4200 Series
Converged Network Appliance

User Manual

Edgewater Networks, Inc.
2730 San Tomas Expressway
Suite 200
Santa Clara, Ca. 95051
Phone: 408.351.7200
info@edgewaternetworks.com

Part Number: 500-10000-001, v2.0, 8-22-03.

Export Notice
This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or re-export may be required by the U.S. Department of Commerce.

Regulatory Compliance
This product was tested to comply with FCC standards for home and office use.

Licensing
Use of this product is subject to Edgewater Networks Software License Agreement.

Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

See *Appendix E: License Information* for more information regarding licenses.

Table of Contents

Chapter 1: Introduction

Thank you for the purchase of your 4200converged network appliance.

This User's Guide describes the 4200 converged network appliance. This document introduces the major features of the 4200 and describes how to perform physical installation and system configuration. This User's manual is intended for network installers, network operators, and security officers.

Typographic conventions

Steps in any particular task are presented using an alphabetized list as follows:

A.
B.
C.

User input is displayed in **boldface** type and can represent either keyboard input or mouse selections in a browser window depending on the context.

Web GUI menus and input areas are called out using *italics.*

Informational statements are denoted using the  symbol and are presented using green type.

WARNING statements are denoted using the  symbol and contained inside of grey text boxes using red type.

The 4200 Converged Network Appliance

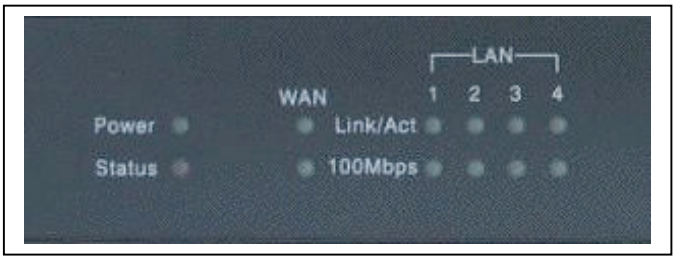
The 4200 is a new generation of edge device providing the demarcation point for real-time, interactive IP services. It is the ideal solution for connecting enterprise PCs and IP Phones to a private or public IP network. It replaces multiple standalone systems by integrating voice-over-IP (VoIP), network security, traffic management and voice call quality monitoring into a low-cost, easily managed device.

Use the 4200 to ensure high quality voice calls, maximize WAN link utilization for data traffic and protect the enterprise LAN from network based attacks.

Features

- Resolves NAT/firewall traversal problems for VoIP by providing a VoIP application layer gateway (ALG) that supports SIP, MGCP, SCCP and H.323
- Supports for 2 to 50 concurrent VoIP calls
- Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for both voice and data traffic
- Provides NAT and PAT for voice and data
- Performs static IP routing
- Performs traffic management including prioritization, classification, queuing, TOS bit setting and call admission control for voice
- Provides voice call quality monitoring and testing
- Provides integrated test tools to facilitate problem isolation
- Provides a DHCP server for enterprise PCs and IP phones
- Performs TFTP relay for IP phone images
- Uses a simple web based GUI for configuration and management
- Supports logging to external syslog servers and interfaces to network management systems using SNMP

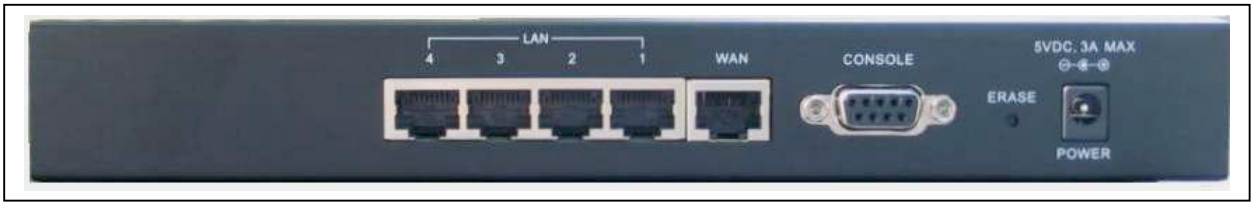
Front Panel LEDs



The LEDs display real-time information for key functions of the 4200. They are as follows:

LED Label	Activity	Description
Power	On	5 volts DC power is supplied to the unit
Status	On	A system fault condition has been detected. Please contact Edgewater technical support.
WAN Link/Act	Flashing	Indicates data traffic sent/received by appliance on the WAN
LAN Link/Act	Flashing	Indicates data traffic sent/received by appliance on the LAN
100Mbps	On	Indicates ethernet link rate of 100Mbps

Back Panel



The back panel of the 4200 contains the following:

- Power connector
- LAN Ethernet ports
- WAN Ethernet port
- Erase switch
- Serial console port

Power Connector

The 4200 comes with an AC power cord and 5vdc, 3.0 Amp power adapter for connecting to this port.

LAN Ethernet port

The 4200 series LAN interface is a 4-port switch that uses a single IP address. The LAN Ethernet ports are 10/100 auto sensing ports that should be connected to IP phones, IADs or PCs installed on the local area network (also known as the private network).

WAN Ethernet port

The WAN Ethernet port is a 10/100 auto sensing port that should be connected to the wide area network (also known as the public network) through a WAN termination device such as an xDSL modem or router

Erase Switch

To erase any custom configuration and restore the 4200 to its factory default state depress the erase button once, wait for the LEDs to illuminate and press again before 2 seconds expires.

WARNING: Using the Erase switch as outlined above means any configuration made to the 4200 will be lost. Additionally the VoIP ALG registration code must be re-entered in the 4200 as covered in *Chapter 4: System Diagnostics, viewing the ALG registration code*. Erasing the configuration means that IP phones installed behind the 4200 will not work and Internet connectivity or network access for PCs will be down until the system is reconfigured.

Serial Console Port

This port is used to establish a local console session with the 4200 using a VT100 terminal or emulation program. The baud rate is 9600. It is used for debug or local diagnostic purposes only. Primary configuration of the 4200 is performed from a web browser as covered in "Chapter 3: Configuring the 4200".

Chapter 2: Getting Started

Physical Installation

The 4200 is designed for either desktop or wall mount installation. Please observe the following guidelines when installing the system:

- Never assume that the AC cord is disconnected from a power source. Always check first.
- Never place objects greater than 5 lbs on top of the 4200 as damage to the chassis may result.
- Always connect the AC power cord to a properly grounded AC outlet to avoid damage to the system or injury.
- Ensure that the physical location of the installation has adequate air circulation and meets the minimum operating conditions as provided in the environmental specifications for the system. These can be found on our website at www.edgewaternetworks.com.

Desktop Installation

A. Remove the 4200 and accessories from the shipping container.
B. Place the 4200 on a flat, dry surface such as a desktop, shelf or tray.
C. Connect the power and network cables to the appropriate ports on the back of the system.

Wall-Mount Installation

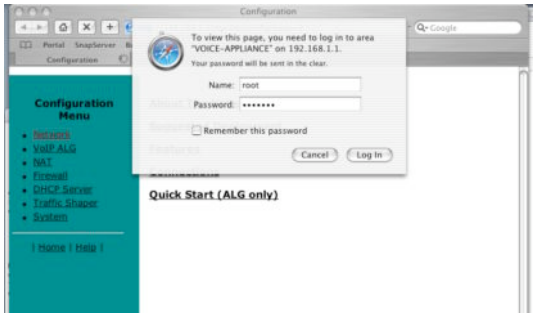
The 4200 can be wall-mounted using the two mounting brackets on the bottom of the appliance. We recommend using two round or pan head screws.

A. Install two screws 5 14/16″ horizontally apart on a wall or other vertical surface. The screws should protrude from the wall so that you can fit the appliance between the head of the screw and the wall.
B. If you install the screws in drywall use hollow wall anchors to ensure that the unit does not pull from the wall due to prolonged strain from the cable and power connectors.
C. Remove the 4200 and accessories from the shipping container.
D. Hang the 4200 on the wall.
E. Connect the power and network cables to the appropriate ports on the back of the system.

WARNING: Secure the power supply using a fastener or nearby shelf so that it does not hang from the power connector.

Connecting to the 4200

The 4200 is configured using a web browser such as Internet Explorer or Netscape Navigator. The 4200is shipped with a pre-configured IP address for its LAN port of 192.168.1.1. To connect to the 4200, do the following:



A. Connect a PC using an IP address of 192.168.1.2 and subnet mask of 255.255.255.0 to one of the 4200 LAN ports.
B. Launch a web browser on the PC and enter the URL string: **192.168.1.1**. Press **Return**. The initial 4200*main configuration* menu appears.
C. Select the **Network** link - enter the username **root** and the password **default** to log into the system.
D. Continue to configure the system using the information provided in "Chapter 3: Configuring the 4200".

Chapter 3: Configuring the 4200

The 4200 is a flexible, easy to use converged network appliance that provides many critical networking functions for IP based voice and data. It can be installed in several different VoIP topologies:

- At the customer premise for IP Centrex applications
- At the station side of enterprise IP PBXs
- At the trunk side of enterprise IP PBXs

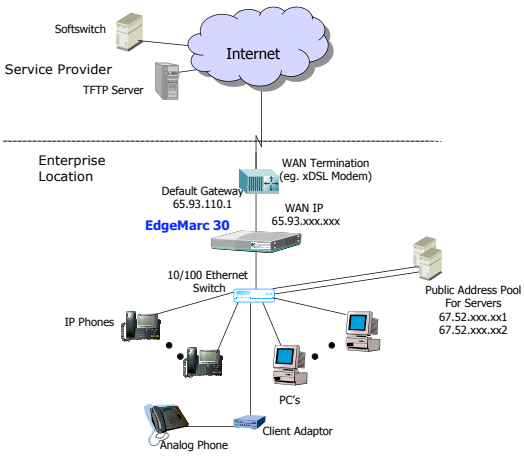
Most users will follow the steps provided in the "Configuring The Systems Settings" section of this manual to initially connect the 4200 into their IP network. The remainder of the configuration can be different based on the application, VoIP topology and presence of other networking equipment such as firewalls or DHCP servers. In general, however, the steps used to configure the 4200 are:

Step	Task
1	System configuration
2	VoIP configuration
3	Data networking configuration
4	Firewall configuration
5	Traffic management configuration

Some of the steps are optional depending on your particular application. We have provided configuration guidelines below for each of the application types supported by the 4200. Additional application notes can be found on our website at www.edgewaternetworks.com.

Configuration Guide For IP Centrex Applications

A typical 4200installation for an IP Centrex application uses an external router, xDSL or cable modem to terminate the WAN link from the service provider. The 4200is then connected directly to the WAN termination device and the LAN port of the 4200is connected to the 7enterprise ethernet local area network (typically a layer 2 switch). VoIP signaling is performed in the service provider network via a softswitch and the 4200 acts as a proxy for the voice devices installed in the enterprise LAN. In this configuration a single public IP address is used to proxy for all of the IP phones and to route to multiple PC's installed on the LAN. This particular example also uses static NAT entries to route to the publicly addressable servers. The 4200 performs the following functions in this application:



- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the

same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.

