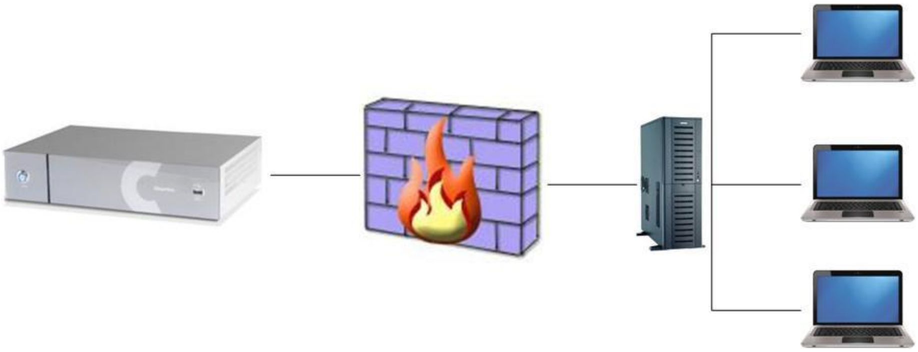
ClearOne®

NetPoint Firewall Traversal Server Installation and Setup Manual



ClearOne
5225 Wiley Post Way
Suite 500
Salt Lake City, UT 84116

Telephone	1.800.283.5936 1.801.974.3760
Tech Sales	1.800.705.2103
FAX	1.801.974.3669
E-mail	tech.support@clearone.com support@netstreams.com
On the Web	Web www.clearone.com www.netstreams.com www.streamnetpartners.com

NetPoint Firewall Traversal Server

Installation and Setup Manual

ClearOne Document
800-000-000-04 _Rev1.0 – October 2012

Information in this document is subject to change without notice.

WARNING: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION! To comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules, all cables used to connect the system and peripherals must be shielded and grounded. Operation with non-shielded cables may result in interference to radio or television reception.

Safety Information

CAUTION! Do not open the NetPoint unit. There are no user-serviceable parts inside. Opening the unit voids the warranty and can also cause injury. Please refer servicing to ClearOne trained service personnel.

DANGER! The internal areas of the unit and auxiliary equipment are sources of voltage that, if not handled properly, constitute danger of bodily harm.
DO NOT operate the unit with any of its covers (including main cover, bezels, filler brackets, front-panel inserts, and so on) removed.
INCORRECT replacement of the Remote Control battery can cause an explosion. Replace only with the same or equivalent-type of battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

When you use a NetPoint system, observe the following safety guidelines:

- Make sure that the power is turned off and all equipment is disconnected from the power supply before making any equipment connections.
- Make sure the monitor and attached accessories are electrically rated to operate with the AC power available in your location.
- To help avoid possible damage to the system cards, wait 5 seconds after turning off the system before disconnecting a device from the computer.
- To help prevent electric shock, plug the unit and accessories' power cables into properly grounded power sources. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Make sure that nothing rests on the unit system's cables and that the cables are not located where they can be stepped on or tripped over.
- Do not install this equipment near water, or in an otherwise wet or damp environment.
- Do not run the equipment in an environment with ambient temperature higher than 35°C or lower than 10°C.
- Keep food and liquids away from the system or accessories.
- Keep the unit away from radiators and heat sources. Also, do not block cooling vents. Avoid placing loose papers underneath the unit, and do not place the computer in a closed-in wall unit or on a bed, sofa, or rug.
- Do not install or operate this equipment if chemical gas leakage is expected in the area.

FCC Warning

Modifications not expressly approved by the manufacturer could void the user authority to operate the equipment under FCC rules.

The FCC Wants You to Know

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Table of Contents

Chapter 1: Overview

IN THIS CHAPTER

This chapter provides an overview to NetPoint and includes the following sections:

- NetPoint Overview
- NetPoint Server

NETPOINT OVERVIEW

NetPoint is a combined hardware and software system designed to enable firewall transversal. NetPoint supports the H.460 standard, and ClearOne Tunneling propriety protocol. It allows end points behind firewalls to communicate with other end points, both in WAN and behind other firewalls.

NetPoint allows the connection of clients (in WAN or behind a firewall) to a Collaborate Central server that is located behind a firewall.

NETPOINT SERVER

Throughout this guide, the name “NetPoint” refers to the NetPoint Server.

