adsl nation

USER GUIDE

Technical Support

TO OBTAIN TECHNICAL SUPPORT. PLEASE RETAIN PROOF OF PURCHASE AND THE WARRANTY INFORMATION.

To get product support or obtain product information and documentation, go to http://www.adslnation.com/support.

If you would like to contact technical support by telephone, please call
0845 125 9426 (low cost non geographical number)
01865 761114 (calls charged at operators standard national tariff)
Technical support is available 9am - 6pm weekdays.

ADSL Nation LTD.
E-mail: support@adslnation.com
www.adslnation.com

Introduction

Congratulations ! You are now the owner of an ADSL Nation X-Station.

From now on your internet experience will be transformed due to the high speed that ADSL technology and the X-Station delivers.

This manual will guide you through setting up your X-Station and provide a reference point for all the features of your wireless modem router.

Safety Instructions

The X-Station is intended for internal desktop use only.

Climate Conditions

•The maximum ambient temperature must not exceed 40 °C (104°F).

•The router must not be mounted in a location exposed to direct sunlight or excessive heat radiation.

•Ensure the router is not subjected to water or condensation.

Cleaning

Unplug the router from the mains outlet and wipe with a damp cloth. Do not use chemical cleaning products or solvents as it may damage the surface of the router.

Water and moisture

Do not use this product near water.

Overloading

Do not overload mains outlets and extensions as it can result in fire or electric shock.

What's in the Box

The following items are supplied with your X-Station:

X-Station

UK Power Supply Unit

RJ11 - RJ11 Cable often referred to as the telephone cable.

RJ45 Cat 5 Ethernet cable.

X-Station Wireless Technology

The X-Station's built-in wireless connectivity confirms to the industry standard 802.11g and is backwards compatible with 802.11b wireless equipment. Any equipment with the WiFi logo or listing 802.11g or 802.11b wireless standards will work with the X-Station. Mac users will be more familiar with the terms Airport & Airport Extreme. The X-Station runs at the full Airport Extreme speed and is backwards compatible with older Airport cards.

The X-Station works on any ADSL service that uses PPPoA or PPPoE with either static or dynamic IP addresses.

In the default configuration the X-Station's employs NAT (Network Address Translation) technology to allow multiple computers to share a single broadband service. This makes the X-Station the perfect solution for people who wish to a connection to the internet that is often described as a home or single user service.

X-Station Overview

Front View

PWR: Shows that power is being received by the router.

WL ACT: Flashes when wireless data is sent or received.

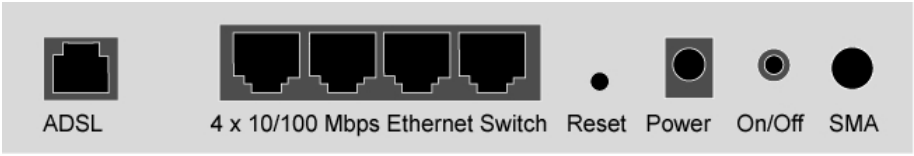
LINK/ACT: 1 LED for each ethernet port labeled 1 - 4 Illuminated when a Ethernet connection has been established on the corresponding Ethernet port, flashes when data is being sent or received on that port.

ADSL: Illuminates when the an ADSL signal has been detected on the line. A flashing link LED indicates that the modem is probing for an ADSL signal.

RxD: Flashes when data to indicate data is being received from the built-in ADSL modem.

PPP: Illuminates when the router is successfully logged into the Internet Service Provider using the account details provided.

Rear View



ADSL: Telephone jack (RJ-11) to connect to your Telephone Wall Socket (ADSL line).

LAN: 10 / 100 Base-T Ethernet jacks (RJ-45) to connect to your Ethernet Equipped computers.

Reset: To reset your router to factory default settings. (All Customised settings that you have saved will be lost!)

Power: To connect to your power outlet using the power adapter.

Before Installing

Gather Configuration Information from your ISP.

When configuring the X-Station to work with a standard BT Wholesale provided ADSL line the only configuration information required is the username and password. For Karoo installations and non UK installations please refer to the advanced settings section of this guide.

Note: Your ISP should have provided you with a summary sheet of all the Information needed to connect your computer to the Internet. If you cannot locate the information, you'll have to contact your ISP. BT Broadband provide a Login name only and do not issue a password.

LOGIN NAME: _____
example john.smith@btinternet.com

PASSWORD: _____

Note: The login name could be called a user name or account name by your ISP. The login name and password are case sensitive. You must type them exactly as given by the ISP.

Computer requirements

The computer that you want to use with the X-Station must have either an available RJ-45 Ethernet port or 802.11b/g wireless adaptor and TCP/IP networking installed.
Note: TCP/IP networking is already installed on most operating systems including Microsoft Windows and MacOS.

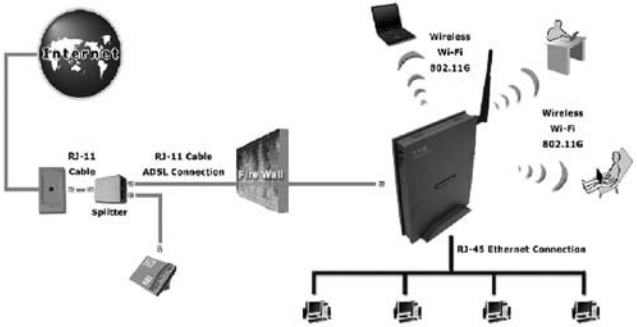
Microfilters

Ensure you have enough ADSL microfilters for your line. At least one microfilter will be required to connect the modem and any existing telephone equipment to. If other telephone equipment is used on the line it must also be connected to a microfilter.

A microfilter prevents high frequency noise from appearing at the telephone and potentially decreasing voice quality. Second, it prevents the telephone equipment from interfering with the modem. For more information on microfilters please visit www.adslnation.com

Connecting the X-Station to a Computer/Notebook

To connect your Computer to the X-Station using a cable, you need to have an Ethernet port available on your Computer. Most Computers/ Notebooks have labels describing the Ports. For the Ethernet Port, you will see either ETHERNET, ETH, RJ45 or <--> labelled near the Port.



Connecting to the ADSL Line

Connect the RJ11 (phone) cable provided to the ADSL/Modem port of the ADSL Microfilter and then connect the opposite end of the cable to the ADSL port on the X-Station.

Plug the microfilter in to the telephone socket and connect any telephone equipment to the phone port on the Microfilter.

Note: You will need to ensure that all telephone equipment on the same line as your X-Station is also connected to a Microfilter. If you do not have enough microfilters remove any unfiltered telephone equipment. Microfilters are available to order on-line at www.adslnation.com.

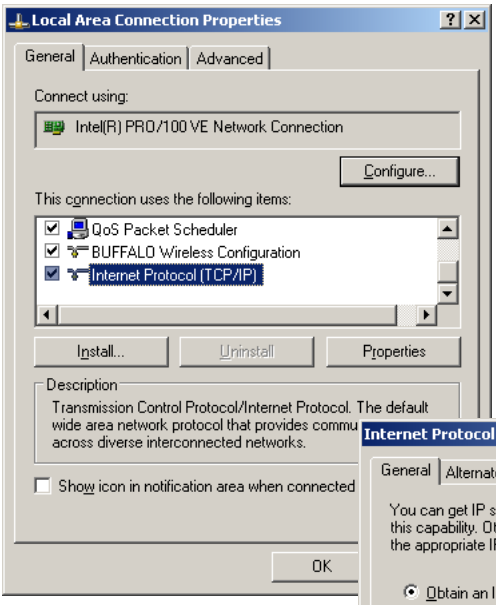
Connect the power to the modem, if an ADSL signal is detected the ADSL LED will illuminate and remain on. If the ADSL LED continues to flash the modem is unable to locate a usable ADSL signal. This may be because the line has not been enabled for ADSL or that a fault condition has occurred such as an unfiltered telephone device causing interference on the line. The ADSL light must stay illuminated before proceeding with the set-up procedure.

Configuring Windows XP Networking

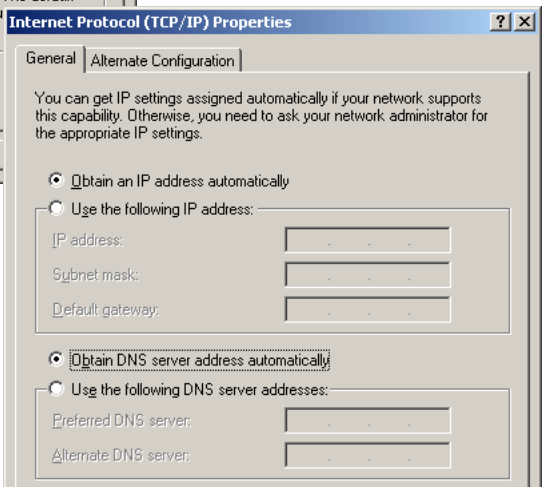
The default network configuration on the computer should already be suitable for connection to the X-Station. However if you are uncertain or any network settings have been changed they will need to be configured as follows.