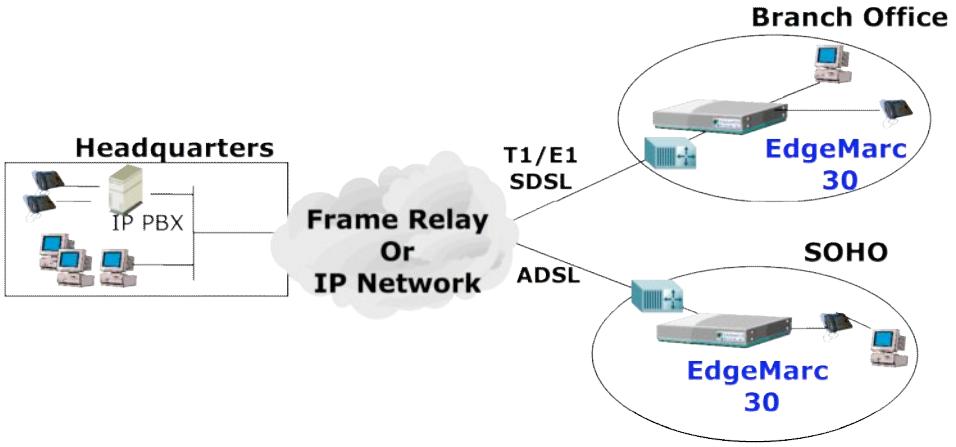
- NAT/PAT translation for IP phones and PC's. This allows a single public IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PC's.
- Static NAT entries. This enables the customer to use a WAN public IP address for data servers (web, mail, ftp, etc.) connected behind the 4200. These servers can then be configured with private IP addresses for additional security.
- A "VoIP" aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new calls and then return the equivalent of a "fast busy" to new call requests.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PC's. This also includes VoIP signaling gateway information (MGCP, SIP, H.323 and SCCP).
- Call quality monitoring and test tools.

Configuration Outline

Task	Subtask	Configure For IP Centrex Application?
System Configuration	configure LAN/WAN interface	**Yes**
	set ethernet link rate	Optional
	enable the DHCP server	Optional but recommended
	configure SNMP	Optional
VoIP Configuration	enable the VoIP ALG	**Yes**
	configure a VoIP subnet route	Optional
Data Networking Configuration	dynamic NAT	Optional but recommended
	static NAT	Optional
	static IP routing	Optional
Firewall Configuration	enable the data firewall	**Yes**
	configure basic settings	Optional
	configure advanced settings	Optional
Traffic Management Configuration	enable traffic shaping	**Yes**
	enable Call Admission Control	**Yes**

Configuration Guide For Station Side IP PBX Applications

Most private enterprise VoIP networks use an IP PBX at the corporate headquarters location to provide voice switching between headquarters, branch offices and the PSTN. The 4200 is used in these environments to securely connect branch office employees to the IP PBX installed in the corporate headquarters location.



The installation of an 4200 on the station side of an enterprise IP PBX is very similar to the IP Centrex application above. The branch office is connected to the corporate network using VPNs or private T1 links terminated by a WAN router. The 4200is then connected directly to the WAN router and the LAN port of the 4200is connected to the enterprise ethernet local area network (typically a layer 2 switch). The IP PBX in the corporate headquarters location performs VoIP signaling and the 4200 acts as a proxy for the voice devices installed at the branch office. The 4200 can perform the following functions in this application:

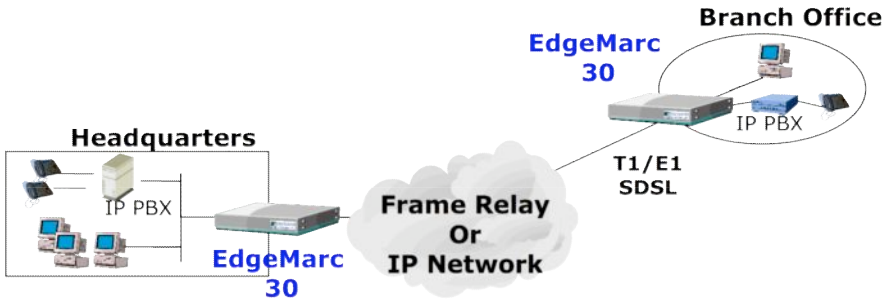
- WAN/LAN IP routing.
- Traffic shaping and priority queuing to guarantee high quality voice traffic. These mechanisms protect voice and data traffic from contending for the same network resources to guarantee low latency and the highest call quality possible for VoIP traffic. At the same time they ensure the best utilization of WAN bandwidth by enabling data traffic to burst up to full line rate in the absence of voice calls. Precedence is given to traffic for the range of addresses reserved for the IP phones.
- NAT/PAT translation for IP phones and PC's. This allows a single IP address to be used on the WAN link to represent all of the private IP addresses assigned to the LAN IP phones and PC's.
- A "VoIP" aware firewall. A full layer 7 gateway for voice traffic and a stateful packet inspection firewall for data traffic.
- Call Admission Control (CAC). CAC uses a deterministic algorithm to decide when there are insufficient network resources available to adequately support new calls and then return the equivalent of a "fast busy" to new call requests.
- DHCP server and TFTP relay. These features are used to simplify and expedite the IP configuration of phones and PC's. This also includes VoIP signaling gateway information (MGCP, SIP, H.323 and SCCP).
- Call quality monitoring and test tools.

Configuration Outline

Task	Subtask	Configure For Station Side IP PBX Application?
System Configuration	configure LAN/WAN interface	**Yes**
	set ethernet link rate	Optional
	enable the DHCP server	Optional but recommended
	configure SNMP	Optional
VoIP Configuration	enable the VoIP ALG	**Yes**
	configure a VoIP subnet route	Optional
Data Networking Configuration	dynamic NAT	Optional but recommended
	static NAT	Optional
	static IP routing	Optional
Firewall Configuration	enable the data firewall	**Yes**
	configure basic settings	Optional
	configure advanced settings	Optional
Traffic Management Configuration	enable traffic shaping	**Yes**
	enable Call Admission Control	Optional

Configuration Guide For Trunk Side IP PBX Applications

Companies using shared WAN links for inter-office IP voice communications can use the 4200 as a traffic shaper to meet the stringent jitter, latency and packet loss requirements for toll quality voice. The 4200 is deployed in the network between WAN and LAN connections in headquarters and branch office locations. One appliance is required for each end of a WAN link and they are installed logically between IP PBX trunk interfaces.



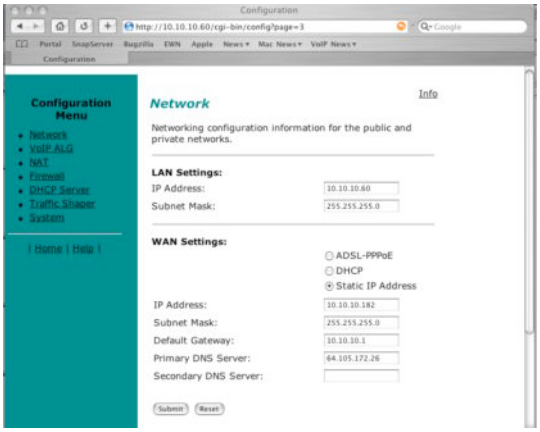
The 4200 performs WAN/LAN IP routing and traffic management functions in this application.

Configuration Outline

Task	Subtask	Configure For Trunk Side IP PBX Application?
System Configuration	configure LAN/WAN interface	**Yes**
	set ethernet link rate	Optional
	enable the DHCP server	Not required
	configure SNMP	Optional
VoIP Configuration	enable the VoIP ALG	Not required
	configure a VoIP subnet route	Not required
Data Networking Configuration	dynamic NAT	Not required
	static NAT	Not required
	static IP routing	Not required
Firewall Configuration	enable the data firewall	Not required
	configure basic settings	Not required
	configure advanced settings	Not required
Traffic Management Configuration	enable traffic shaping	**Yes**
	enable Call Admission Control	Not required

System Configuration

This section explains how to configure the 4200 to function in your IP network. You will configure the ethernet interfaces, network addresses, DNS settings, default gateway, SNMP settings and change the administrative password.



Configure the WAN interface

A. Select the **Network** link.
B. Select **Static IP address** if you want to manually assign the IP address configuration to the WAN interface.

1. Enter the **IP Address.**
2. Enter the **Subnet Mask** (egg. 255.255.255.0).
3. Enter the **Default Gateway**. Packets destined for IP networks not known to the 4200 are forwarded to the default gateway for handling.
4. Enter the **Primary DNS Server**. The DNS server is used by the 4200 to resolve domain names to IP addresses. The value entered into this field is provided to IP devices that use the 4200 as a DHCP server. The 4200 VoIP ALG also uses it if domain names are used instead of IP addresses to identify signaling and/or TFTP servers (see the section entitled "Configuring the VoIP ALG" for more details).
5. Enter the **Secondary DNS Server**. This server will be used in the event that the primary DNS server is not reachable.
6. Press **Submit**.

C. Select **ADSL-PPPoE** if you are connecting to the Internet using an ADSL link. The WAN IP address for the 4200 is provided by your service provider as a part of the PPPoE protocol automatically and does not have to be manually configured. Please contact your service provider for the PPPoE username and password as this will be required for link authentication. PLEASE note: The 4200 uses PAP authentication and you should inform your provider that this is required to ensure compatibility.

1. Press **Submit**.
2. Enter the **User Name** and **Password**.
3. Press **Submit**. The service provider will automatically assign your WAN IP address.

D. Select **DHCP** if you want to receive your WAN IP address from a DHCP server located in the WAN.
E. Press **Submit**.

Configure the LAN interface

A. Select the **Network** link.

B. Enter the **IP Address**.
C. Enter the **Subnet Mask** (e.g. 255.255.255.0).
D. Press **Submit**.

WARNING: After pressing submit the 4200 will become unreachable until you use a PC with an address on the same subnet as entered in steps B and C above.

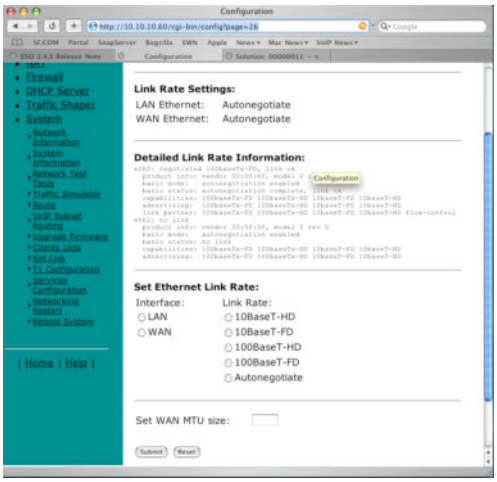
Set Ethernet Link Rate

WARNING: The vast majority of ethernet networking devices including the 4200 use "autonegotiate" as a default setting. Chances are that you will not have to set the ethernet link rate as described below. Please use caution if manually configuring the link rate as a speed or duplex mismatch will result in a loss of connectivity.

If needed configure the rate of the physical ethernet port on the 4200. The default setting for the Ethernet port is to "autonegotiate" both the link speed and duplex with locally attached devices.

A. Select **System**.
B. Select **System Overview**.
C. Select **Set Link Rate**.
D. Select **LAN** and/or **WAN**.
E. Select the appropriate link rate for your ethernet network:

   10baseT-HD = 10Mbits per second using half duplex transmission
   10baseT-FD = 10Mbits per second using full duplex transmission
   100baseT-HD = 100Mbits per second using half duplex transmission
   100baseT –FD = 100Mbits per second using full duplex transmission
   Autonegotiate = The 4200 will autonegotiate link rate and duplex with the directly attached device.