Chapter 2: Negotiating NATs and Firewalls

IN THIS CHAPTER

ClearOne's NetPoint allows organizations to conduct H.323 audio and video communication, while continuing to protect their local area networks (LANs) with NATs and firewalls using proprietary and/or H.460 protocols. This chapter includes the following sections:

- NATs and Firewalls in Enterprises
- Effects of Firewalls and NATs on H.323 Videoconferencing
- The NetPoint System Solution

NATS AND FIREWALLS IN ENTERPRISES

To protect the nodes within their networks, many organizations employ firewalls and NAT (Network Address Translation) devices. Together or separately, these devices present challenges for implementing IP videoconferencing solutions.

NETWORK ADDRESS TRANSLATION DEVICES (NATS)

NAT is a protocol in which a LAN uses one set of IP addresses for internal communication (within an organization's LAN) and a different address for communication with external network, such as the Internet. It provides a solution for two main conditions:

- **Network security** - Internal IP addresses are hidden from external users. This helps protect the network's computers from hackers and spammers.
- **Finite number of available IP addresses** - The number of public IP addresses is limited. By defining addresses for internal use only, an organization can use a large number of different addresses without conflicting with addresses used elsewhere.

Within a NAT, the nodes have internal addresses which are inherently unreachable to nodes from outside. Without a traversing device, internal nodes cannot receive calls or communication from external nodes. Even if a node within the NAT initiates communication, it cannot receive a reply - the reply is being sent to a non-routable IP address.

A NAT device maps public IP addresses to private IP addresses and ports. It also assigns ports to nodes within its network, but the private IP addresses remain unknown to outside users. To enable external communication, the NAT device opens a channel to the public network. The NAT appends the public IP address to all data packets sent outside the network. Likewise, for incoming data, the NAT device replaces its public address with the mapped internal address.

Usually, NAT assignments last for a short period of time and are then released. It's important that a NAT assignment remain valid for the duration of an open connection. To accomplish this, any node communicating through a NAT device must send a "keep-alive" packet periodically to prevent remapping during an open session.

FIREWALLS

To protect their networks and data resources from external hazards such as hacking and virus propagation, some organizations install firewalls.

Firewalls check the IP address and destination port of each data packet received from external sources. The type of permitted incoming traffic depends on the firewall's configuration. For example, the firewall may allow traffic from an external source to pass if a node inside the firewall initiated communication with it. Usually, they will block or discard unsolicited packets.

In order to deal with desirable requests for information while protecting most of their user nodes, many organizations place relevant information on a web server inside the firewall. The firewall is then configured to permit traffic to and from the web server's IP address and port 80 to pass.

EFFECTS OF FIREWALLS AND NATS ON H.323 VIDEOCONFERENCING

Compared to other data communications protocols such as HTTP and FTP, H.323 has unique characteristics that cause difficulties in enterprise environments protected by firewalls and NATs.

- H.323 transmissions include the embedding of the sender's IP address inside the data packets. The call recipient transmits audio and video in return to the initiating user at the IP address embedded in the original transmissions. If this IP address is private, Internet routers typically discard the audio and video packets sent from the external endpoint because they are being sent to an un-routable private IP address.
- During H.323 communications, several protocol parameters, including IP port values, are determined dynamically during call setup negotiation instead of in advance. This poses a problem in security devices such as firewalls, which usually require a security schema based on opening specific known ports.
- The use of H.323 video and voice communication requires a firewall to open a wide range of ports so that traffic can pass unhindered. The IP voice and video communications protocols require several open ports to receive call control messages and to establish the voice and video data channels. These additional port numbers are determined dynamically, not in advance. Therefore, network administrators would have to open up all the firewall ports to allow the H.323 traffic to pass through. This constitutes a breach of the firewall's purpose, which prefers to close as many ports as possible.
- H.460.18 and H.460.19 are ITU standards that enable H.323 devices to exchange signaling and media across boundaries imposed by NAT and firewalls, without the need for any additional equipment.

In most organizations, firewalls are configured to severely limit the types of inbound data traffic that will arrive to internal users' workstations, servers, and peripheral equipment.

Firewalls support many different protocols, but they do not specialize in H.323 communications. This may cause variations in the level of support for H.323 among different vendors' firewalls. This results in occasional call failures.

NATs also impose obstacles for IP voice and video communications. NATs assign private IP addresses to workstations and servers located within a private LAN. However, most routing devices that control the flow of information across the Internet can send data only to devices with routable or public IP addresses. The addresses of users in NAT-protected networks are unknown to devices on the public side of the NAT. As a result, the users behind the NAT cannot receive calls from the public side of the LAN.

NATs also hinder H.323 calls which are dialed out by private LAN users to the public side. As previously mentioned, the IP address of the sender is embedded in the video and audio transmissions. If this IP address is not able to be routed, any return transmission will not penetrate the network protected by the NAT. The user behind the NAT never receives the public side user's audio and video.