(Instructions are based on default XP Start menu option)
From the Windows desktop, click Start > All Programs > Accessories > Communications > Network Connections.

Right-click on the Local Area Connection icon that reflects the model of your Ethernet or Wireless Network Card that is used to connect to the X-Station and click Properties.



Ensure that the field Connect Using shows the model of your Ethernet or Wireless Network Card that will be used to configure your X-Station. Select Internet Protocol (TCP/IP) and click Properties.



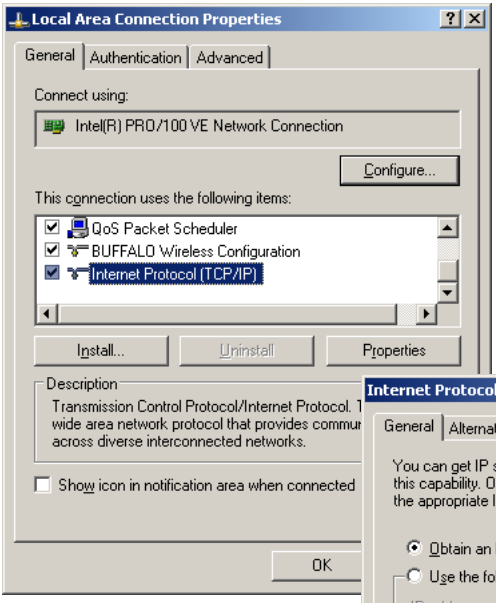
Select the option Obtain an IP address automatically and Obtain DNS server address automatically. Click OK and close to apply.
Ensure that your X-Station is powered on and restart your system.

Configuring Windows 2000 Networking

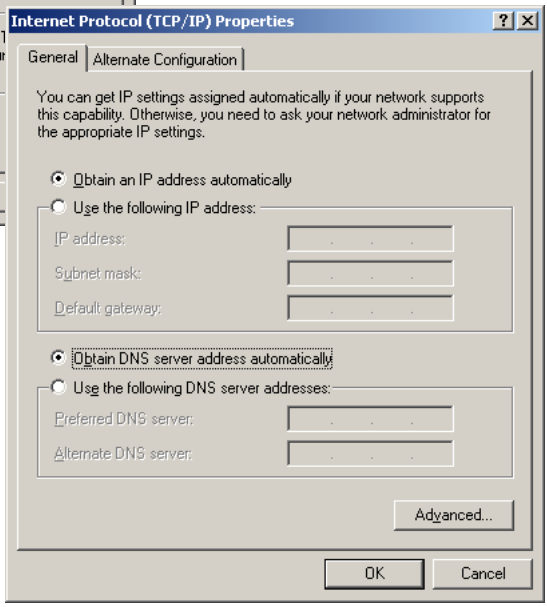
The default network configuration on the computer should already be suitable for Ethernet connection to the X-Station, wireless connections however will require additional software supplied by the wireless card manufacturer to be installed. If you are uncertain or any network settings have been changed they will need to be configured as follows.

Click the Start > Settings and choose “Network & Dial-up Connections”.

At the Network and Dial-up Connections window. Right-click on the Local Area Connection icon that reflects the model of your Ethernet Network Card that is connected to the X-Station and click Properties.



Ensure that the field Connect Using shows the model of your Ethernet Network Card that is connected to your ADSL Ethernet Modem. Select Internet Protocol (TCP/IP) and click Properties.

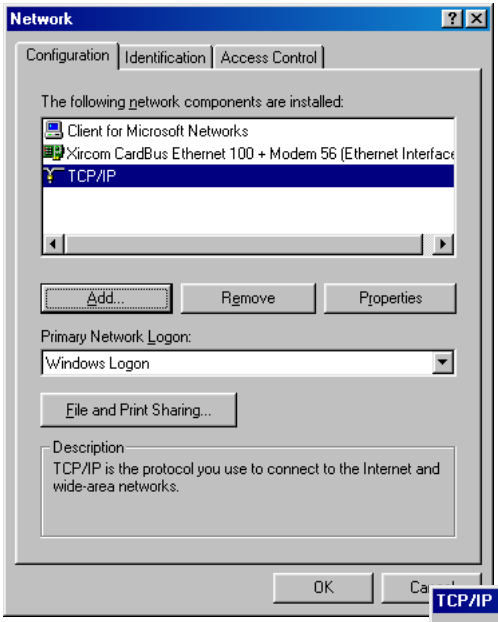


Select the option Obtain an IP address automatically and Obtain DNS server address automatically. Click OK and OK again to close.
Ensure that your Modem is powered on and restart your system.

Configuring Windows 98/ME Networking

From your Windows desktop, right-click on the Network Neighbourhood icon.

Select Properties.



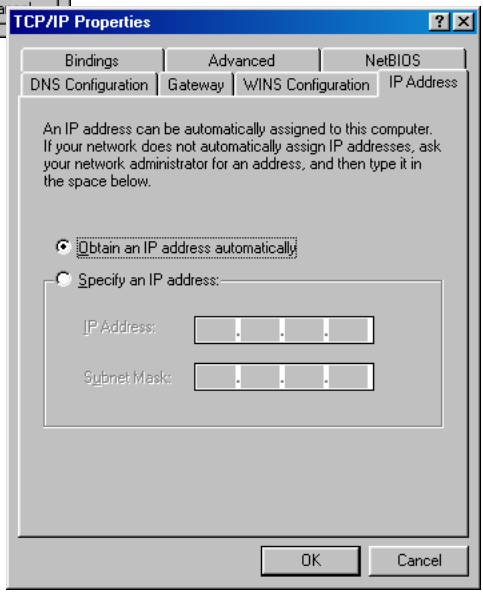
From the Configuration tab, select TCP/IP-> if multiple instances of TCP/IP are shown select the one that refers to the model of your Ethernet Network Card that is connected to the X-Station.

Click Properties.

Click the option Obtain an IP address automatically and click OK to save the settings.

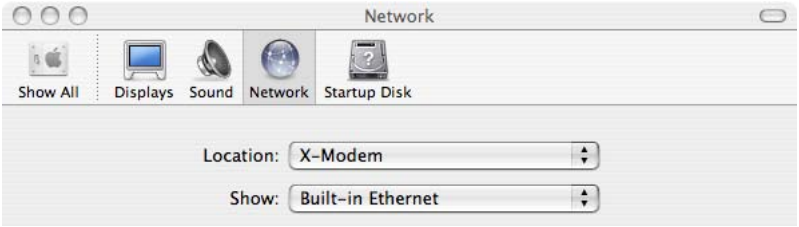
Ensure that your X-Station is powered on. Restart your system.

Wireless connectivity for Windows 98/ME is not covered here, please refer to the documentation supplied with your wireless adaptor to configure it to connect to the X-Station.



Configuring Mac OS X Networking

Open the System Preferences utility and click on the network icon.



Select New Location from the Location drop down list and name it X-Station, click Apply Now all default settings are correct. The network status window will show the current status of available network connections. If connecting via Built-In-Ethernet a green light should be displayed next to the Built-In-Ethernet.

If connecting Via Airport a green light should be shown next to Airport. If the light is Amber please check in the Airport status menu to ensure your Airport has found the X-Station wireless signal.

Ensure that your X-Station is powered on. Restart your system.

Configuring Mac OS 9 Networking

Open the TCP/IP control panel. You can find it in the Apple Menu under the folder “Control Panels.”

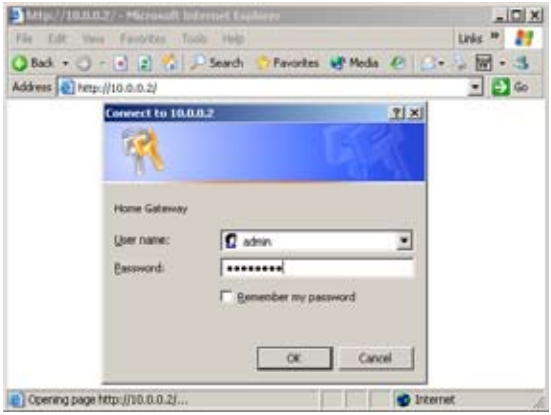
Make sure your network card is selected usually “built-in Ethernet” or “Airport” and set configure using DHCP.

Close the window and save changes if prompted.

Ensure that your X-Station is powered on. Restart your system.

Connecting to the X-Station

The X-Station provides a web-based (HTML) graphical user interface allowing users to manage the router using a standard browser such as Microsoft Internet Explorer, Firefox, or Apple's Safari Browser. No extra software or drivers are required to configure the X-Station.
To connect to the X-Station, open your web browser and enter the X-Station default IP address **http://10.0.0.2** in to the browsers address bar.



When prompted enter the default login User Name and Password.