F. Press **Submit**.

Set WAN MTU size

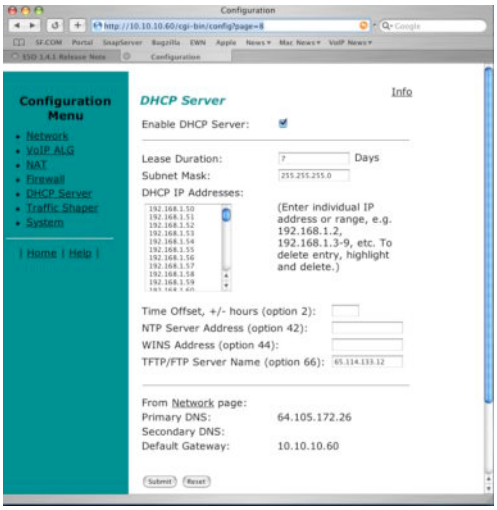
The WAN MTU size may be set to reduce the latency that is introduced when large data packets are sent over a slow link. The default setting is 1500 bytes for static IP addresses. PPPoE links negotiate the value automatically although the value can be overridden using this field. If the WAN Upstream Bandwidth is less than 256 Kbit/s, the MTU size is automatically reduced to 800 bytes.

WARNING: When manually configuring the MTU size we recommend that you use a setting of 800 bytes or greater. You may experience problems with certain types of VoIP traffic if the MTU size is set

below 800 bytes.

A. Select **System**.
B. Select **System Overview**.
C. Enter the **WAN MTU size**
D. Press **Submit**.

Configure the DHCP Server



The 4200 can act as a DHCP server granting IP addresses to PCs, workstations, servers or voice devices (IP phones, IADs or softphones). DHCP is a protocol that enables IP devices to obtain temporary or permanent IP addresses (out of a pool) from centrally administered servers. The user can configure blocks of IP addresses, a default gateway, DNS servers, NTP server address, Time offset from NTP value, WINS address and TFTP/FTP server name that can be served to the requesting IP devices. In addition the 4200 will provide its LAN IP address in DHCP user options 150 and 151 for use by IP phones. Some IP phones use these values for configuration of their TFTP server and MGCP control server addresses.

PLEASE note: The DHCP server in the 4200 should not be used if a DHCP server already exists in the same subnet as the 4200. Also, it is recommended that you assign static IP addresses for common-access devices such as network printers or fax machines.

A. Select **DHCP Server**.
B. The default value for the DHCP server is **enabled**.
C. Enter the **Lease Duration**.

The lease duration is the amount of time in days that an IP device may use an assigned IP address before requesting that it be renewed. The default value is 7 days and the valid range of input is 1 to 30 days.

D. Enter the **Subnet Mask**.

This is the subnet mask that will be sent via DHCP to the requesting IP devices.

E. Enter the **DHCP IP Addresses**.

This is the pool of IP addresses that will be provided to the requesting IP devices. You can enter both individual IP addresses or a range of addresses using the following format:

192.168.1.3-5

where 192.168.1.3 is the starting address and 192.168.1.5 is the ending address.
PLEASE note: The range format can only be used for class C addresses.

F. Enter the **Time Offset (DHCP user option 2)**.

Set the time offset in hours from UTC for your local location.

G. Enter the **NTP Server Address (DHCP user option 42)**.

This is the IP address of your NTP server.

H. Enter the **WINS Address**.

PLEASE note: If you are not using WINS this field may be left blank.
The Windows Internal Naming Service (WINS) is a service that keeps a database of computer name-to-IP address mappings so that computer names used in Windows environments can be mapped to IP addresses. The WINS Address is the IP address of the WINS server in your network.

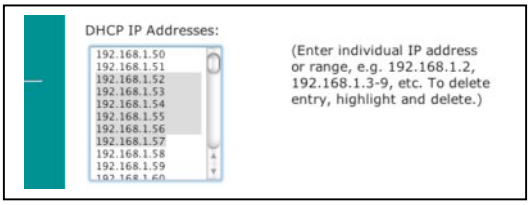
I. Enter the **TFTP/FTP Server Name (DHCP user option 66)**.

Some IP phones use this setting to locate the TFTP or FTP servers which contain the phone software image used during boot. By default this option is the same as the TFTP server on the **VoIP ALG** page.

J. Press **Submit**.

Delete a DHCP IP Address

A. Select **DHCP Server**.
B. To delete an IP address or a range of IP addresses **highlight** the entry in the *DHCP IP Addresses* list and press the **Delete** key on your keyboard.
C. Press **Submit**.

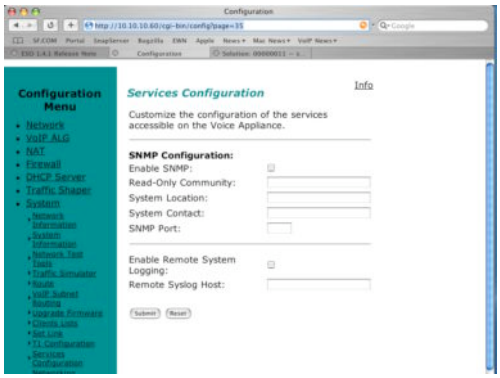


Disable The DHCP Server

A. Select **DHCP Server**.
B. **Uncheck** the *Enable DHCP Server* checkbox.
C. Press **Submit**.

Configure SNMP

The 4200 can be managed remotely by an SNMP network management system such as HP Openview. The 4200 supports SNMPv1 and MIB-II (RFC1213). All MIB-II variables are read only. The MIB variables sysContact and sysLocation are set by the web GUI.



A. Select **System**.
B. Select **System Overview**.
C. Select **Services Configuration**.
D. Select the **Enable SNMP** checkbox.

E. Enter the **Read-Only Community**.

This is the community string that the management station uses when accessing read-only objects from the 4200. The default is 'public'.

F. Enter the **System Location**.

This is a comment string that can be used to indicate the location of the 4200. By default, no value is set.

G. Enter the **System Contact**.

This is the administrative contact information for the 4200. By default, no value is set.

H. Enter the **SNMP Port**.

This is the port that the 4200 uses for SNMP communications with the network management system. The default is 161.

I. Press **Submit**.

Disable SNMP

A. Select **System**.
B. Select **System Overview**.
C. Select **Services Configuration**.
D. **Uncheck** the *Enable SNMP* checkbox.
E. Press **Submit**.

Enable Remote System Logging

The 4200 can be configured to log system messages to an external syslog server.

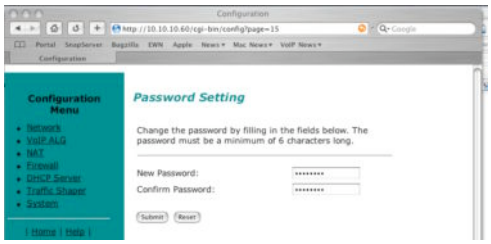
A. Select **System**.
B. Select **System Overview**.
C. Select **Services Configuration**.
D. Select the *Enable Remote System Logging* checkbox.
E. Enter the IP address of the **Remote Syslog Host**.
F. Press **Submit**.

Disable Remote System Logging

A. Select **System**.
B. Select **System Overview**.
C. Select **Services Configuration**.
D. **Uncheck** the *Enable Remote System Logging* checkbox.
E. Press **Submit**.

Change the Administration Password

We strongly recommend that you change the default password for the "root" administrative account using the following steps:



A. Select **System**.
B. Select **changed** in the *Change Password* section of the GUI.
C. Enter the **New Password**.

PLEASE note: the new password must be between 6 and 20 characters in length. Any combination of alpha and numeric characters is accepted.

D. Enter the **password** you chose in step C again in the *Confirm Password* to ensure that there were no mistakes in the initial entry.
E. Press **Submit**.

VoIP Configuration

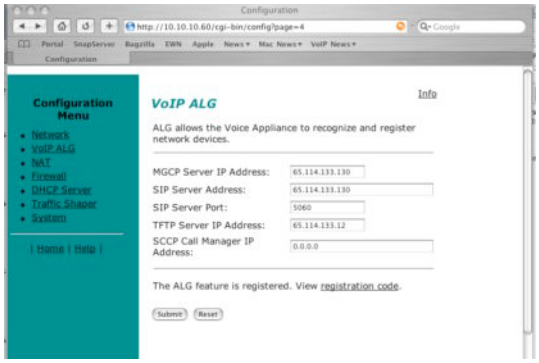
The 4200 provides a VoIP application layer gateway (ALG) for the SIP, MGCP, H.323 and SCCP protocols. The ALG proxies the connection between the VoIP softswitch or IP PBX and voice devices such as IP phones, IADs or softphones. By acting as a proxy the 4200 is able to provide several important functions for IP based voice:

- Provide NAT/PAT services for voice traffic. NAT/PAT for VoIP enables you to use a single public IP address on the WAN interface of the 4200 to represent multiple private IP addresses assigned to voice devices on the LAN. The NAT function maps both IP address and IP port number between the public and private addresses so that all signaling and VoIP media packets are translated. A single public IP address can support up to 253 voice devices.
- Provide security services for voice traffic.
  - NAT/PAT services hide enterprise LAN topology from hackers.
  - The ALG acts as a "voice aware" firewall and ensures only authenticated voice traffic enters the enterprise LAN. This is accomplished by the dynamic provisioning of signaling and media ports for authenticated voice devices. The implementation is stateful and open ports are closed automatically when no longer required to support the voice call.
- Automatically re-register voice devices with the softswitch subsequent to a WAN IP address change. The WAN IP address can change when using WAN DHCP and/or PPPoE. This is a typical combination for ADSL and cable modem links.
- Enable mobility in the enterprise LAN for voice devices. This is useful, for example, when using WiFi or moving office locations. In these instances the IP address of the voice device may be changed.

Configure the VoIP ALG

In order to configure the VoIP ALG the 4200 must be told where to reach the signaling servers and TFTP server on behalf of the voice devices.

A. Select **VoIP ALG**.
B. If you are using MGCP enter the **MGCP Server IP Address**.
C. If you are using SIP enter the **SIP Server IP Address** and **SIP server port**. The SIP server port is the port used by the SIP registrar. The default value is port 5060.
D. If you are using SCCP enter the **SCCP Call Manager IP address**.
E. Enter the **TFTP Server Address**. This address is used to identify the TFTP server that contains the images used by IP phones at boot up. The 4200 performs a TFTP server relay function.

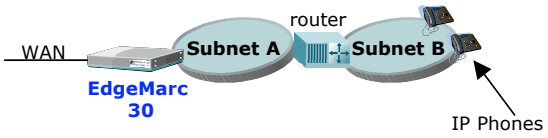


PLEASE note: It is not necessary to program in an FTP server address if your IP phones use the FTP protocol instead of TFTP to retrieve their images. A relay function is not needed for FTP as the 4200 will forward FTP traffic to the destination server as programmed in your IP phone.