THE NETPOINT SYSTEM SOLUTION

ClearOne's NetPoint of products provides connectivity for videoconferencing networks within organizations that are protected by NAT and firewalls.

PERMITTED NETWORK TRAFFIC

The NetPoint allows passage by the following types of network traffic:

- Gatekeeper registration
- Call setup messages
- RTP-based audio and video (as well as data) streams
- Collaborate Central Administrator login
- Remote end point/device configuration (from Collaborate Central Administrator)
- Neighboring gatekeeper and directory gatekeeper messages (between Collaborate Central's or to non-Collaborate Central gatekeepers that are not behind a NetPoint).

HARDWARE CONFIGURATIONS

Each proxy configuration may handle up to 100 concurrent video calls.

NETPOINT SUPPORT IN A FIREWALL

If a firewall is installed in the organization, the NetPoint requires that you open pinholes through three specific ports, outward to the public network. You do not have to open any ports inward, and the firewall does not have to accommodate requests to open random or dynamic ports. Traffic through the pinholes is directed through NetPoint components only.

As a result, external addresses never connect directly to the private network and devices in the private network never connect directly to the public network.

QoS Support

ClearOne's PacketAssist Architecture, which delivers Quality of Service (QoS) to IP videoconferencing, is integrated into the NetPoint. The QoS helps provide the best possible audio and video quality, at a given data rate, for all H.323/H.460 end points located behind the NetPoint. The NetPoint's QoS settings override the local QoS settings of any of the end points behind it.

- The QoS settings are accessible either directly through the NetPoint's configuration utility or through the Collaborate Central Administrator (for those systems installed in Collaborate Central-managed networks).

Chapter 3: Collaborate Central/Gatekeeper Management

IN THIS CHAPTER

This chapter provides examples of basic topologies for networks which receive management services from ClearOne's Collaborate Central™ (Collaborate Central). Each sample illustration provides examples of typical locations for NetPoint and end points within these topologies and the IP addresses required to receive Collaborate Central/gatekeeper management.

This chapter includes the following sections:

- Registering NAT/Firewall Protected Nodes to the
- Negotiating Firewalls

REGISTERING NAT/FIREWALL PROTECTED NODES TO THE COLLABORATE CENTRAL

This section suggests basic network scenarios and guidelines for registering the NAT/firewall protected nodes with the Collaborate Central:

- Collaborate Central Outside of LAN
- Collaborate Central Inside LAN

COLLABORATE CENTRAL OUTSIDE OF LAN

In this configuration, NetPoint is not required. Collaborate Central supports H.460, allowing an endpoint to use either H.323 or H.460 for firewall/NAT traversing. To register with the Collaborate Central:

- The nodes outside of LAN send H.323 login requests to the Collaborate Central.
- The nodes at LAN (behind firewall/NAT) send H.460 login requests to the Collaborate Central.

COLLABORATE CENTRAL INSIDE LAN

In this configuration, the Collaborate Central routes all signaling packets of public-public and private-public calls through the NetPoint. Data passes through the NetPoint during calls between public and private network devices (not for public-public).

NEGOTIATING FIREWALLS

To enable H.323 videoconferencing to traverse firewall-protected networks, ClearOne suggests employing its NetPoint solution, opening pinholes outward in your firewall as directed below.

Setting Up the Firewall to Support NetPoint Deployment

To add NetPoint support to your firewall, set up Collaborate Central in your organization’s private network and NetPoint in your organization’s DMZ (**D**e**M**ilitarized **Z**one).

To enable communication between the Collaborate Central in the private network and the NetPoint in the DMZ, open pinholes outward for three specific ports that interface with the private network.

To enable incoming H.323 conferencing calls to connect to the NetPoint in the DMZ, open all ports designated for H.323 communication that interface with the public network (H.323 selects ports dynamically while the calls are connected).

The NetPoint’s deployment does not affect other ports or rules of the firewall. As a result, it is not required to open ports inward or to open random or dynamic ports. External users cannot connect directly to the private LAN and the LAN’s users cannot connect directly to the public network.

To add NetPoint support to a firewall

1. In the firewall’s configuration, open any range of three ports outward as the pinholes. We recommend that you use the suggested default port selections although you may change them if your networking specifications require it.

   NOTE: The Outbound TCP Signaling Port (lowest of the range of three ports) must be set identically in the Collaborate Central and NetPoint servers.

Open a range of ports configured for H.323 connection, which will be used for routing calls between the DMZ and the public network.