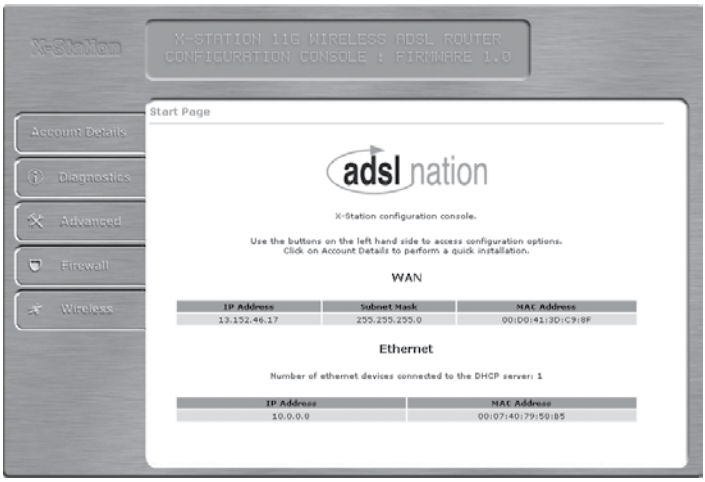
Default login details

User Name: admin
Password: password

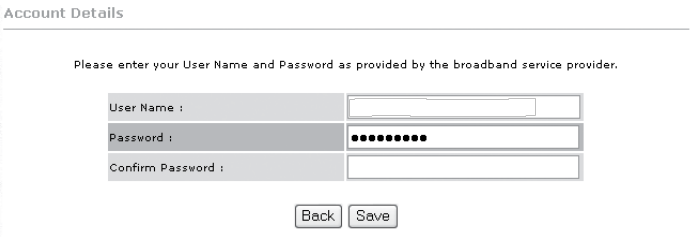
Note: The user name and password prompt may take up to 1 min. the first time the modem is accessed. If the prompt does not appear please check your browsers proxy settings to ensure that no proxy servers are configured.

Quick Set-up Procedure

In order to make the installation process quick and easy the X-Station comes pre-configured for use on a standard BT phone line in the UK. If your phone line is not provided by BT some additional settings may need to be adjusted.



Click the Account Details button on the left of the screen.



Enter your account details as provided by your Internet Service Provider.

Note: Usernames and passwords are case sensitive and often passwords contain a combination of letters and numbers.

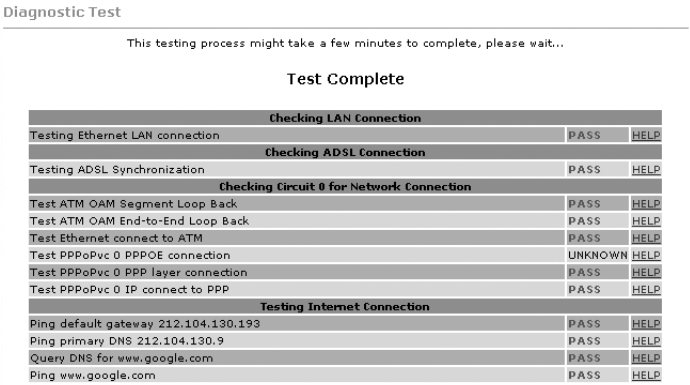
Click save, the X-Station will save your details and reboot. After rebooting is complete you will automatically be connected to the internet.

Testing The Connection

When the modem has been configured with the ISP account details and rebooting has completed the connection can be tested.

Note: after reboot it may take up to 2 min for the modem to negotiate a connection to the ISP depending on the quality of the phone line.

To test the connection click the Diagnostics button, after a short pause test results will begin to appear.



Diagnostic Test

This testing process might take a few minutes to complete, please wait...

Test Complete

Checking LAN Connection		
Testing Ethernet LAN connection	PASS	HELP
Checking ADSL Connection		
Testing ADSL Synchronization	PASS	HELP
Checking Circuit 0 for Network Connection		
Test ATM OAM Segment Loop Back	PASS	HELP
Test ATM OAM End-to-End Loop Back	PASS	HELP
Test Ethernet connect to ATM	PASS	HELP
Test PPPoPvc 0 PPPOE connection	UNKNOWN	HELP
Test PPPoPvc 0 PPP layer connection	PASS	HELP
Test PPPoPvc 0 IP connect to PPP	PASS	HELP
Testing Internet Connection		
Ping default gateway 212.104.130.193	PASS	HELP
Ping primary DNS 212.104.130.9	PASS	HELP
Query DNS for www.google.com	PASS	HELP
Ping www.google.com	PASS	HELP

If no Fail results are reported the X-Station has successfully connected to the internet. Further details are available about the meaning of each test by clicking the help link by each test.

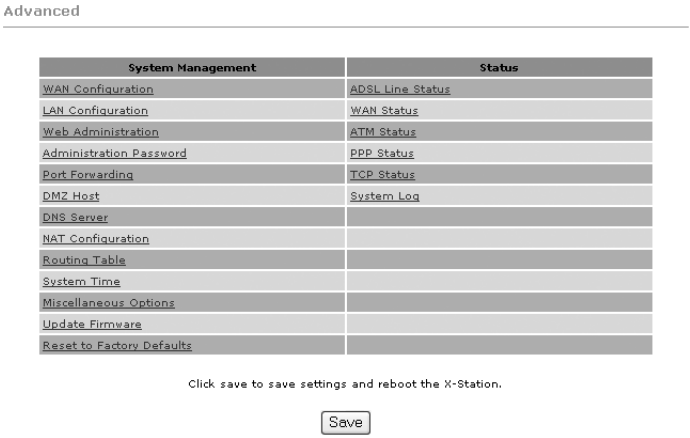
Note: The most common test to fail is the “Test simple PPP session layer connection”. This means that when the modem attempted to login to the ISP it was rejected. Double check your account details are correct, remember that both the username and password are case sensitive. Make sure that you have the full username including the part after the @ symbol. Also it is common practice for passwords to contain numbers so what looks like the letter l could be the number 1.

Now that the line tests are complete the connection can be verified by visiting a web site such as http://www.adslnation.com

Congratulations you are now on-line !

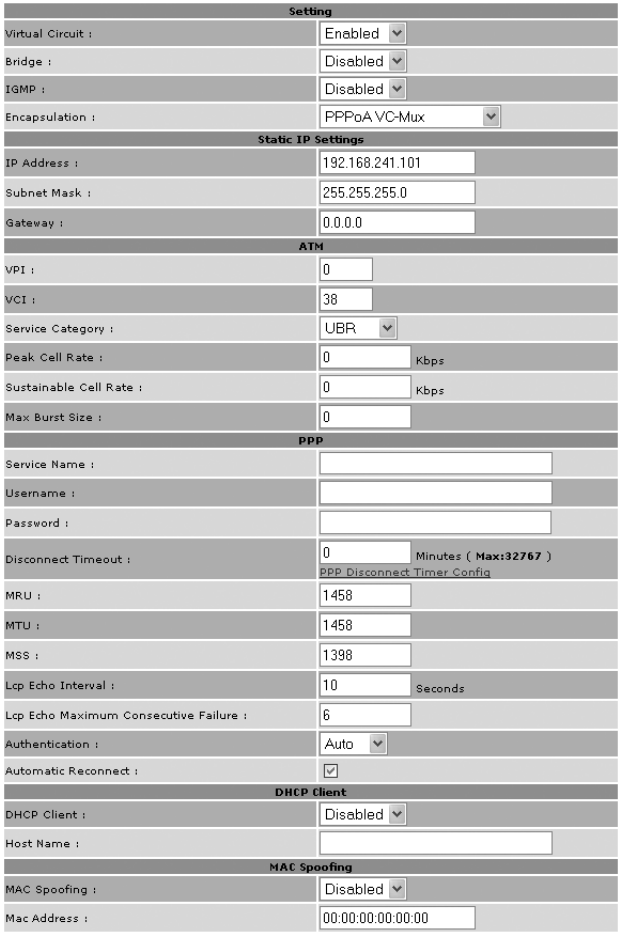
Advanced Configuration Options

In most circumstances it will not be necessary to change any of the settings under the advanced options. Users of ADSL outside the UK or lines not provided by BT may however need to change some settings here.



Any modifications made in the advanced options will require saving before changes take effect. To save any changes click on the save button. The Advanced screen can be returned to at any time by clicking the advanced button.

WAN Configuration



Setting	
Virtual Circuit :	Enabled
Bridge :	Disabled
IGMP :	Disabled
Encapsulation :	PPPoA VC-Mux
Static IP Settings	
IP Address :	192.168.241.101
Subnet Mask :	255.255.255.0
Gateway :	0.0.0.0
ATM	
VPI :	0
VCI :	38
Service Category :	UBR
Peak Cell Rate :	0 Kbps
Sustainable Cell Rate :	0 Kbps
Max Burst Size :	0
PPP	
Service Name :	
Username :	
Password :	
Disconnect Timeout :	0 Minutes (**Max:32767**) PPP Disconnect Timer Config
MRU :	1458
MTU :	1458
MSS :	1398
Lcp Echo Interval :	10 Seconds
Lcp Echo Maximum Consecutive Failure :	6
Authentication :	Auto
Automatic Reconnect :	☑
DHCP Client	
DHCP Client :	Disabled
Host Name :	
MAC Spoofing	
MAC Spoofing :	Disabled
Mac Address :	00:00:00:00:00:00

Setting

Virtual Circuit: Select Enabled to activate the current PVC configuration. The current PVC is displayed at the top of the page in parenthesis. Default is “Enabled” for “PVC0” and “Disabled” for “PVC1 ~ PVC7”.