F. Press **Submit**.

Configure VoIP Subnet Routing

It is not necessary to configure VoIP subnet routing if all of your voice devices are installed on the same IP subnet as the 4200. In some installations the voice devices are located in different subnets than the 4200 and connected via intermediate routers. In these instances it is necessary to configure a return path in the 4200 by specifying the intermediate router who knows how to reach the voice devices. This router must be reachable by the 4200.



Enter a VoIP Subnet Route

A. Select **System**.
B. Select **System Overview**.
C. Select **VoIP Subnet Routing**.
D. Enter the **IP Network** (egg. 10.10.12.0).

This is the IP address of the remote subnet containing the voice devices.

E. Enter the **Netmask** (egg. 255.255.255.0).

This is the mask of the IP address of the subnet containing the voice devices.

F. Enter the **Gateway** (egg. 10.10.10.2).

This is the IP address of the intermediate router that knows the return path to the remote subnet from the 4200.

G. Press **Submit**.

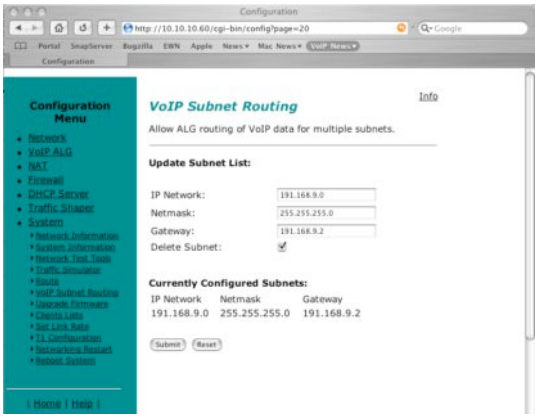
Perform steps A through G for each remote subnet containing the voice devices.
PLEASE note: the 4200 is limited to a total of 20 different VoIP subnets.

Delete a VoIP Subnet Route

A. Select **System**.
B. Select **System Overview**.
C. Select **VoIP Subnet Routing**.
D. Enter the **IP Network** (egg. 10.10.12.0) .

This is the IP address of the remote subnet containing the voice devices.

E. Enter the **Netmask** (egg. 255.255.255.0).



This is the mask of the IP address of the subnet containing the voice devices.

F. Enter the **Gateway** (egg. 10.10.10.2) .

This is the IP address of the intermediate router that knows the return path to the remote subnet from the 4200.

G. Select the **Delete Subnet** checkbox.
H. Press **Submit**.

Perform steps A through H for each remote subnet that you wish to delete.

Configure IP Phones, IADs or Softphones

After configuring the 4200 VoIP ALG the voice devices must be configured to point to the LAN interface of the 4200 as their signaling gateway and optionally as their TFTP server (if they use the TFTP protocol to retrieve their software images). The steps required to setup these devices differ from vendor to vendor. Using the DHCP server included in the 4200 will significantly simplify the setup of these devices if they are able to obtain their IP configuration via DHCP. Please consult the applicable users guide of each device for detailed instructions. For your convenience we have provided the configuration steps for a number of these devices in the support section of our website at: www.edgewaternetworks.com

A sample manual IP phone configuration using a Cisco 7960 with MGCP is provided below.

A. Press **settings**.
B. Scroll down to **Network Configuration** .
C. Press **Select**.
D. Scroll down and enter the following parameters:

IP address =LAN IP address of phone egg 192.168.1.20

Subnet Mask= Subnet Mask of LAN egg 255.255.255.0

TFTP Server = 4200 LAN port IP address= egg 192.168.1.1

PLEASE note: The 4200 does TFTP pass-through to the TFTP server address configured in step E of the "Configuring The VoIP ALG" section of this guide.

Default Router = Default router for data on this subnet. This is usually the LAN ip address of the 4200.

DHCP Enabled = No

E. **Save** the settings.

Note: To reboot your Cisco telephone, press and release the following three buttons simultaneously: "*" + "6" + Settings . Depending on the firmware version in the telephone you may need to "Unlock" the configuration to change a parameter. To unlock the phone, enter * * # on the telephone or by scrolling down the menu options on the phone to the "Unlock Configuration" option.To change a parameter, enter * * # on the telephone.

F. Under settings, select **MGCP configurations**.
G. Set the **Media Gateway Controller address** = the LAN IP address of the 4200 (egg. 192.168.1.1).

PLEASE note: The 4200 forwards signaling messages sent to this address by the phone to the **MGCP Server IP Address** configured in step B of the "Configuring The VoIP ALG" section of this guide.

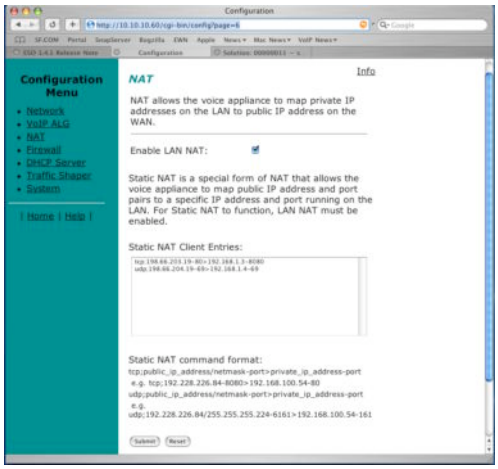
H. **Save** and **Reboot** the telephone.

The phone should now register with the 4200. To complete the installation a one-time activation code may be required by the network based softswitch or IP PBX. Please consult your service provider or IT administrator for additional information.

Data Networking Configuration

The 4200 provides static IP routing and two types of Network Address Translation (NAT) functions for data traffic. This chapter explains the use and configuration of these features.

NAT for Data Traffic



NAT allows hosts on a private internal network (the LAN side of the 4200) to anonymously communicate with devices on an external network (the WAN side of the 4200). The 4200 with NAT enabled will re-write outbound packet headers using public IP addresses in place of private IP addresses so that the private IP addresses are not exposed to the external network. Additionally, the ports used by the IP addresses are also changed as they traverse the 4200. This is known as Port Address Translation(PAT) and provides an additional security measure. The 4200 maintains a table of these mappings so that return packets can be forwarded to the correct host on the private network.

The 4200 provides two types of NAT functions: dynamic NAT and static NAT. Dynamic NAT allows many private IP addresses to be mapped to a single public IP address (using different port numbers of the public IP address). Static NAT maps private IP addresses and port numbers to public IP addresses and port numbers on a one-to-one basis.

PLEASE note: The 4200 ALG automatically handles NAT for voice devices as described in Chapter 3 "VoIP Configuration".

Configure Dynamic NAT
Use Dynamic NAT when you have multiple PCs installed on the LAN side of the 4200 that require Internet or WAN access. Once Dynamic NAT is enabled the 4200 will automatically perform an address translation for all packets to/from the LAN side PCs.

A. Select **NAT**.

The default value for dynamic NAT is **enabled.**

B. Use the *Enable Lan NAT* checkbox to **enable** or **disable** dynamic NAT.
C. Press **Submit**.

Configure Static NAT
Use Static NAT when a server or PC located in the private network needs to be accessible from the external network. Some examples include a corporate web server, a mail server or an FTP server. In these instances, the 4200 statically maps

the public IP address of each server to the actual private IP address of the server. PLEASE note: In order for Static NAT to function dynamic NAT must be enabled.

A. Select **NAT**.
B. Enter the **public and private IP addresses and ports** to be mapped in *Static NAT Client Entries* using the following format: Protocol;PublicIPAddress/netmask-port>PrivateIPAddress-port

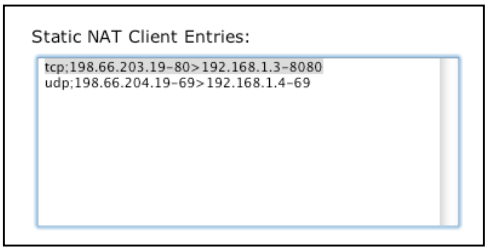
For example the entry "tcp;198.66.203.19-80>192.168.1.3-8080" will map all web traffic destined to public IP address 198.66.203.19 to the private webserver 192.168.1.3 port 8080. The public IP address of 198.66.203.19 is automatically created as a "subinterface" or "secondary address" on the WAN interface of the 4200 so that external hosts can reach the web server.

Each entry should be placed on a new line.

C. Press **Submit**.

Delete a Static NAT entry

A. Select **NAT**.
B. To delete an IP address or a range of IP addresses **highlight** the entry in the *Static NAT Client Entries* list and press the **Delete** key on your keyboard.
C. Press **Submit**.

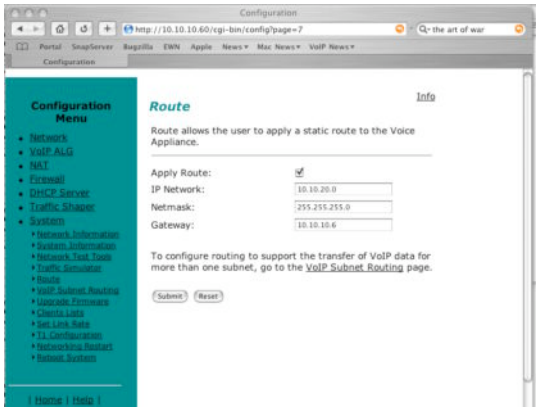


Static IP routing

In addition to locally connected IP networks the 4200 can forward traffic for one remote data network by configuring a static route entry. Any packets destined for the remote data network will be forwarded to the specified gateway address in the entry.

Configure the static route

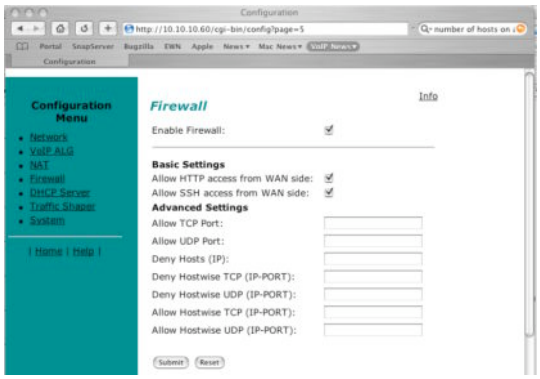
A. Select **System**.
B. Select **System Overview**.
C. Select **Route**.
D. Select the **Apply Route** checkbox.
E. Enter the **IP Network** address. This address is the remote data network you would like the 4200 to forward to the gateway. The hosts portion of the IP address should be set to "0". For example, 10.10.20.0
F. Enter the **Netmask** of the remote data network. For example, 255.255.255.0
G. Enter the **Gateway** IP address of the interface that will receive all packets destined for the remote data network.
H. Press **Submit**.



Delete the static route

A. Select **System**.
B. Select **System Overview**.
C. Select **Route**.
D. Remove the check in the **Apply Route** checkbox.
E. Press **Submit**.

Firewall Configuration



The 4200 uses a Stateful Packet Inspection (SPI) firewall to protect data devices installed behind the LAN interface. The 4200 ALG as described in the "Configure the VoIP ALG" section of this manual protects voice devices. The firewall is enabled by default. The default behavior of the firewall is to:

- deny all traffic originating from the WAN
- allow all traffic originating from the LAN
- allow only return traffic for connections that originated from the LAN
- deny all traffic originating from the WAN to the 4200 itself **except** for http and SSH connections
- allow all traffic originating from the LAN to the 4200

The default behavior can be modified using the basic and advanced settings fields on the firewall configuration page. We recommend that you use the 4200 firewall however it can be disabled if the 4200 is installed behind an existing legacy firewall.