Chapter 4: Configuring NetPoint in Collaborate Central

IN THIS CHAPTER

When your organization purchased a NetPoint solution, it received an installed, pre-configured system of NetPoint products. If it becomes necessary to change settings later on (such as a running of the NetPoint recovery option), you will have to reconfigure the system.

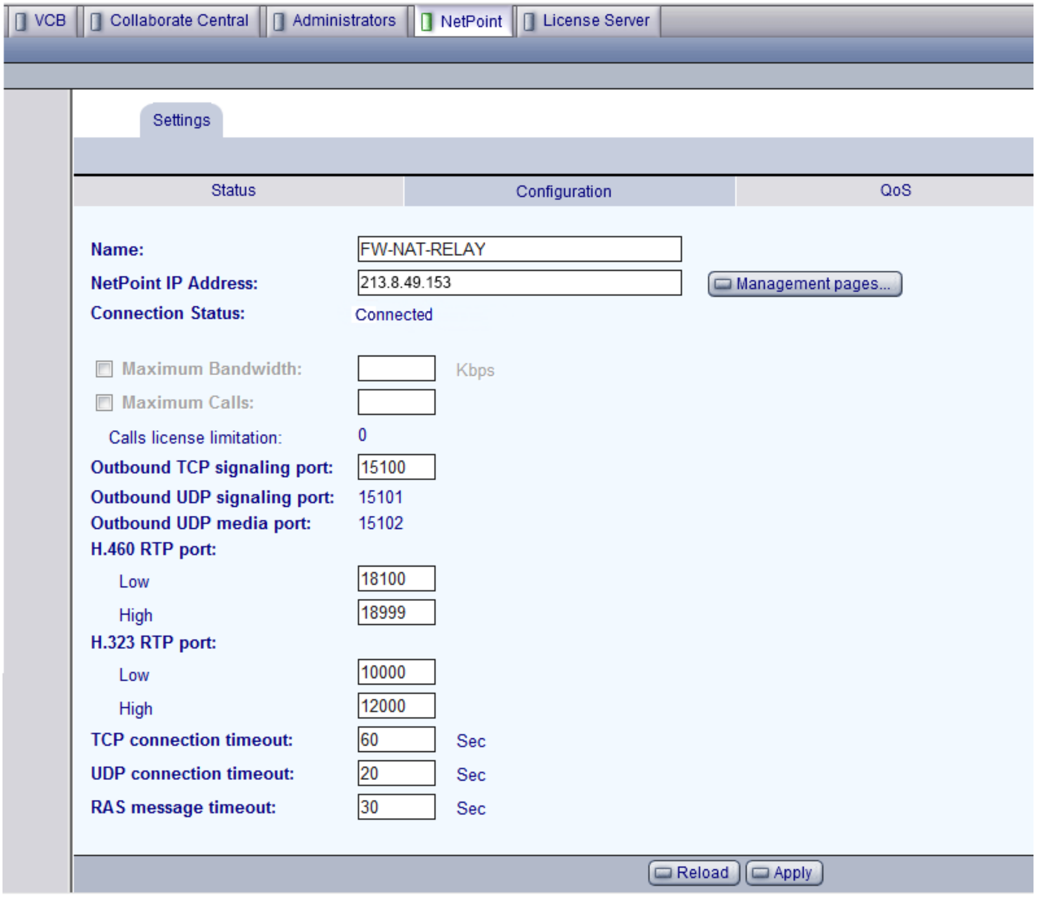
This chapter and includes the following sections:

- Configuration
- Verifying NetPoint status
- QoS

CONFIGURATION

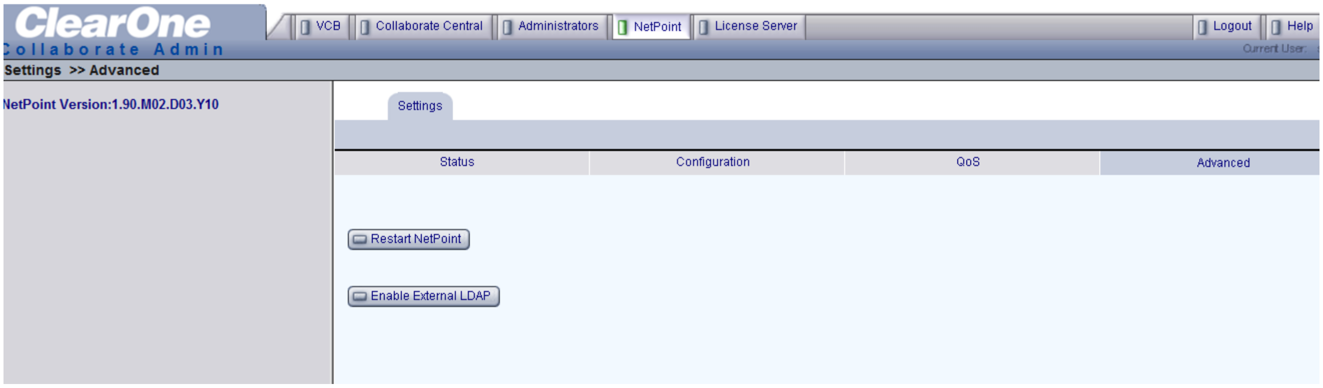
To configure NetPoint in Collaborate Central:

1. Log in to EVCAdmin ([IP Address]EVCAdmin. The default user name is **su**, and the default password is **1234**.
2. Select **NetPoint**->**Settings**->**Configuration**.



Name:	FW-NAT-RELAY	
NetPoint IP Address:	213.8.49.153	
Connection Status:	Connected	
□ Maximum Bandwidth:		Kbps
□ Maximum Calls:		
Calls license limitation:	0	
Outbound TCP signaling port:	15100	
Outbound UDP signaling port:	15101	
Outbound UDP media port:	15102	
H.460 RTP port:		
Low	18100	
High	18999	
H.323 RTP port:		
Low	10000	
High	12000	
TCP connection timeout:	60	Sec
UDP connection timeout:	20	Sec
RAS message timeout:	30	Sec

3. Enter the **NetPoint IP Address**. All other parameters are configured to default values automatically. If you have no special reason to change them, leave the default values and click **Apply**.
4. After you enter the NetPoint IP address, verify that **Connection Status** is “Connected”. If the status is still “Disconnected”, do the following:
   - Verify the NetPoint IP address; If the address is correct and in the Advanced tab click **Restart NetPoint**.



Settings >> Advanced

NetPoint Version:1.90.M02.D03.Y10

5. If you decide to change the **Outbound TCP Signaling Port** before establishing the connection with NetPoint, you have to click on the **Management Pages** button, and change the port number in the NetPoint configuration page accordingly.

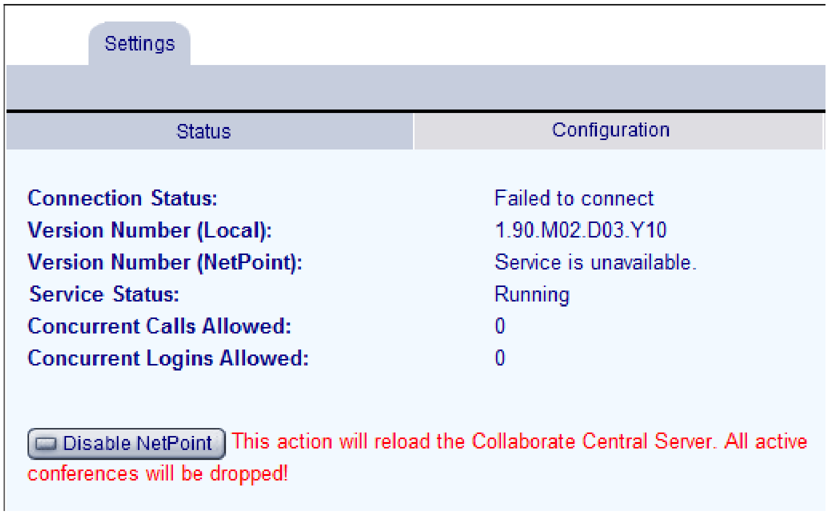
Parameters Description

Name	Description
Name	Identity of the server. This name appears in the Main View.
NetPoint IP Address	IP address of the server.
Management Pages	This button opens the NetPoint Home Page in the NetPoint tab. This tab is practically the same as the current screen, allowing you to manually synchronize the Outbound TCP Signaling Port with Collaborate Central. The NetPoint Admin web application includes several additional tabs, which are similar to the tabs of EVC Admin (License Server, Network, Administrators, Restore and Upgrade).
Connection Status	Displays the status of the current connection.
Maximum Bandwidth	Set up the total bandwidth that the local Collaborate Central allocates to all calls routed through the NetPoint.
Maximum Calls	Set up the maximum number of calls that may be routed through the NetPoint at the same time (in both directions). The number of calls cannot exceed the number of calls allowed by your license (indicated below the field).
Calls license limitation	Number of concurrent calls you can make according to your license.