Bridge: Passes PPP data through to LAN PPP host (dumb modem mode). This is available in PPPoE Modes only and is not generally used in the UK. The default setting is Disabled.

WAN Configuration

IGMP: (Internet Group Management Protocol) relay/proxy specification and environment, default is “Disabled”. IGMP is available in all modes and all encapsulations.

Note: Before the IGMP mode is enabled; please go to the “Misc Configuration” page to enable the IGMP proxy. Otherwise, the IGMP selection will not be valid.

Encapsulation: The different types of encapsulation, the encapsulation selected must match that used by your network operator. The Default setting that is suitable for all UK services is “PPPoA VC-Mux”

Static IP Settings

Static IP Settings are for users who are required to configure a static IP address (WAN side). Most ISP’s automatically assign IP addresses even when a fixed address or range of addresses are requested from the ISP. The IP address automatically assigned by the ISP always overrides anything entered here so this section can be ignored by most users.

ATM

Asynchronous Transfer Mode is a method of transfer in which data is organized into 53-byte cell units. ATM is the standard used by UK carriers to carry broadband services between the ISP and customer.

VPI: Virtual Path Identifier, this information will be supplied by your ISP the default for the UK networks is 0.

VCI: A Virtual Channel Identifier, this information will be supplied by your ISP the default for the UK networks is 38.

Service Category: This field allows you to select from the following service categories, with “UBR” as the default.

UBR (Unspecified Bit Rate): When configured as UBR, traffic is delivered with best efforts but with no guarantee. This allows for fluctuation in available bandwidth.

CBR (Constant Bit Rate): When a PVC is specified as a CBR, that PVC is guaranteed a certain bandwidth, characterized by the Peak Cell Rate (PCR).

WAN Configuration

PPP

Service Name: The Service Name of the PPP session is required by some ISPs mainly in the USA. If the ISP does not provide the Service Name, please leave it blank.

Username: The username or login ID provided by the ISP.

Password: The password provided by the ISP.

Disconnect Timeout: The Disconnect Timeout allows you to set the specific period of time, in minutes, to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

MRU: (Maximum Receive Unit) indicates the maximum size IP packet that can be received. The default value is 1458.

MTU: (Maximum Transmission Unit) indicates the largest size packet that can be sent. If a packet is larger than the MTU value, then the packet will be fragmented before the transmission. The default value is 1458.

MSS: (Maximum Segment Size) is the largest size of data that TCP will send in a single, unfragmented IP packet. The default value is 1398.

Lcp Echo Interval: This is the time interval, in seconds, between PPP session connection attempts, default value is 10.

Lcp Echo Maximum Consecutive Failure: This is the number of times a PPP session can fail while trying to connect before stopping. If a PPP session fails this number of times, you must manually reconnect the PPP session, the default value is 6.

Authentication : If the ISP requires a manual authentication method it should be set here, otherwise the Auto setting should be used.

Auto Reconnect : With this option set the modem will attempt to reconnect if the connection to the service is lost. Default setting = on.

WAN Configuration

DHCP Client

DHCP Client: When enabled the WAN is configured as a DHCP client, where the ISP would be the DHCP server. The default setting is Disabled.

This option is for non-static (dynamic) IP addresses.
DHCP Client is generally used in the following encapsulations:

1483 Bridged IP LLC
1483 Routed IP LLC
1483 Bridged IP VC-MUX
1483 Routed IP VC-Mux
Classical IP over ATM.

Host Name: When DHCP Client is “Enabled”, enter the ISP recognized Host Name here. The Host Name can be up to 19 characters.

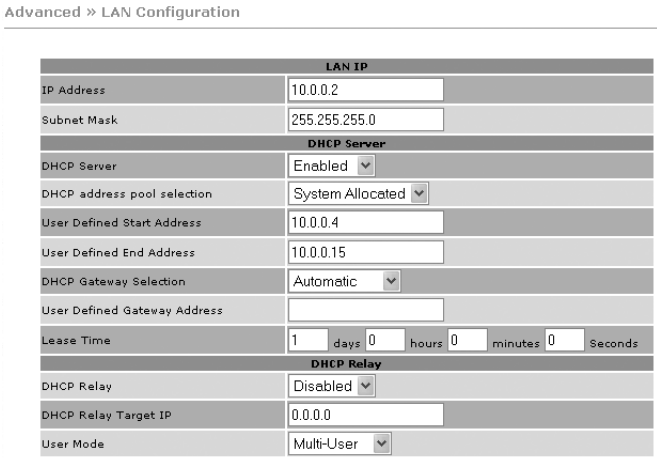
MAC Spoofing: MAC Spoofing: Enable MAC Spoofing to make a different MAC Address appear on the WAN side. This is also used to solve the scenario where the ISP only recognizes one MAC Address.

Default is “Disabled”.

MAC Address: When MAC Spoofing is enabled, copy the ISP-recognized MAC address here. Format for MAC address is six pairs of hexadecimal numbers (0-9, A-F) separated by colons.

Default is 00:00:00:00:00:00.

LAN Configuration



LAN IP

The IP address used by the X-Station. The subnet mask is used to determine the size of the local network. The default setting should be left at 255.255.255.0 unless and special mask configuration is required.

DHCP Server

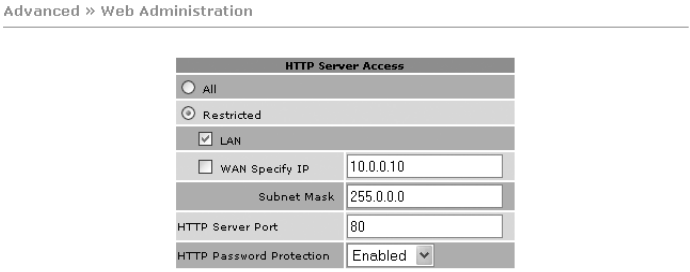
The DHCP server automatically hands out IP addresses to computers on the network. It should remain enabled unless the X-Station is to be used on a network that already has a DHCP server. By default all DHCP settings are provided automatically but can be set manually if required.

The range of IP addresses issued by the DHCP server can be selected manually by setting the pool selection to Manually Assigned and selecting the start and end Address. The Start and End Addresses must be in the same range as the LAN IP.

DHCP Relay

This feature is not currently used in the UK and should be Disabled, the default setting. The DHCP relay feature allows the ISP to control IP addresses issued to the local network.

Web Administration



Access Restrictions

Access to the X-Station web administration by default is restricted to computers on the local network only. Access restrictions can be relaxed to allow a specific computer, range of computers, or any computer on the internet to access the X-station for the purpose of remote management.

Note: We strongly advise against allowing remote administration of the X-Station as the security risk is high that someone may guess the password and gain unauthorized access to the X-Station. If you must allow remote administration please change the default http port as described below to reduce the risk.

HTTP Port

The port used by the built-in web server to serve the web administration interface. The should be changed if access to a public web server hosted on the computer attached to the X-Station is required and is also recommended for improved security when allowing remote administration.

Note: When changing the http port the X-Station will not be able to report that saving the configuration has been successful. To access the web interface on a new port it will be necessary to append the new port to the web address for example http://10.0.0.2:8080 for port 8080.

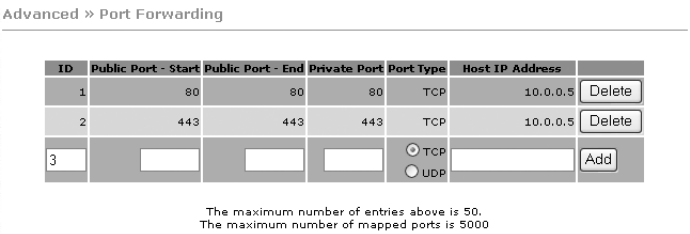
Administration Password

Password Protection

Access to the X-Station web administration is protected by a password. To prevent unautorized access to the X-Station the default password should be changed to a password of your choice.

Note: For the strongest security use a combination of letters and numbers in the new password.

Port Forwarding



Special Applications

The default X-Station configuration uses Network Address Translation that prevents incoming connections from the Internet entering the local network. This is usually a desirable situation as it provides a basic firewall facility to protect the network. However some special applications may require that an incoming connection is allowed.

The Port Forwarding option allows selection of a special port to be redirected from the modem to a specified IP address. The example shows how to forward port 80 the standard http web port to a computer with the IP address 10.0.0.5 20 Special ports can be added to the port forward screen.

To add a port simply fill out the boxes.

Public Port Start: The first port number that the external client will be connecting to to access the service.

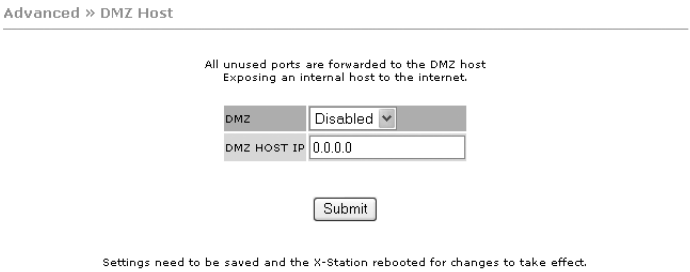
Public Port End: The last number that the external client will be connecting to to access the service. Where a single port is required the Start and End port numbers are the same.