Enable or disable the firewall

A. Select **Firewall**.
B. Use the **Enable Firewall** checkbox to either enable or disable the firewall.
C. Select **Submit**.

Configure Basic settings

To allow or deny http and SSH traffic originating from the WAN to the 4200 simply use the checkboxes provided in the basic settings area of the firewall configuration page.

WARNING: Denying http or SSH traffic from the WAN may result in losing management connectivity to the 4200 if you are configuring the system remotely using the WAN link.

A. Select **Firewall**.
B. Use the **Allow HTTP access from WAN side** and **Allow SSH access from the WAN side** checkboxes to either enable or disable the http or ssh access.
C. Select **Submit**.

Configure Advanced Settings

A comprehensive security policy can be created using the advanced settings of the 4200 firewall. The policy actions that can be taken on any packet processed by the 4200 are summarized in the following table:

Action	Description	Input format
Allow TCP Port	Allows traffic with the specified TCP port to terminate on the 4200.	*Valid values range from 1 through 65535. *Multiple entries are separated by a space *Range value specified by ":" character. For example, 25:50 means perform the action on ports 25 through 50
Allow UDP Port	Allows traffic with the specified UDP port to terminate on the 4200.	*Valid values range from 1 through 65535. *Multiple entries are separated by a space *Range value specified by ":" character. For example: 25:50 means perform the action on ports 25 through 50
Deny Hosts (IP)	Denies all traffic with the source IP address matching the specified hosts	*Multiple entries are separated by a space *Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class "c" mask. Subnets can be specified using the "/" notation. Egg. 192.168.3.1/24
Deny Hostwise TCP (IP-Port)	Denies all traffic matching the specified TCP port numbers **and** the specified **source** IP addresses	*Multiple entries are separated by a space *Port are specified using a "-" character. For example: 192.168.3.1-23 for Telnet. *Port ranges are specified using a ":" character. For example: 192.168.3.1-23:50 means port 23 through 50 *Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class "c" mask. Subnets can be specified using the "/" notation. Egg. 192.168.3.1/24
Deny Hostwise UDP (IP-Port)	Denies all traffic matching the specified UDP port numbers **and** the specified **source** IP addresses	*Multiple entries are separated by a space *Port are specified using a "-" character. For example: 192.168.3.1-23 for Telnet. *Port ranges are specified using a ":" character. For example: 192.168.3.1-23:50 means port 23 through 50 *Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class "c" mask. Subnets can be specified using the "/" notation. Egg. 192.168.3.1/24
Allow Hostwise TCP (IP-Port)	Allows all traffic matching the specified TCP port numbers **and** the specified **source** IP addresses	*Multiple entries are separated by a space *Port are specified using a "-" character. For example: 192.168.3.1-23 for Telnet. *Port ranges are specified using a ":" character. For example: 192.168.3.1-23:50 means port 23 through 50 *Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class "c" mask. Subnets can be specified using the "/" notation. Egg. 192.168.3.1/24
Allow Hostwise UDP (IP-Port)	Allows all traffic matching the specified UDP port numbers **and** the specified **source** IP addresses	*Multiple entries are separated by a space *Port are specified using a "-" character. For example: 192.168.3.1-23 for Telnet. *Port ranges are specified using a ":" character. For example: 192.168.3.1-23:50 means port 23 through 50 *Classful IP addresses are assumed by default. For example: 192.168.3.1 uses a class "c" mask. Subnets can be specified using the "/" notation. Egg. 192.168.3.1/24

A. Select **Firewall**.
B. Enter the desired **Advanced Settings** using the table above as a guide.
C. Select **Submit**.

Remove Advanced Setting Entries

To remove an advanced firewall setting simply highlight the value in the entry box and delete it using the keyboard.

A. Select **Firewall**.
B. Highlight the entry to be deleted in the **Advanced Settings** list and press the **Delete** key on your keyboard.
C. Press **Submit**.

Traffic Management Configuration

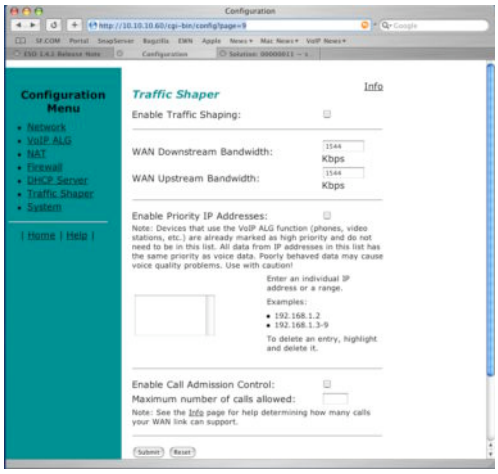
Traffic management is required to ensure high quality voice calls when both voice and data traffic share the same WAN link. Voice traffic must be prioritized for transmission over data traffic to meet the stringent jitter, latency and packet loss requirements for toll quality voice. The 4200:

- Automatically prioritizes voice traffic over data traffic to ensure toll quality voice calls.
- Manages bandwidth using different upstream and downstream link speeds (e.g. ADSL).
- Maximizes WAN link utilization by allowing data traffic to burst up to full line rate in the absence of voice calls.
- Controls the data transfer rate of upstream TCP devices to limit WAN link congestion.
- Optimizes throughput for low-bandwidth WAN links (eg. ADSL) by automatically adjusting the Maximum Transmission Unit (MTU) and Maximum Segment Size of IP datagrams during periods of WAN congestion.
- Supports network-based QoS applications by setting the TOS bits for all VoIP packets sent to the WAN and the LAN. TOS bits are used so that VoIP packets can be prioritized in the network by DiffServ enabled routers. The TOS bit value used by the 4200 is to "minimize delay and maximize throughput" or 8p hexadecimal. This value is set for all VoIP packets processed by the 4200 and overwrites any specific TOS bit configuration set by VoIP endpoints.
- Ensures that bandwidth allocated to new voice calls does not adversely affect the quality of existing active calls (Call Admission Control or CAC).

The 4200 combines sophisticated traffic management mechanisms including classification, prioritization, queuing, rate limiting and CAC to ensure toll quality voice calls. Fortunately the system manages this complexity for you and configuring traffic management is very straightforward:

1. Enable traffic shaping.
2. Specify the upstream and downstream bandwidth of your WAN link.
3. Enable CAC.

Please follow steps A through H below to configure and enable traffic management.



Enable Traffic Shaping

A. Select **Traffic Shaper**.
B. Select the **Enable traffic shaper** checkbox.

Specify the upstream and downstream bandwidth of your WAN link

C. Enter the **WAN Downstream Bandwidth** in Kbps.
D. Enter the **WAN Upstream Bandwidth** in Kbps.

If you are unsure of the WAN link bandwidth available

your IT administrator or service provider can usually provide these values. Some typical examples are as follows:

WAN Link	WAN Downstream Bandwidth	WAN Upstream Bandwidth
T1	1.544Kbps	1.544Kpbs
SDSL	768Kbps	768Kbps
ADSL	Example 1 - 768Kbps	Example 1 - 256Kbps
	Example 2 - 512Kbps	Example 2 - 128Kbps

Optionally enable priority IP addresses

VoIP traffic from devices that use the VoIP ALG function (phones, video stations, softphones on Pcs, etc.) are already marked as high priority and **do not** need to be manually configured in this list. This list is used to prioritize voice traffic from trunk interfaces of IP PBXs or other high priority devices that do not use the VoIP ALG function of the 4200.

E. Enter the IP address of other high priority devices in the **priority IP Addresses** box.

You can enter individual IP addresses or a range using by appending a "-" character to the last octet. For example, 10.10.10.2-5 would specify 10.10.10.2, 10.10.10.3, 10.10.10.4 and 10.10.10.5 as voice devices.

WARNING: Care must be taken to ensure that the IP addresses entered do not include data devices such as PCs or workstations. Traffic from these devices will be placed in the priority voice queue internal to the 4200 and burst up to full line rate. This will starve actual voice devices by consuming priority bandwidth and result in dropped calls, busy signals & poor voice quality.

Enable CAC

The 4200 uses CAC to limit the number of active voice calls over the WAN link. This is necessary because a typical installation uses a ratio of 1:2 or 1:4 active voice calls to voice devices on the assumption that 50% or 25% of all users are on the phone at the same time. These ratios are guidelines only and at times the number of concurrent calls may exceed the amount of WAN bandwidth available to process the calls. In this instance existing phone calls will experience poor quality or be dropped all together. To prevent this from occurring a typical voice installation will set a threshold for the maximum number of concurrent voice calls supported by the WAN access link. New call requests in excess of this threshold will receive the equivalent of a "fast busy" and the WAN link will not become oversubscribed.

For IP Centrex installations the maximum number of concurrent voice calls is usually configured in the 4200 by enabling CAC. When the 4200 is deployed in IP PBX applications the maximum number of concurrent calls **could** be configured in the IP PBX. If the PBX is responsible for this setting you do not need to configure CAC in the 4200. Please check with your IT administrator to determine if this is the case.

PLEASE note that CAC is available in the 4200 for the MGCP and SIP VoIP protocols only.

Determining the maximum number of concurrent calls

The maximum number of concurrent calls that can be supported by the WAN access link is calculated using the following formula:

Max calls = (Maximum WAN upstream bandwidth * .85)/VoIP codec rate

where,

Maximum WAN upstream bandwidth = value entered in step D above (in Kbps)
VoIP codec rate = 85.6Kbps for G.711 voice devices or 29.6Kbps for G.729 voice devices.

The maximum WAN upstream bandwidth is multiplied by .85 in the formula above to reduce the total bandwidth available for voice calls by 15%. This reduction is necessary because the 4200 automatically reserves 15% of the total WAN bandwidth for low priority data traffic so that it is not starved completely. Starving data traffic completely would increase the number of retry attempts and exacerbate congestion on the link during periods of peak usage.

Examples

The maximum number of G.711 voice calls supported by a T1 (1.544 Kbps) WAN is calculated as follows:

(1544*.85)/85.6 = 15.3 or 15 total voice calls.

The maximum number of G.711 voice calls supported by a 768Kbps SDSL WAN is calculated as follows:

(768*.85)/85.6 = 7.6 or 7 total voice calls

The maximum number of G.711 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

(256*.85)/85.6 = 2.5 or 2 total voice calls

The maximum number of G.729 voice calls supported by an ADSL WAN with 768Kbps downstream WAN bandwidth and 256Kbps upstream WAN bandwidth is calculated as follows:

(256*.85)/29.6 = 7.4 or 7 total voice calls

After determining the maximum number of voice calls CAC is enabled as follows:

F. Select the **Enable Call Admission Control** checkbox.
G. Enter **Maximum number of calls allowed** as calculated above.
H. Press **Submit**.

A Closer Look at Traffic Management in the 4200

The traffic management mechanisms provided by the 4200 are designed to ensure high priority real time voice traffic is processed before lower priority data traffic. At the same time, bandwidth not in use by voice traffic is made available so that data traffic can burst up to full line rate making efficient use of WAN bandwidth. Traffic management mechanisms are applied to traffic in both the upstream (LAN to WAN) and downstream (WAN to LAN) direction. Each direction is independent of the other and can support different size priority queues. This is particularly useful in the case of ADSL where the downstream bandwidth is greater than the upstream bandwidth and it would be undesirable to limit downstream data traffic to the rate of the slower upstream link.

