## W

WAN Ping Blocking 68  
WDS 49  
Web Browser Location Field 27  
Web Proxy 26  
WiFi Protected Access 45, 48  
Wireless  
  networking 81  
  NIC 14  
Wireless Configuration Screen 43  
Wireless Settings Screen 31, 32, 33, 35, 36, 43  
Wireless WDS Settings Screen 49  
WPA (with RADIUS Server) Screen 48  
WPA-PSK (no server) Screen 45