Private Port: The port number that the service is running on, on the local machine. Usually both Public & Private ports are the same.

Port Type: Set the required type of port, usually TCP.

Host IP Address: IP address of local computer hosting service.

DMZ Host

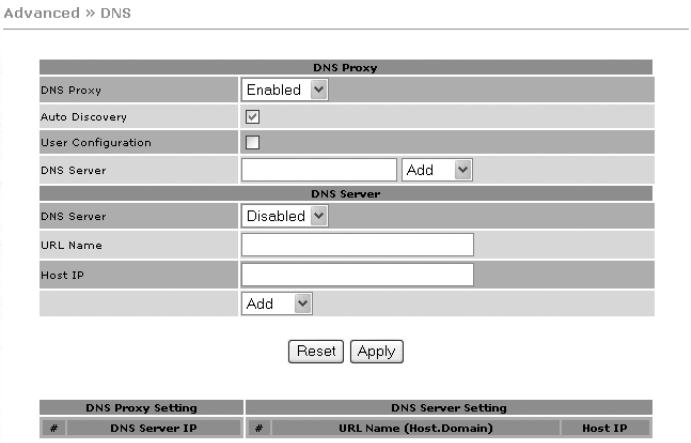


DMZ

Sometimes it is necessary to completely expose a computer to the internet for example when so many ports are required that port forwarding is not practical. Enabling the DMZ function forwards all unused ports to a chosen computer. Put the IP address of the chosen computer in the DMZ Host IP box.

Note: Use of the DMZ function is a big security risk as the computer selected has no protection from the internet. If DMZ is used ensure that every security precaution is taken on the exposed computer such as ensuring all security related software updates are installed, up-to-date anti-virus and firewall software is installed.

DNS Server



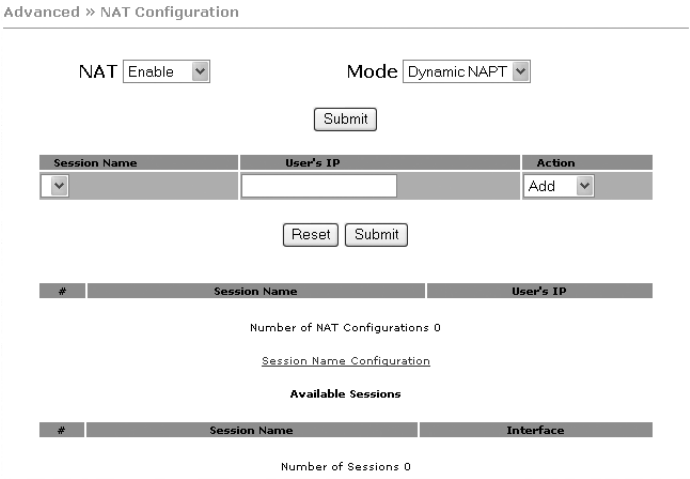
DNS Proxy

The Domain Name System is the way names are converted to IP addresses on the internet. The X-Station includes a DNS server that automatically redirects name lookups to the ISP's DNS servers. The default setting is enabled.

DNS Server

The X-Station can act as a DNS server for the local network if required. By default this option is disabled as it is only required for advanced network configurations.

NAT Configuration



NAT

By default NAT is enabled and the X-Station shares a single public IP address with multiple computers. NAT would typically be turned off where multiple public IP addresses are provided by the ISP and no sharing is required.

Mode

(NAT) Static peer-to-peer mode (1x1), (NAPT) Static multiple mapping mode (1xN), (Dynamic NAPT) Dynamic multiple mapping mode (NxN).

Session Name: Select the session from the configured NAT Session Name Configuration.

User's IP: Assigns the IP address to map the corresponding NAT/NAPT sessions.

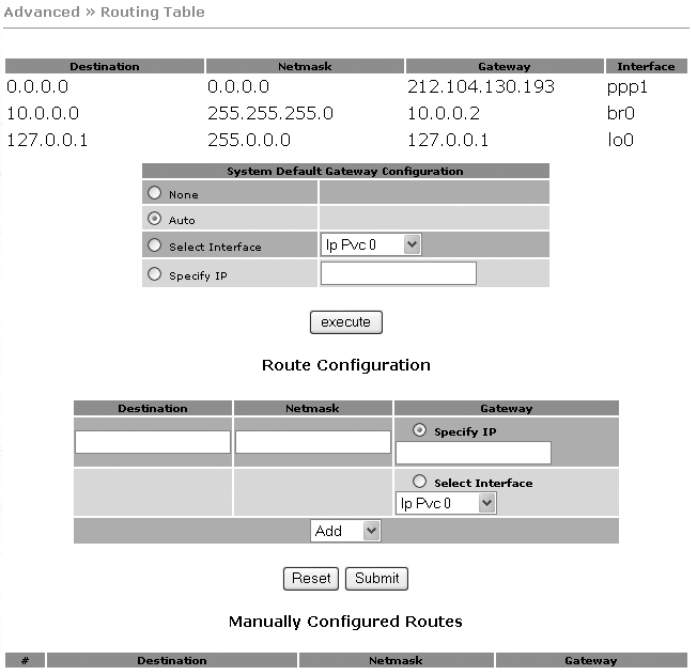
Session Name Status: Table showing the Session Name with IP Address.

Number of NAT Configurations: Displays the total NAT Sessions.

Available Sessions: This table will be displayed at the bottom of the page to show all the available Session Names with their corresponding WAN Interface.

Number of Sessions: This field displays the total number of NAT Sessions entered.

Routing Table

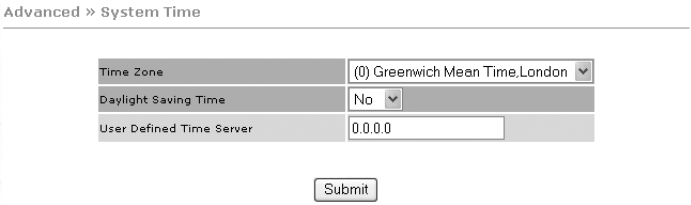


The Routing Table displays the routing table and allows you to manually enter a routing entry. The routing table will display the routing status of Destination, Netmask, Gateway, and Interface. The interface “br0” is unused; “lo0” indicates the loopback interface; “ppp1” indicates the PPP interface. The Gateway is the learned Gateway.

The Gateway field of the static route entry allows users to either enter a Gateway IP address or select a Network Interface.

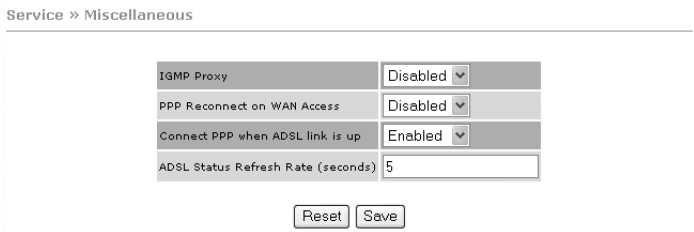
If the selected Network Interface is static or dynamic and the connection is already up, then the route entry appears in the Routing Table immediately. If there is a Gateway associated with the selected Network Interface, then that Gateway’s IP address appears in the Gateway field of the route entry. If the selected Network Interface is dynamic but the connection is not established, then the route entry does not appear in the Routing Table. When the interface comes up later, the route entry is then added.

System Time



The X-Station will attempt to automatically obtain time server information from the ISP in order to set the time automatically. If your ISP does not provide the required time server information a NTP time server can be added manually here.

Miscellaneous Options



IGMP Proxy: This is the global setting for IGMP Proxy. If it is enabled, then the enabled IGMP Proxy on WAN PVCs will be working. Otherwise, no WAN PVC can have IGMP Proxy working on it. System default is Disabled.

PPP Reconnect on WAN Access: If enabled, the PPP session will automatically establish a connection when a packet tries to access the WAN. System default is “Disabled”.

Connect PPP when ADSL Link is Up: If this option is “Enabled”, X-Station will automatically connect the PPP session whenever an ADSL connection is established. System default is “Enabled”.

Update Firmware

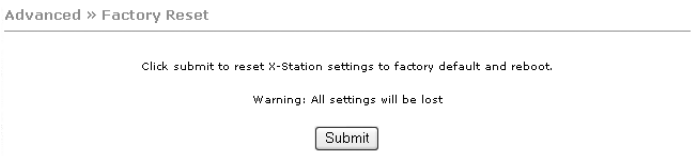
Firmware Updates

ADSL Nation may make firmware updates available to download from our web site.

Detailed instructions are provided with firmware updates.