Classifying

High priority voice traffic generated by endpoint devices such as IP phone and client adaptors are identified by their IP address. The user configures these addresses into a priority list using the traffic shaping section of the 4200 web GUI. As the 4200 processes packets they are marked as either high or low priority based on this configuration.

Upstream Traffic Management

The 4200 appliance uses a combination of Class Based Queuing and simple classless queuing to send data in the upstream direction. The Class Based Queue (CBQ) consists of two priority classes (high and low), a scheduler to decide when packets need to be sent earlier than others and a traffic shaper to rate limit by delaying packets before they are sent. Voice traffic is placed in the high priority class and data traffic is placed in the low priority class. High priority data is sent out at up to the configured priority data rate and this class is polled before lower priority data to reduce overall latency for voice traffic. Although preferential treatment is given to priority data it is bounded so that low priority data is not starved. To smooth bursts from high speed data links (typically from the LAN Ethernet segment to the WAN) the 4200 appliance uses a buffer that clocks data out at a rate not exceeding the maximum amount for the slowest link. Any lasting burst condition will cause packets to be delayed and then dropped.

Downstream Traffic Management

In the upstream direction (LAN to WAN) it is easy to see how QoS mechanisms can be applied to traffic being sent by the 4200 to guarantee sufficient bandwidth for voice traffic. We have control over how packets are handed to the WAN interface. In the downstream direction (WAN to LAN) we are installed at the CPE end of a service provider link and have no control over the amount of voice or data traffic being sent to the WAN interface. How then can we still guarantee the quality of voice traffic when it is entirely possible for an FTP session, for example, to consume the vast majority of downstream bandwidth?

Fortunately this is possible by shaping on both the egress LAN and egress WAN ports of the 4200 appliance and leveraging the congestion avoidance mechanisms built into TCP to reduce the amount of data traffic on the link. Essentially, data packets received at a rate that exceeds the configured maximum are delayed (then dropped

if necessary) when sent to the LAN interface by the 4200 appliance. Similarly data traffic sent back to the 4200 for transmission to the WAN are also delayed. This results in the end stations slowing down their transmit rate. This technique is quite effective in practice as end stations usually reduce their transmit rate before VoIP signaling has completed for new call setup.

For example consider the scenario where there are no voice calls over a SDSL WAN link and multiple FTP sessions are consuming all available bandwidth:

1) A new call request is received by the 4200 from the WAN.
2) All signaling messages for the call are classified as voice traffic and prioritized for transmission over the LAN before servicing FTP data.
3) RTP traffic is similarly classified as voice traffic and treated with priority.
4) FTP data is buffered (or dropped) on the egress LAN port and ACKs are also delayed on the egress WAN port. This throttles the transmit rate of the FTP hosts to reduce overall WAN bandwidth consumption.

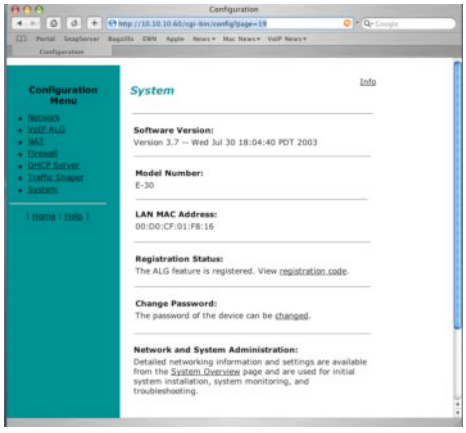
Excessive UDP traffic must be shaped in the service provider network, as UDP does not provide congestion avoidance mechanisms. The exception to this is in the case of RTP messages for voice traffic. Although RTP is based on UDP, the 4200 appliance provides its own congestion avoidance mechanism for voice traffic using Call Admission Control (CAC).

Chapter 4: System Diagnostics

The 4200 provides a powerful set of diagnostic information, troubleshooting tools and utilities for system maintenance to network operators.

Viewing Software Version, Hardware Platform and the LAN MAC Address

The software version, hardware platform, and LAN MAC address are common pieces of information requested by technical support and are accessed directly through the **System** page of the 4200 web GUI.



To ensure that you are running the latest software version please visit our website for a complete listing of software releases at:

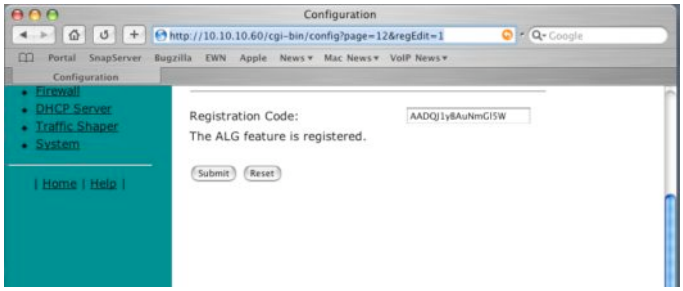
http://www.edgewaternetworks.com/Support/SupportDocLanding.html#ReleaseNotes

Viewing the ALG registration code

You will also find a link to the ALG registration code on the **System** page. The

registration code enables the ALG and is pre-installed at the factory. If the registration code is inadvertently deleted you can re-enter the code using the following steps:

Enter the Registration Code

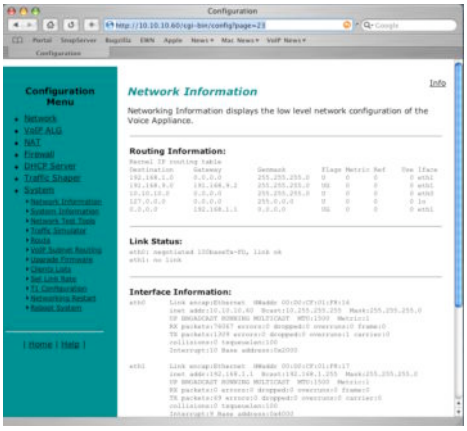


A. Select **System**.
B. Select **registration code**.
C. Select **Edit Registration Code**.
D. Enter the **Registration Code**.

The registration code can be found on the sticker located on the bottom of the 4200.

E. Press **Submit**.

Viewing Networking Information



To view the networking configuration and status of the 4200 proceed to the **Network Information** page as follows:

A. Select **System**.
B. Select **System Overview**.
C. Select **Network Information**.

The following networking information is displayed:

Routing Information

The system routing table contains the static routes for hosts and networks that are configured on the 4200. If just the LAN and WAN IP addresses have been configured there will be four lines displayed:

- The private subnet will be associated with the LAN interface.
- A public subnet present for the WAN interface.
- An entry for the 4200 loopback interface
- The 4200's default gateway forwarding to the WAN interface

Additional lines may be displayed depending on the contents of the Route and VoIP Subnet Routing pages. Each of the entries on these pages will cause an additional entry in the routing table.

Link Status

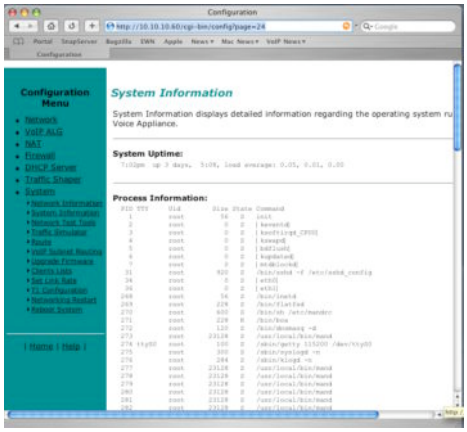
Link Status displays the status of the ethernet interfaces. Ethernet autonegotiation is often unreliable, especially between different vendors or old and new networking equipment. Failure of autonegotiation is generally not a cause for concern. However, if the negotiated rates change intermittently or the link is reported as down or no link, the link rate may need to be set manually on the *Set Link Rate* page. Intermittent data and voice outages may be caused by link "flapping" when the two endpoints of the Ethernet cable cannot reach agreement using

"autonegotiation". If the link rate is set manually, ensure that the device at the far end of the connection can communicate at the desired rate. Incompatible rates can cause a loss of communication with the 4200.

Interface Information

The specific status and configuration information for the system interfaces is displayed in the Interface Information section.
The interface statistics can point to areas of congestion in the network. If the errors statistic is a few percent or more of the total packets sent it may be an indication of excessive congestion on the network interface. If the congestion is not corrected the quality of voice calls will be affected. The topology of the network attached to the network interface with the errors should be examined and modified to better segment and isolate network traffic.

Viewing Advanced System Information



To view advanced system information for the 4200 proceed to the **System Information** page as follows:

A. Select **System**.
B. Select **System Overview**.
C. Select **System Information**.

The following system information is displayed:

System Uptime

System Uptime displays the current time, the amount of time elapsed since the last system reboot, and the system load averages for the past 1, 5, and 15 minutes. Uptime can help trace when a power outage may have interrupted service. Load averages that remain greater than 2 indicate excessive system loading. Partitioning voice traffic using a second system may be required.

Process Information

Displays the active processes in the 4200.

Memory Usage

Displays detailed memory allocation information that may be of use to technical support.

System Logging Messages

Displays information logged during system boot and normal operation. Logging messages may indicate unauthorized attempts to access the 4200, process restart messages, and excessive resource utilization messages.

Passive Voice Call Monitoring

The 4200 monitors live voice calls and performs objective speech quality assessment. This information enables the network operator to assess voice quality for the purposes of SLA tracking or problem isolation. Mean Opinion Score (MOS) results for RTP streams in both directions of a VoIP call are calculated at call

completion. This information along with the IP addresses of the VoIP endpoints supporting the call are logged locally and optionally sent to an external syslog server (see **Enable Remote System Logging** for instructions on enabling logging to a remote syslog server). Additionally the 4200 will generate a real-time message for any MOS values calculated less than 2.5 (considered poor quality) during an active call.

Voice call quality information is found locally in the **System Logging Messages** section of the **System Information** page and a sample output is provided below.