Name	Description
Outbound TCP signaling port	The port in the firewall through which the system routes TCP/IP signals. This port must be identical on both Collaborate Central and NetPoint servers. If you decide to change the Outbound TCP Signaling Port before establishing the connection with NetPoint, you have to click on the Management Pages button, and change the port number in the NetPoint configuration page accordingly.
Outbound UDP signaling port	The port in the firewall through which the system routes UDP signals. This parameter is configured automatically based on Outbound TCP Signaling Port (+1).
Outbound UDP media port	The port in the firewall through which the system routes data. This parameter is configured automatically based on Outbound TCP Signaling Port (+2).
H460 RTP port Low/High	The range of ports in the firewall through which the system routes data, when communication is external to the organization network.
H323 RTP port Low/High	The range of ports in the firewall through which the system routes inbound and outbound data.
TCP connection timeout	Frequency for sending Keep Alive messages over the TCP/IP connection, if applicable.
UDP connection timeout	Frequency for sending Keep Alive messages over the UDP connection, if applicable.
RAS message timeout	Amount of time until an unanswered Registration Admission Status (RAS) request to the Collaborate Central is discarded.

VERIFYING NETPOINT STATUS

The Status tab allows you to verify all indications concerning the connection, and allows you to stop and start the NetPoint service.



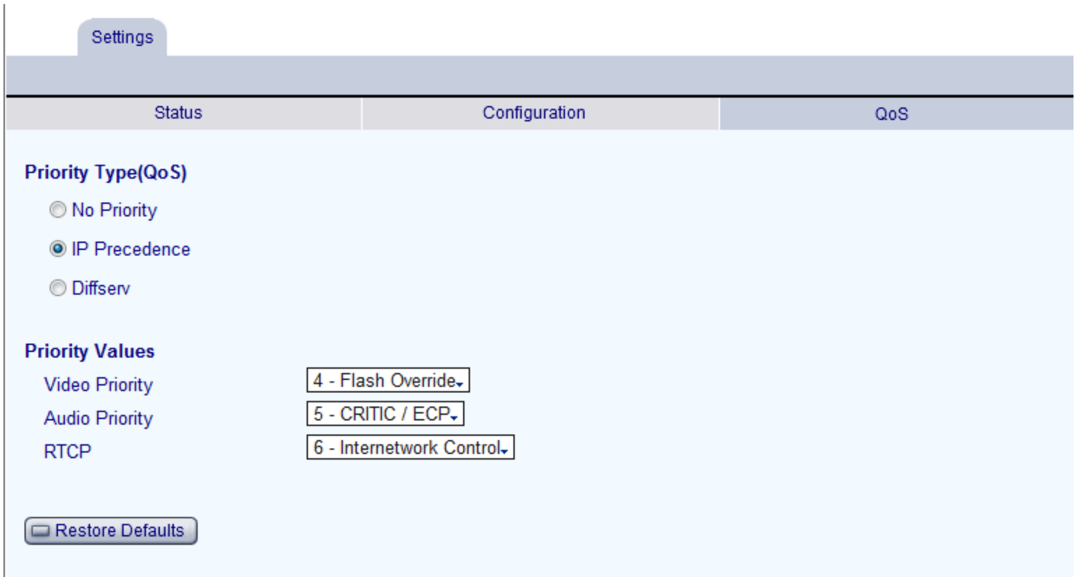
Connection Status:	Failed to connect
Version Number (Local):	1.90.M02.D03.Y10
Version Number (NetPoint):	Service is unavailable.
Service Status:	Running
Concurrent Calls Allowed:	0
Concurrent Logins Allowed:	0

This action will reload the Collaborate Central Server. All active conferences will be dropped!

QOS

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets through this NetPoint.

These settings override the local QoS settings of any end points communicating through this NetPoint.



Priority Type(QoS)

○ No Priority

● IP Precedence

○ Diffserv

Priority Values

Video Priority	4 - Flash Override
Audio Priority	5 - CRITIC / ECP
RTCP	6 - Internetwork Control

Set QoS properties as follows.

PRIORITY TYPE (QOS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

- **No Priority** – Network transfers packets using normal Best-effort (or Routine) packet transmission.
- **IP Precedence** – Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.
- **Diffserv** – Network transfers packets according to the ISP's allocation of resources, in response to network behavior.

PRIORITY VALUES

- **Video, Audio and RTCP Priority** – For each packet type, select an appropriate priority level. If network conditions cause congestion or transmission delays, the item with the lowest priority number may be discarded in order to send the rest of the packets successfully.

  The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see the Collaborate Central Administrator's Guide, Appendix I, "QoS Priority Values".