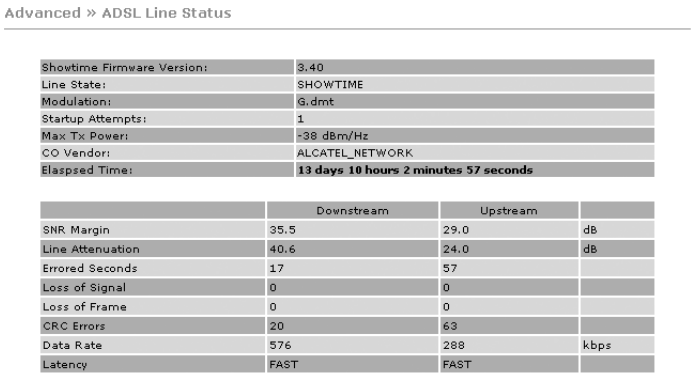
Note: If the update button has been clicked in error the firmware update must be cancelled to resume normal operation.

Reset to Factory Defaults



When resetting the X-Station to factory defaults ALL settings will be restored back to the original settings when the X-Station left the factory.

ADSL Line Status



Advanced » ADSL Line Status

Showtime Firmware Version:	3.40
Line State:	SHOWTIME
Modulation:	G.dmt
Startup Attempts:	1
Max Tx Power:	-38 dBm/Hz
CO Vendor:	ALCATEL_NETWORK
Elaspsed Time:	**13 days 10 hours 2 minutes 57 seconds**

	Downstream	Upstream	
SNR Margin	35.5	29.0	dB
Line Attenuation	40.6	24.0	dB
Errored Seconds	17	57	
Loss of Signal	0	0	
Loss of Frame	0	0	
CRC Errors	20	63	
Data Rate	576	288	kbps
Latency	FAST	FAST	

SNR Margin: Signal to Noise Ratio indicates the amount of usable signal compared to unwanted noise. The higher the value the better quality the connection, a connection may not be possible if the SNR value drops below 16db.

Line Attenuation: Indicates the amount of signal lost due to the natural resistance in the phone line. The lower the value the better quality the connection. A connection may not be possible if Attenuation exceeds 60db.

Loss of Signal: If the ADSL connection is lost due to the modem being disconnected from the line or a fault condition it will be recorded here. An excessive number of signal losses indicates a problem with the line.

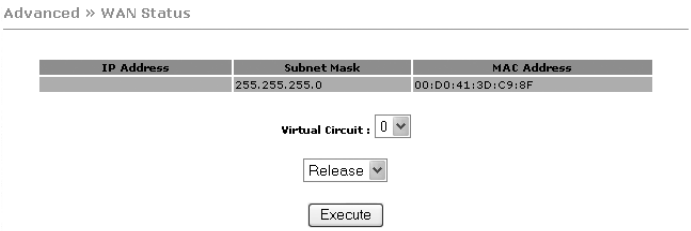
Loss of Frame: When data fails to be sent across the ATM network the frame may be lost. A small number of frames may be reported lost if the line quality is poor. An excessive number of lost frames indicates a fault condition.

CRC Errors: Data is checked for integrity as it is transmitted, some CRC errors are normal due to interference on the line. An excessive number of crc errors indicates a potential problem with interference.

Data Rate: The speeds in kilobytes that the modem has negotiated with the exchange equipment.

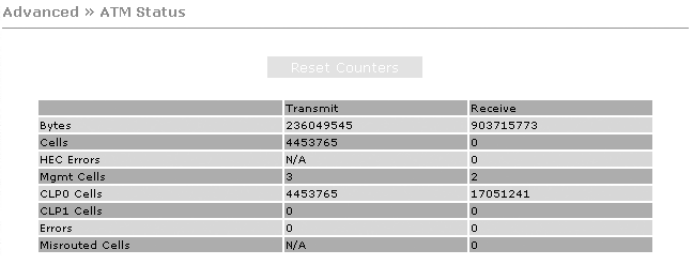
Latency: The delay introduced on the line sometimes referred to as ping.

WAN Status



Displays the current IP Address, Subnet Mask, and MAC address for the current active connection. The connection can be disconnected or reset using the drop down menu and clicking the Execute button.

ATM Status



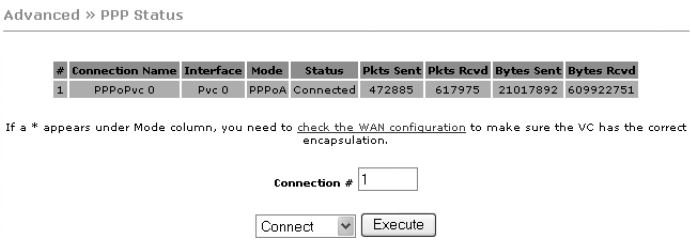
	Transmit	Receive
Bytes	236049545	903715773
Cells	4453765	0
HEC Errors	N/A	0
Mgmt Cells	3	2
CLP0 Cells	4453765	17051241
CLP1 Cells	0	0
Errors	0	0
Misrouted Cells	N/A	0

Status information of ATM cells. This page contains information that is dynamic and will refresh every 2 seconds.

Reset Counters: This button resets the ATM Status counter.

ATM Status Fields: Tx Bytes, Rx Bytes, Tx Cells, Rx Cells, Rx HEC Errors, Tx Mgmt Cells, Tx CLP0 Cells, Rx CLP0 Cells, Tx CLP1 Cells, Rx CLP1 Cells, Rx Errors, Tx Errors, and Rx Misrouted Cells.

PPP Status



The PPP Status page shows the status of each PPP session for each PPP interface. This page contains information that is dynamic and will refresh every 8 seconds.

Connection Name: This is user defined. User defined connections for PPP can be created in PPP Configuration page.

Interface: States the interface that is being used.

Mode: There are two available modes for the connection, PPP over Ethernet (PPPoE) & PPP over ATM (PPPoA)

Status: States whether PPP connection is Connected or Not Connected.

Packets Sent: Number of packets sent over the PPP Connection.

Packets Received: Number of packets received by the PPP Connection.

Bytes Sent: Number of bytes sent by a particular PPP Connection.

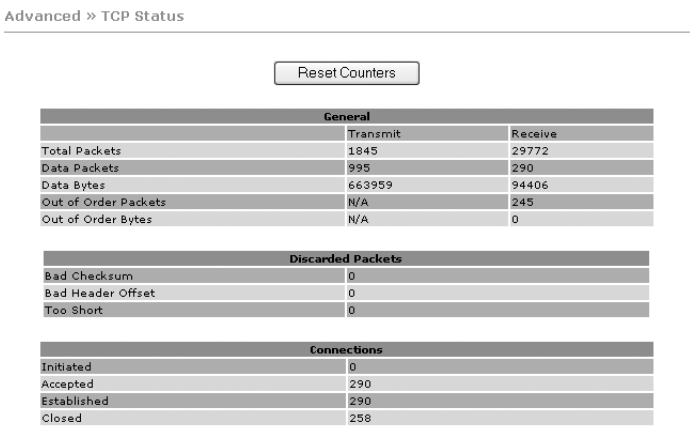
Bytes Received: Number bytes received by a particular PPP Connection.

Connect and Disconnect: Manually connect/disconnect the PPP connection.

Connection #: Specifies the PPP session to be connected/disconnected.

Connect/Disconnect Execute: Press this button to connect or disconnect.

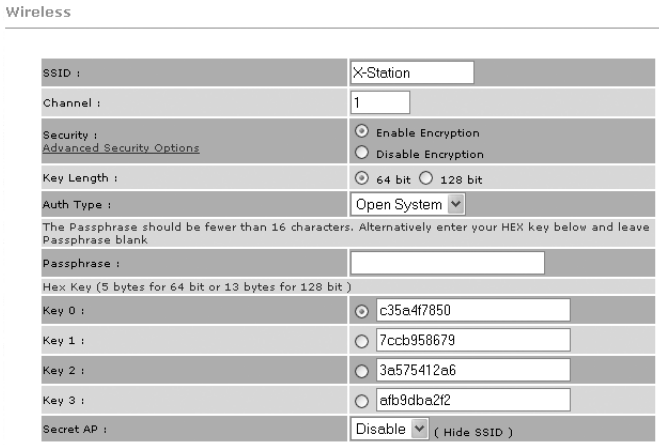
TCP Status



TCP/IP Network Statistics

Diagnostic information provided for troubleshooting networking. You may be asked for information from this status window when talking to your ISP or ADSL Nation support staff.

Wireless



SSID: The Service Set Identifier (SSID) is a unique name for your wireless network. The SSID can be up to 31 characters. The default is “X-Station” and can be kept unless there are other X-Stations in range. If other X-Stations are in range the SSID must be changed to a unique name to prevent interference from other X-Stations.

Channel: Select a channel between 1 and 14. As wireless equipment becomes more popular there is a chance that your neighbours will have similar wireless equipment. If you experience poor wireless performance try selecting a different wireless channel to reduce interference from other wireless equipment. All access points and wireless adaptors sharing the same network must share the same channel to interoperate.

Security: The X-Station provides a security encryption feature known as WEP (Wired Equivalent Privacy). WEP is designed to provide security and privacy on a wireless network. This is done by encrypting the data sent between client and host with an encryption key. Both the client and the X-Station must have the same WEP key in order to communicate.