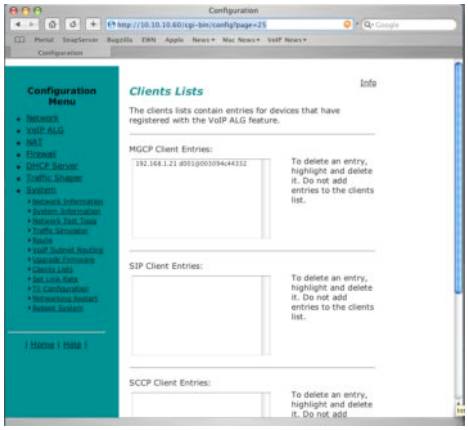
```
Recent Call Log:
<14>Sep 29 17:44:17 mand: Creating call ID 0 between 172.16.38.100 and 209.247.23.73
<14>Sep 29 17:44:56 mand: Ending call ID 0 between 0.0.0.0 and 0.0.0.0
<14>Sep 29 17:44:56 mand: Call ID 0 172.16.38.100->209.247.23.73: Call complete.  Minimum MOS=4.39
<14>Sep 29 17:44:56 mand: Call ID 0 209.247.23.73->172.16.38.100: Call complete.  Minimum MOS=4.39
<14>Sep 29 17:48:00 mand: Creating call ID 0 between 172.16.38.100 and 209.247.23.73
<14>Sep 29 17:49:47 mand: Ending call ID 0 between 0.0.0.0 and 0.0.0.0
<14>Sep 29 17:49:47 mand: Call ID 0 172.16.38.100->209.247.23.73: Call complete.  Minimum MOS=4.39
<14>Sep 29 17:49:47 mand: Call ID 0 209.247.23.73->172.16.38.100: Call complete.  Minimum MOS=4.39
<14>Sep 29 17:52:07 mand: Creating call ID 0 between 172.16.38.100 and 209.247.23.74
<14>Sep 29 17:52:44 mand: Creating call ID 0 between 172.16.38.100 and 209.247.23.74
<14>Sep 29 17:53:34 mand: Call ID 0 172.16.38.100->209.247.23.74 MOS=1.59 below threshold 2.50
<14>Sep 29 17:53:46 mand: Ending call ID 0 between 0.0.0.0 and 0.0.0.0
<14>Sep 29 17:53:46 mand: Call ID 0 172.16.38.100->209.247.23.74: Call complete.  Minimum MOS=1.59
<14>Sep 29 17:53:46 mand: Call ID 0 209.247.23.74->172.16.38.100: Call complete.  Minimum MOS=4.39
```

Accessing Troubleshooting Tools

The 4200 provides convenient test tools to facilitate problem isolation and resolution. A network operator can use these tools to verify connectivity to/from the 4200 as well as trace datapaths to endpoints throughout the network.

Verify Registered Voice Devices

The 4200 maintains a list of all registered voice devices called a "clients list" so that it can properly route voice calls. At startup, voice devices register their IP addresses with the 4200. The 4200 then registers on behalf of the voice devices by providing its own WAN IP address to the softswitch or IP PBX. If a user or network operator reconfigures the IP address of the voice device it will re-register the new address with the 4200. In this instance voice calls may be routed improperly because the 4200 clients list contains out of date information. To update the clients list simply highlight and delete the stale entry using the following steps:

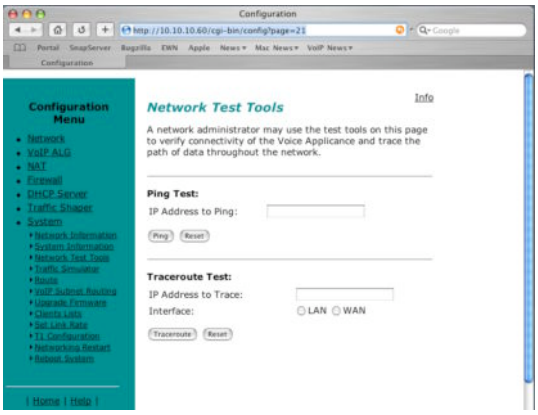


A. Select **System**.
B. Select **System Overview**.
C. Select **Clients List**.
D. Proceed to the appropriate signaling section, highlight the duplicate entry or entries and press the **delete** key on the keyboard

E. Press **Submit**.
F. Restart the VoIP ALG by following the instructions found in the *Restarting Networking Process* section of this manual.

Performing a Ping Test

A ping test is the most common test used to verify basic connectivity to a networking device. Successful ping test results indicate that both physical and virtual path connections exist between the 4200 and the test IP address. Successful ping tests do not guarantee that all data traffic is allowed between the 4200 and the test IP address but is useful to verify basic reachability. The following steps are used to perform a ping test:



A. Select **System**.
B. Select **System Overview**.
C. Select **Network Test Tools**.
D. Enter the **IP Address to Ping**.
E. Press **Ping**.

The *Network Test Tools* page will be refreshed and the results of the ping test are displayed (this may take several seconds). The **Reset** button is used to clear the IP address entry used in step "D" above.

Performing a Traceroute Test

A traceroute test is used to track the progress of a packet through the network. The test can be used to verify that data destined for a WAN device reaches the remote IP address via the desired path. Similarly, internal network paths can be traced over the LAN to verify the local network topology. The following steps are used to perform a traceroute test:

A. Select **System**.
B. Select **System Overview**.
C. Select **Network Test Tools**.
D. Enter the **IP address to Trace**.
E. Select either the **WAN** or the **LAN** radio button
F. Press **Traceroute**.

The *Network Test Tools* page will be refreshed and the results of the traceroute test are displayed (this may take several seconds). The *Reset* button is used to clear the IP address entry used in step "D" above.

Performing a VoIP Traffic Test

The 4200 includes the VoIP Test Module traffic simulation client manufactured by NetIQ. The client allows remote monitoring of the quality of service that can be delivered to the 4200.

The simulation client can be activated on the 4200 and then controlled remotely by a NetIQ console test application (sold separately). The test application can initiate VoIP tests as well as other data sessions between the test client in the 4200 and test clients placed in other parts of the network to simulate different traffic patterns. Latency, jitter, MOS scores, and other QoS or data measurements can be reported

by the console test application. The following steps configure the traffic simulation client:

A. Select **System**.
B. Select **System Overview**.
C. Select **Traffic Simulator**.
D. Select the **Enable Endpoint** checkbox.
E. Enter the **Endpoint IP Address**.

This is IP address of the remote test client.

F. Enter the **Console IP Address**.

This is the IP address of the workstation running the netiQ console.

G. Press **Submit**.

The following steps are used to disable the traffic simulator:

A. Select **System**.
B. Select **System Overview**.
C. Select **Traffic Simulator**.
D. **Uncheck** the **Enable Endpoint** checkbox.
E. Press **Submit**.

WARNING: The traffic simulator should be used for testing purposes only. Do not leave the traffic simulator enabled for extended periods of time as it generates simulated traffic that may interrupt and negatively impact the quality of voice calls.

Restarting Networking Processes

In extreme circumstances while troubleshooting you may be asked to restart the networking processes including the VoIP ALG in the 4200 by technical support. Please use the following steps to restart the networking processes:

A. Select **System**.
B. Select **System Overview**.
C. Select **Networking Restart**.
D. Press **restart**.

WARNING: Restarting network services will interrupt the system for up to a minute. All voice and data sessions currently in progress will be interrupted.

Rebooting the 4200

In extreme circumstances while troubleshooting you may be asked to reboot the 4200 by technical support. Please use the following steps to reboot the system:

A. Select **System**.
B. Select **System Overview**.
C. Select **Rebooting System**.
D. Press **reboot**.

Alternatively a reset can be performed locally by temporarily disconnecting the power cable from the 4200.

WARNING: Rebooting the system will interrupt services for a few minutes. All voice and data sessions currently in progress will be interrupted.

Chapter 5: Saving and Restoring the 4200 Configuration

The 4200 stores all configuration information for the system in a series of individual files that reside in local flash memory. These files are read at boot time to determine the configuration identity of the 4200 and then stored in RAM as "running" state. As you configure the 4200 the *submit* command writes the configuration changes to both RAM and flash so that the files stored in flash are always up to date with the running state of the system.

The 4200 provides a utility that enables you to copy the individual configuration files stored in flash to a single, consolidated backup file. This single file can then be used as a backup for the entire system and restored at a later date if necessary. Multiple backup files with different system configurations can also be created and stored locally in the 4200 or on remote TFTP servers.

PLEASE note: No more than 2 backup files can be stored in the 4200's flash due to size constraints. Also, it is recommended that you create a backup file after any configuration changes are made to the 4200. This is to prevent the loss of any configuration changes made since your last backup in the event that you must restore the system configuration.

Backup file operations are performed in the 4200 CLI using the **ewn** command.

The ewn Command

The syntax for the ewn command is as follows:

```
USAGE:
  ewn help|list
  ewn save|load|delete [file name]
  ewn upload|download [file name] [ip address]

 where file name must use extension .conf1 or .conf2
```

The **ewn** command can be used with a local terminal connection or remotely using SSH.

A. Use a NULL modem cable to connect to serial port 1 of the 4200
B. Use a terminal emulator such as Hyperterminal set to a baud rate of 115200, 8, 1 and non (databits, stop bits and parity)

Alternatively you can connect to the 4200 remotely using SSH:

A. Logon as **root**
B. Enter the **password**

Once you are at the command prompt (bash#) you can create the backup file, store it to local flash, copy it to a remote TFTP server, copy it from a remote TFTP server, delete it, load it or list all available backup files.

Create a Backup File and Save in Local Flash

bash# **ewn save <filename>**

Saves the current running configuration.

Filename format (must use extension .conf1 or .conf2):
<filename1>.conf1
<filename2>.conf2

<filenameX> can be a combination of both letters and characters. For example, EWN4200_041503.conf1 or location1_E4200.conf2. Trying to use any other filename format will result in the error message: "EWN_ERROR_BAD_FILE_NAME".

WARNING: The ".conf" extensions have special significance. If you save a configuration with <filename-new>.conf1, then any existing <filename-old>.conf1 will be overwritten with the new one.

Copy a Backup File to a Remote TFTP Server

bash# **ewn upload <filename> <tftp server IP Address>**

Copy a backup file from the 4200 to a TFTP server.

Download a Backup File from a Remote TFTP Server

bash# **ewn download <filename> <tftp server IP Address>**

Download a backup file from a TFTP server to the 4200.

List the Available Backup Files

bash# **ewn list**

List all backup files stored in FLASH. If no file has been saved, the command will only return the bash# prompt.

Delete a Backup File

bash# **ewn delete <filename>**

Delete the backup file specified in the filename.

Load a Backup File so that it Becomes the Running Configuration

bash# **ewn load <filename>**

Loads the specified backup file into RAM and makes it the active running configuration.

WARNING: Issuing this command will automatically restart the 4200 and therefore interrupt any active voice calls and data sessions.

Chapter 6: Upgrading the 4200

This chapter describes how to upgrade your 4200 to the latest software release available from Edgewater Networks. Information on the latest release can be found in the release notes section of our website at:

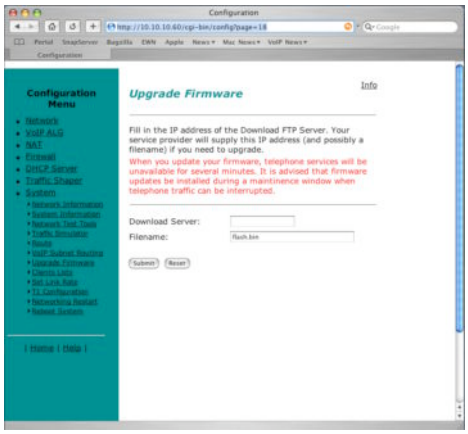
http://www.edgewaternetworks.com/Support/SupportDocLanding.html#ReleaseNotes

It is recommended that you reboot the 4200 prior to performing the upgrade. This is to make sure there is enough dynamic memory available to handle the upgrade process.

WARNING: When you update your software telephone services will be unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when telephone traffic can be interrupted.

Upgrade Procedure for Software Revision 1.3.11 or Later

Use this procedure if your 4200 is running software revision 1.3.11 or later. The software version can be found on the **System** page of the web GUI.



A. Select **System**.
B. Select **System Overview**.
C. Select **Upgrade firmware**.
D. Enter the **Download Server** IP address of 204.202.2.188 is the public IP address of the FTP site hosted by Edgewater Networks.
E. Enter the **Filename**: flash.bin
F. Press **Submit**.