To reset the Priority default values, click **Restore Defaults**.

Chapter 5: Firewall Requirements on Endpoint Side

IN THIS CHAPTER

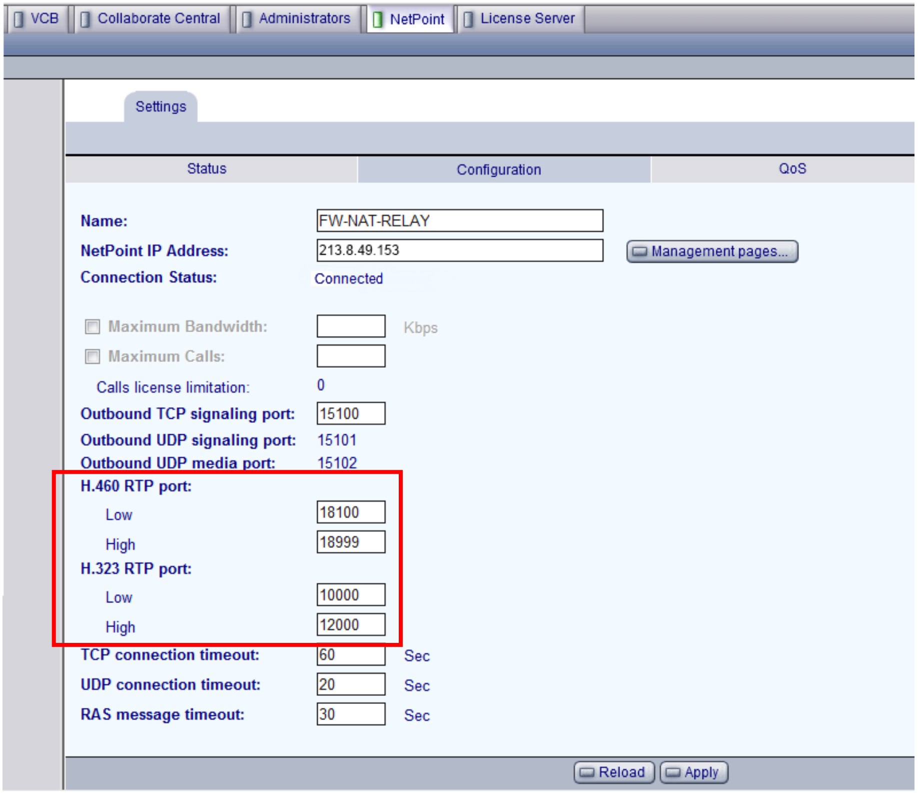
This chapter details the endpoint side ports that should be opened in the firewall and includes the following section:

- Endpoint Side Ports

ENDPOINT SIDE PORTS

The following ports should be opened in the firewall on the endpoint side to allow the endpoints to work properly:

- Two static ports:
  - 1719 UDP
  - 1720 TCP
- Up to 5 dynamic ports:
  - 1 TCP port for H.245 – from the range of H.323 Media Ports (see snapshot below)
  - Up to 4 UDP ports for Audio, Video, Data, and FECC (1 UDP port for every media type or 1 UDP port for all if multiplex mode enabled) – from the range of H460 Media Ports (see snapshot below)



Name: FW-NAT-RELAY
NetPoint IP Address: 213.8.49.153
Connection Status: Connected

□ Maximum Bandwidth: Kbps
□ Maximum Calls:

Calls license limitation: 0
Outbound TCP signaling port: 15100
Outbound UDP signaling port: 15101
Outbound UDP media port: 15102
H.460 RTP port:
Low 18100
High 18999
H.323 RTP port:
Low 10000
High 12000
TCP connection timeout: 60 Sec
UDP connection timeout: 20 Sec
RAS message timeout: 30 Sec

Chapter 6: Using NetPoint

IN THIS CHAPTER

This chapter covers NetPoint usage, and includes the following sections:

- Unpacking and Connecting NetPoint Server
- Logging in
- Main Screen
- Administrators
- Network
- License
- Log Out
- Shut Down
- Restart
- Backup / Restore

UNPACKING AND CONNECTING NETPOINT SERVER

- Unpack and connect the NetPoint server to the Internet.
- Configure an IP address for the NetPoint server from the NetPoint Admin page network tab or by using cross cable.