In order to simplify the initial set-up the X-Station has the encryption feature disabled. We advise that this feature should be enabled if you wish to prevent unorthorized access to your wireless network.

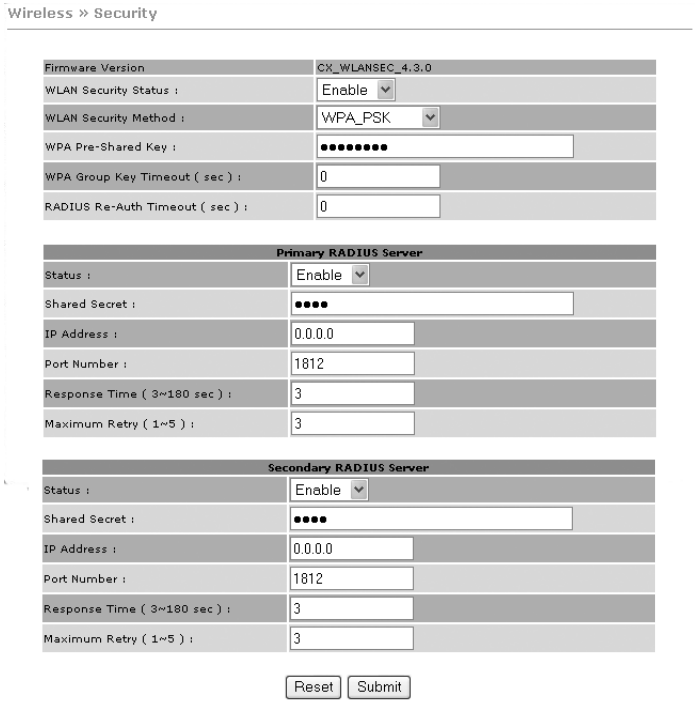
Key Length: Choose between 64-bit (default) and 128-bit. The higher the bit value on the encryption, the more secure the data transmission. 128-bit offers more security, but at the cost of slower data processing.

Wireless

Key 0 ~ 4: You are able to enter 4 encryption keys, only one of which is enabled at any given time. All devices on the network must share the selected key in order to communicate with the X-Station. The key length for 64-bit is 10 hexadecimal characters and the key length for 128 bit is 26 hexadecimal characters. Hexadecimal characters are the numbers 0-9 and letters A-F.

Note: If you have the WLAN Security (see next section) enabled, always choose WEP Key ID 2. This will allow the 802.1x client and non-802.1x client to work simultaneously in the 802.1x WLAN security Method.

Wireless Security



Security Options

Firmware Version: Wireless security firmware installed on the X-Station.

WLAN Security Status: Enable/disable WLAN Security.

WLAN Security Method: There are three available methods of WLAN Security:

(802_1X) This option uses 802.1X for authentication with the RADIUS server while using WEP encryption.

(WPA RADIUS) This option uses 802.1X for authentication with RADIUS server while using TKIP encryption.

(WPA PSK) This option uses a pre-shared key for authentication while using TKIP encryption.

Wireless Security

WPA Pre-Shared Key: This is the pre-shared key for use in WPA PSK security method.

WPA Group Key Timeout (sec): This is the time-out value for the WPA Group Key.

RADIUS Re-Auth Timeout (sec): When this value is timed out, 802.1X will re-authenticate every associated client.

Note: With WLAN Security enabled, select “Enable Encryption” and choose WEP Key ID 2 on the Wireless Page (see previous section). This will allow the 802.1x client and non-802.1x client to work simultaneously in the 802.1x WLAN security Method.

Radius Server

The X-Station can retrieve passwords from an external RADIUS server rather than storing the password locally on the X-Station. This is useful in corporate networks where a central RADIUS authentication is used to control remote access to the network. Two RADIUS servers can be configured primary/secondary as required.

Status: This is the status of the primary RADIUS server.

Shared Secret: This is the password shared between an 802.11 access point and the RADIUS server.

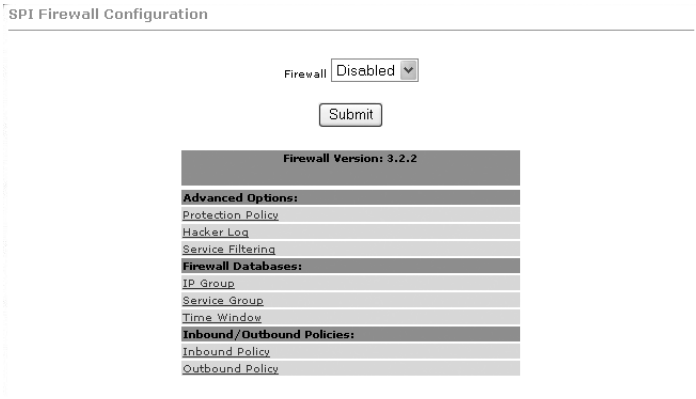
IP Address: This is the IP address of the RADIUS server.

Port Number: This is the UDP port of the RADIUS server.

Response Time (3~180 sec): This is the amount of time the X-Station will wait before it retries.

Maximum Retry (1~5): This is the maximum amount of retry attempts to connect to the RADIUS server before the server responds with and “Authentication failure” message.

Firewall

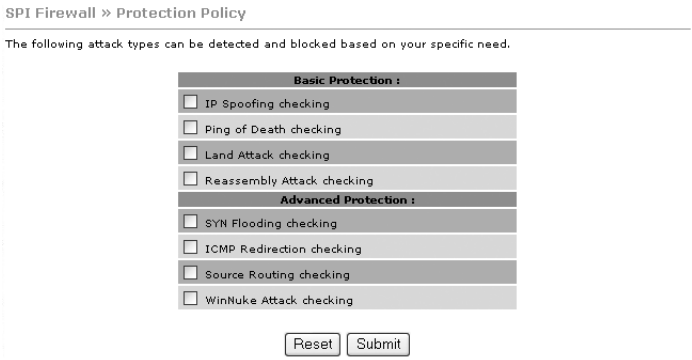


A firewall is a method of implementing user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

By default the X-Station is configured to use NAT as a basic firewall and the advanced SPI firewall is disabled. The basic NAT firewalling offers adequate protection for most users but increased security is available by enabling the advanced SPI firewall. The SPI firewall is disabled by default because it may be considered a complicated extra to users who have no previous experience of firewalls. This User Guide will briefly cover each feature for experienced firewall users, people new to firewalls are advised to visit http://www.adslnation.com/support for more detailed help and advice with configuring the firewall.

This screen allows the firewall to be enabled/disabled and provides access to all of the various option screens.

Firewall Protection Policy



Protection Policies defend against common methods of attacking a network and computers within the network. Some of these attacks are classified as a DoS (Denial of Service). DoS, is an attack in which a network or components of a network are disabled, usually by overloading traffic on the network, in order to prevent authorized and legitimate users to access network resources.

Basic Protection

IP Spoofing checking: IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network.

Ping of Death checking: Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly.

Land Attack checking: Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). Since the source and the destination are the same, the victim receives the request it just sent out. The received data does not match what the victim is expecting, so it re transmits the request. This process repeats until the network crashes.

Reassembly Attack checking: Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. In Reassembly Attack, the sub-packets have malformed criteria (Fragment offset), which can easily cause a system to crash, freeze, or reboot.

Firewall Protection Policy

Advanced Protection

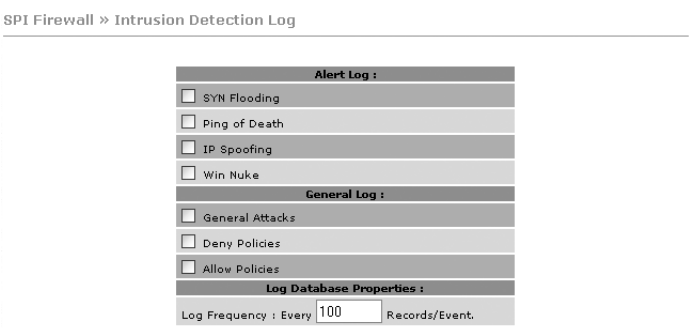
SYN Flooding checking: SYN Flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYNchronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (Many) of these attacks are sent simultaneously, the server will probably overload and crash.

ICMP Redirection checking: Also known as an ICMP storm attack or smurf attack, ICMP Redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network.

Source Routing checking: Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about nodes in a network, making it easy to exploit any weakness.

WinNuke Attack checking: WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of-Band) data that Windows is unable to process, causing the target computer to crash.

Firewall Intrusion Detection Log



Configure which Protection Policy (See previous section) violations to log for admin viewing.

Alert Log

"Enabled/Disabled" for SYN Flooding, Ping of Death, IP Spoofing, and Win Nuke (All of these are explained in the previous section). Enable to log violations of individual policies.

General Log

Deny Policies: Enabling this will add Deny Policy violations to the log. Deny Policies are discussed later in the Inbound/Outbound policy section.