You can follow the progress of the upgrade by selecting the **refresh the upgrade status** link.

WARNING: Do not change the configuration or power off the device

until the write is 100 percent complete. The 4200 may become unusable if the write is interrupted. The flash write can take up to 5 minutes depending on the speed of the download server.

The system will automatically restart after the new image has been loaded.

G. Verify that the upgrade was successful by checking the software revision number found on the **System** page

Upgrade Procedure for Software Version 1.3.9 or Earlier

Use this procedure if your 4200 is running software revision 1.3.11 or later. The software version can be found on the *System* page of the web GUI.

We recommend running the upgrade command using the CLI rather than the web GUI. This is because running the command in the CLI provides more feedback to the operator). It is recommended that you perform the upgrade with a local terminal connection to the system by using the following steps.

C. Use a NULL modem cable to connect to serial port 1 of the 4200
D. Use a terminal emulator such as Hyperterminal set to a baud rate of 115200, 8, 1 and non (databits, stop bits and parity)

Alternatively you can connect to the 4200 remotely using SSH:

C. Logon as **root**
D. Enter the **password**
E. Ping the Edgewater Networks FTP server to determine if you can reach the upgrade server by issuing the following command: **ping 204.202.2.188**
F. If the ping was successful enter the upgrade command as follows: **netflash -fk 204.202.2.188 pub/e_4200/flash.bin**

You will be prompted for a user ID and password. The user ID is 'anonymous' and there is no password. The following is a log of the process:

```
netflash: login to remote host 204.202.2.188
Name (204.202.2.188:root): anonymous
Password:
netflash: ftping file "pub/4200/flash.bin" from 204.202.2.188
.....................................................................
.....................................
netflash: got "pub/e_4200/flash.bin",  netflash: image is compressed, decompressed    length xxxxx
netflash: programing FLASH device /dev/mtd3
.....................................................................
.....................................................................
Restarting system.
```

The upgrade process takes between 5 and 10 minutes, depending on the speed of the FTP download.

WARNING: Do not change the configuration or power off the device until the write is 100 percent complete. The 4200 may become unusable if the write is interrupted. The flash write can take up to 5 minutes depending on the speed of the download server.

You may see a "Restarting system" message or your SSH session will exit. This is an indication the system is rebooting. The system takes 1-2 minutes to reboot.

G. Verify that the upgrade was successful by checking the software revision number found on the *System* page
H. If you opened an SSH session you should logout of the 4200 and close the SSH session by entering **exit** in the command line.

Appendix A: Troubleshooting Tips

This section contains possible solutions to problems regarding the installation of the 4200. If you cannot find an answer here please visit our website at www.edgewaternetworks.com.

I am having trouble reaching the Internet through the 4200.

We recommend connecting a PC directly (or via a switch) to the LAN port of the 4200. The default LAN IP address of the 4200 is 192.168.1.1 so please be sure that the IP address of the PC is on the same network (eg. 192.168.1.2). Once you have connected please verify that the IP configuration information in the *Network* page is correct. Some other items to try:

- Ping the WAN interface of the 4200 from the attached PC
- Ping the DNS server for your network. Sometimes connectivity problems occur when the domain name being used cannot be mapped to the proper IP address.
- Ping a well known address on the Internet (e.g. www.edgewaternetworks.com)
- Ping the IP address of the remote softswitch or IP PBX.

I do not receive dial tone when going "off hook" or my phone will not register with the softswitch/IP PBX.

- Verify the configurations on the *VoIP ALG* page.
- Check that the ALG registration code is configured
  A. Select **System**.
  B. Select **registration code**.
- Attempt to ping the softswitch using the ping tool in the web gui
  A. Select **System**.
  B. Select **System Overview**.
  C. Select **Network Test Tools**.
  D. Enter the softswitch address in the **IP Address to Ping** field.
  E. Press **Ping**.

Appendix B: Contact Information

Contact and Support Information

Edgewater Networks, Inc.
2730 San Tomas Expressway
Suite 200
www.edgewaternetworks.com
Phone: 408.351.7200

General: info@edgwaternetworks.com
Sales: sales @edgewaternetworks.com

Edgewater Networks, Inc. - Technical Assistance Center
Phone: 408.351.7200 ext. 2
support@edgewaternetworks.com

Appendix C: Specifications

WAN Ports	1x10/100 Ethernet
LAN Ports	1x10/100 Ethernet
Serial Ports	1xRS-232 (DB9)
Dimensions	10.25"x6.75"x1.5" (260mmx172mmx40mm)
Weight	1 lb. (500g)
LEDs	Power, System, Online, LAN tx, LAN rx, WAN tx, WAN rx, Serial, QoS Test, Calls
Power	5V 2A
Warranty	1 Year

Appendix D: Warranty Information

Software Warranty

Edgewater warrants that the Software on the Product will substantially conform with Edgewater's published specifications for such Software on the date of the order for such Product for a period of ninety (90) days after the shipment of the Product, if properly used in accordance with the procedures described in the documentation supplied by Edgewater. Edgewater's exclusive obligation with respect to nonconforming Software shall be, at Edgewater's option, to: (a) replace that copy of the Software with one that conforms to the specifications; (b) use diligent efforts to provide a correction of the defect, or (c) refund the purchase price paid for the Product on which the Software is installed. Defects in the Software must be reported during the warranty period and be reported to Edgewater in a form and with supporting information reasonably requested by Edgewater to enable it to verify, diagnose and correct the defect.

Hardware Warranty

For a period of one (1) year after shipment of the Product, Edgewater warrants that such Hardware will substantially conform to Edgewater's published specifications for such Hardware on the date of order if properly used in accordance with procedures described in the documentation supplied by Edgewater. End-user shall notify Edgewater of any nonconformance during the warranty period, obtain a return authorization for the nonconforming Hardware from Edgewater, and return the nonconforming Hardware to Edgewater's designated repair facility, freight prepaid, with a statement describing the nonconformity. Edgewater's exclusive obligations with respect to nonconforming Hardware shall be, at Edgewater's option, to repair or replace such Hardware, if it is determined to be defective, or to refund to End-user the purchase price paid for the Product.

Appendix E: License Information

EdgeMarc™ Software License Agreement

EDGEWATER NETWORKS, INC. IS WILLING TO LICENSE THIS SOFTWARE AND THE ACCOMPANYING DOCUMENTATION TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS IN THIS AGREEMENT.

PLEASE READ THE TERMS CAREFULLY BEFORE INSTALLING, USING, OR ACCESSING THE SOFTWARE, AS BY SUCH ACTIONS YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS.

IF YOU DO NOT AGREE TO THESE TERMS, EDGEWATER NETWORKS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND WE ASK THAT YOU IMMEDIATELY RETURN THIS PRODUCT FOR A FULL REFUND.

LICENSE. You are permitted to install, perform and display the Software and use the Software only on the EdgeMarc™ converged network appliance that accompanies this Software. You may copy the Software only for backup purposes, provided that you reproduce all copyright and other proprietary notices that are on the original copy of the Software.

1. RESTRICTIONS. You may not use, copy, modify, or transfer the Software, or any copy thereof, in whole or in part, except as expressly provided in this Agreement. You may not reverse engineer, disassemble, decompile, or translate the Software, or otherwise attempt to derive the source code of the Software, except to the extent allowed under any applicable law. Any attempt to transfer any of the rights, duties or obligations hereunder is void. You may not rent, lease loan, resell for profit, or distribute the Software, or any part hereof.

2. OWNERSHIP. The Software is licensed, not sold, to you for use only under the terms of this Agreement, and Edgewater Networks reserves all rights not expressly granted to you.

3. TERM. This Agreement will terminate immediately upon notice to you if you materially breach any term or condition of this Agreement. You agree upon termination to promptly destroy the Software and all copies.

4. WARRANTY DISCLAIMER. Edgewater Networks warrants to You that the Software, when operated in an environment supported by Edgewater Networks, will perform substantially in accordance with its user documentation for the ninety (90) day period immediately following your receipt of the Software (the "Warranty Period"). If You notify Edgewater Networks during the Warranty Period that the Software does not perform substantially in accordance with the user documentation and Edgewater Networks is able to reproduce such failure, the entire and exclusive liability and remedy shall be limited to either, at Edgewater Networks' sole discretion: (i) providing a correction or a workaround for such failure;

(ii) replacing the Software with conforming software; or (iii) refunding of the license fee paid for the Software.

EXCEPT AS EXPRESSLY PROVIDED, THE SOFTWARE IS PROVIDED TO YOU "AS IS" AND EDGEWATER NETWORKS AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR WRITTEN INFORMATION OR ADVICE GIVEN BY EDGEWATER NETWORKS, ITS EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENS SHALL INCREASE THE SCOPE OF THE ABOVE WARRANTIES OR CREATE ANY NEW WARRANTIES. Some states or jurisdictions do not allow the disclaimer of certain implied warranties, so the above disclaimer may not apply to You.

5. LIMITATION OF REMEDIES. REGARDLESS OF WHETHER ANY REMEDY SET FOTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL EDGEWATER NETWORKS OR ITS SUPPLIERS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOST PROFITS, LOST DATA, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILTY TO USE THE SOFTWARE OR ANY DATA SUPPLIED THEREWITH, EVEN IF EDGEWATER NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE. IN NO EVENT SHALL THE LIABILITY OF EDGEWATER NETWORKS EXCEED THE AMOUNT RECEIVED BY EDGEWATER NETWORKS FROM YOU FOR THIS SOFTWARE LICENSE. Some states or jurisdictions do not allow the exclusion or limitation of incidental, consequential, indirect or special damages, so the above limitations may not apply to You.

6. EXPORT LAW. The Software and related technology are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export or import as may be required.

7. U.S. GOVERNMENT END USERS. The Software is a "commercial item" as that term is defined at FAR 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212 (Sep 1995) and is provided to the U.S. Government only as a commercial end item. Consistent with FAR.12.212 and DFARS 227.7202 (Jun 1995), all U.S. Government End Users acquire the Software with only those rights set forth herein.

8. GENERAL. This Agreement will be governed by the laws of the State of California, without regard to or application of conflicts of law rules or principles. The State and Federal Courts located in Santa Clara County shall have sole jurisdiction over any disputes arising hereunder. If any provision of this Agreement is held to be unenforceable, that provision will be removed and the remaining provision will remain in full force. This Agreement is the complete and exclusive statement of the agreement between us which supersedes any proposal or prior agreement, oral or written, and any other communications between us in relation to the subject matter of this Agreement.

If you have any questions regarding this Agreement, please contact Edgewater Networks, Inc. at 2730 San Tomas Expressway, suite 200, Santa Clara, CA 95051 or call 408.351.7200.

THE SOFTWARE AND ACCOMPANYING USER DOCUMENTATION ARE PROTECTED BY UNITED STATES COPYRIGHT LAW AND INTERNATIONAL TREATY. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES.

Software included in this product contains a module called PsyVoIP which is protected by copyright and by European, US and other patents and is provided under licence from Psytechnics Limited.

Portions of this product also include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE:

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a

"work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose

permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash,

DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson(tjh@cryptsoft.com)

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.