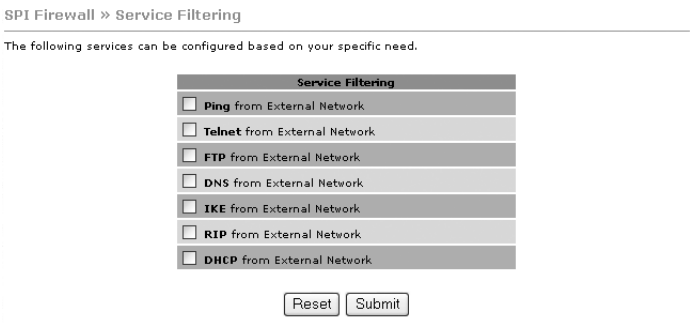
Allow Policies: Enabling this will add Allow Policy acceptances to the log.

Allow Policies: Discussed later in the Inbound/Outbound policy section.

Log Database Properties

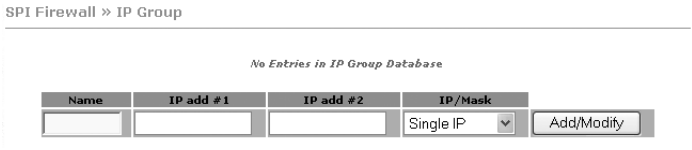
Log Frequency: This field lets you specify how many records to keep of each event. Default is 100. Range for Log Frequency Field is 1 ~ 65535.

Firewall Service Filtering



Service filtering disables service requests from external sources.

Firewall IP Group



The “IP Group” lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

IP Entry Name: This is the name you assign to the group of IP addresses and subnet masks. The IP Entry Name can be up to 19 characters.

IP addr. 1: This is the IP address or subnet mask you are specifying when creating a group.

IP addr. 2: This field is only active if you select to group a range of IP addresses or subnet masks, in which case this is the end address of that range whereas the “IP addr 1” is the first address of that range.

IP/Mask: This field allows you to specify the address type assigned to the group.

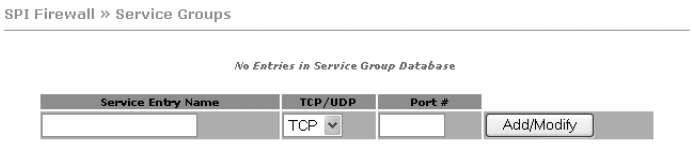
(Single IP) This will let you specify one IP address for a given group.

(IP Range) This will let you specify a range of IP addresses for a given group, starting with “IP addr 1” and ending with “IP addr 2”.

(Subnet Mask) This will let you specify a range of subnet masks for a given group.

ADD/MODIFY: Click “ADD/MODIFY” button to “ADD” or “MODIFY” the corresponding policy.

Firewall Service Group



The “Service Group” lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.

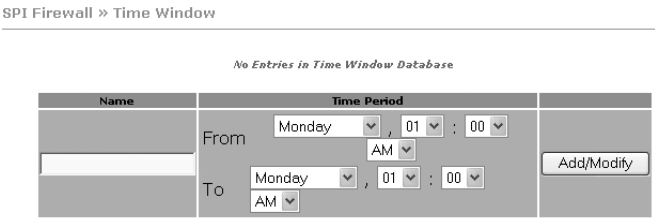
Service Entry Name: This is the name you assign to the group containing the port number. The Service Name Entry can be up to 19 characters.

TCP/UDP: This specifies whether the port goes through TCP or UDP.

Port #: This is the port number associated with the group name.
Range for Port # is 1 ~ 65535.

ADD/MODIFY: Click “ADD/MODIFY” button to “ADD” or “MODIFY” the corresponding policy.

Firewall Time Window



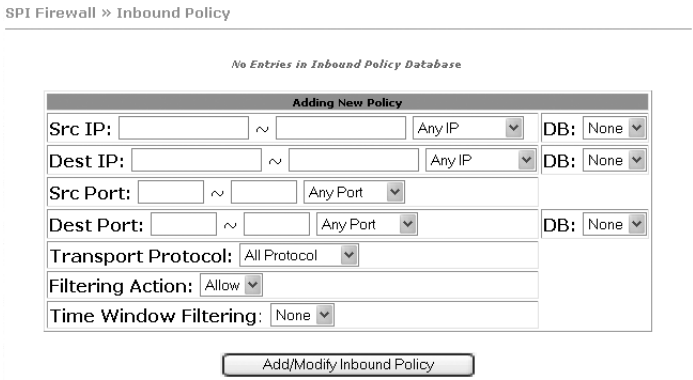
The “Time Window” lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

Time Window Name: This is the name you assign to the group that is given the time designation. The Time Window Name can be up to 19 characters.

Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

ADD/MODIFY: Click “ADD/MODIFY” button to “ADD” or “MODIFY” the corresponding policy.

Firewall Inbound Policy



The “Inbound Policy” allows you to filter inbound (From the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security.

A table of inbound policies is displayed with the following information. If there are no policies, then a message stating “No Entries in Inbound Policy Database” will be displayed in place of the table.

IP Address: The IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: Specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act.: Short for action, this specifies actions: “Allow” or “Deny”.

Opt. Filtering: Optional Filtering specifies the time period to which the policy applies.

Up: Moves the corresponding policy up one space in the table.

Dn: Moves the corresponding policy down one space in the table.

Note: The Inbound Policy works in a Top-Down fashion according to the Inbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom.

Firewall Inbound Policy

Add/Modify Inbound Policy

Clicking this button will bring up a table with all the add configurations as shown in figure above.

Src IP: This specifies the Source IP for the Inbound Policy. This is the external IP address or addresses and Subnet Masks that will be affected by the policy.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and network that will be affected by the policy.

Src Port: This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy.

Safe Ports: Any port greater than 1024 (1025 ~ 65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

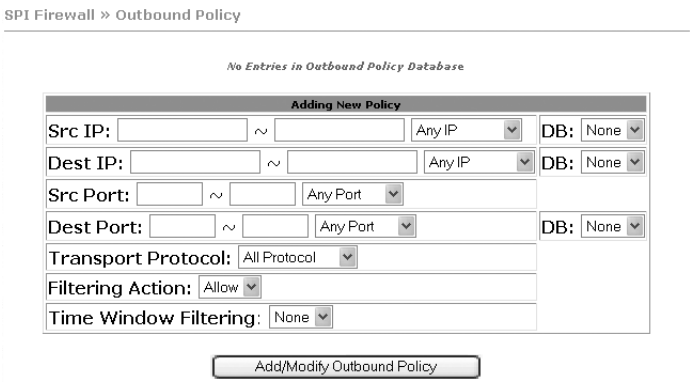
Filtering Action: This specifies what action the policy takes:

(Allow) Allows packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP.
(Deny) Denies packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP.

Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active.

DB: Select a user-defined IP Group for the Src IP and Dest IP fields and a user-defined Service Group for the Dest Port.

Firewall Outbound Policy



The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security.

A table of outbound policies is displayed with the following information. If there are no policies, then a message stating “No Entries in Outbound Policy Database” will be displayed in place of the table. Click, “ADD INBOUND POLICY” to add the corresponding policy.

IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act.: Specifies two possible actions: “Allow” and “Deny”.

Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.

Up: Clicking on this button will move the corresponding policy up one space in the table.

Dn: Short for down, clicking on this button will move the corresponding policy down one space in the table.

Firewall Outbound Policy

Add/Modify Outbound Policy

Clicking this button will bring up a table with all the add configurations as shown in figure above:

Src IP: This specifies the Source IP for the Outbound Policy. This is the internal IP address or addresses and Subnet Mask(s) that will be affected by the policy.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the external IP address or addresses and network that will be affected by the policy.

Src Port: This specifies the Source Port for the Inbound Policy. This is the internal port(s) that will be affected by the policy.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal Port that will be affected by the policy. See Src Port above for configuration detail.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

Filtering Action: This specifies what action the policy takes:

(Allow) Selecting this will cause the policy to allow packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

(Deny) Selecting this will cause the policy to deny packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active.

DB: Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and a user-defined Service Group for the Dest Port. User defined IP and Service Groups are created in IP Group and Service Group pages respectively.

Frequently Asked Questions

Q: 'The page cannot be displayed' is prompted when I launch my browser.
A: Ensure that you are using the Ethernet Network cable that comes with your X-Station package to connect to the Modem. Restart your computer and try to launch your browser again. If the problem persists, please contact our support line.

Q: The ADSL Link light keeps on blinking consistently.
A: Ensure that your ADSL line has been activated by the Service Provider. Ensure that you have connected the telephone cable properly and that all telephone equipment is filtered. If the problem persists, first try removing all telephone equipment and test the modem on it's own. If the light still continues to flash please contact the ADSL Service Provider.

Q: The ADSL link light is on. But I am unable to connect to the internet.
A: Run the diagnostics, Ensure that you have entered the correct username and password, enter and re-submit the username and password.

Support

To get product support or obtain further information and documentation, go to http://www.adslnation.com/support.

If you would like to contact technical support by telephone, please call
0845 125 9426 (calls charged at local rate)
01865 761114 (calls charged at operators standard national tariff)
Technical support is available 9am - 6pm weekdays.