ASSIGNING STATIC IP ADDRESSES TO NETPOINT SERVER WITH DHCP ADDRESS

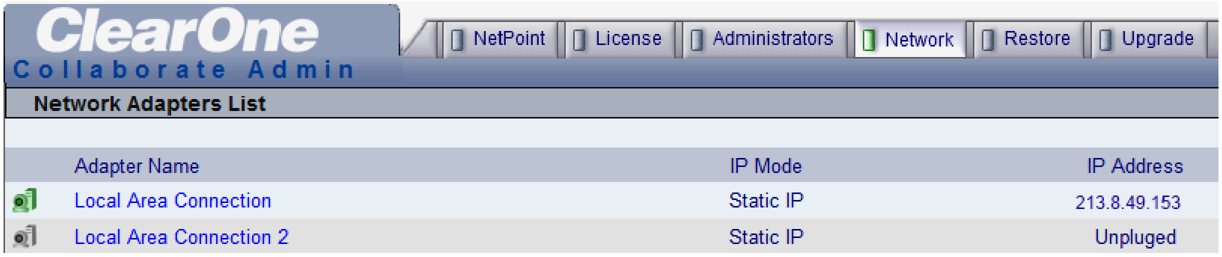
This procedure describes how to set a static IP Address when Netpoint is connected to the network, and has acquired a DHCP address.

From a remote computer connected to the network, connect to the Netpoint configuration application using an IE web browser.

CONFIGURING NETPOINT SERVER VIA NETPOINT ADMINISTRATION INTERFACE

1. Connect the network cable to GBE1.
2. Connect the VGA monitor and configure an IP address for the NetPoint server. Start your IE browser and point it to the NetPoint admin configuration screen at [IP address]/admin. The default user name/password is *admin*/*admin*.

3. In the NetPoint Admin Interface, select the **Network** tab. A list of available networks are displayed (green icon).

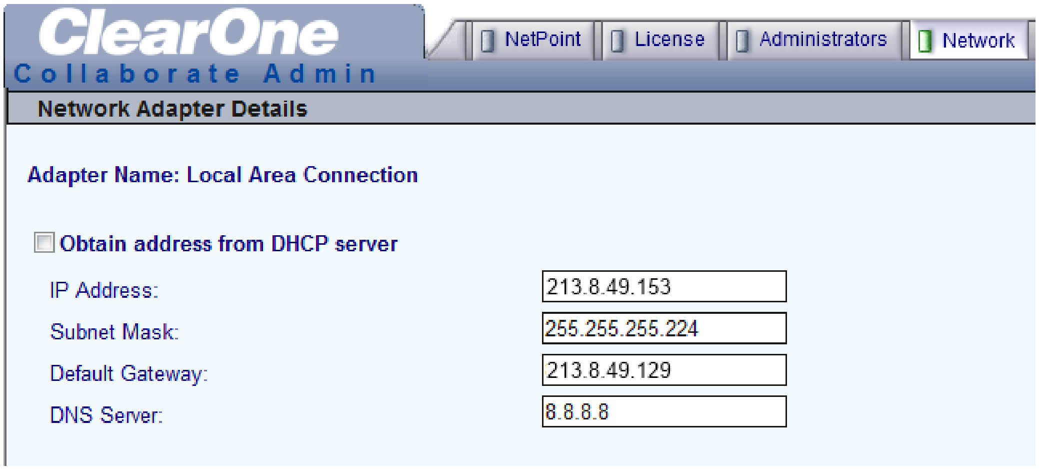


Network Adapters List

Adapter Name	IP Mode	IP Address
Local Area Connection	Static IP	213.8.49.153
Local Area Connection 2	Static IP	Unpluged

4. Click the first network (Local Area Connection) to open it for editing.

5. To set a static IP address, uncheck the **Obtain address from DHCP server** option.



Network Adapter Details

Adapter Name: Local Area Connection

□ Obtain address from DHCP server

IP Address:	213.8.49.153
Subnet Mask:	255.255.255.224
Default Gateway:	213.8.49.129
DNS Server:	8.8.8.8

6. Assign a static IP address by entering the following information :

- IP Address
- Subnet Mask
- Default Gateway

NOTE: DNS Server is optional.

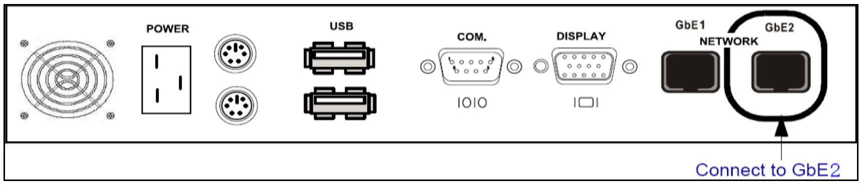
7. When you are done click **Apply** and connect the public network cable.

After completion, from another PC, start your IE browser and point it to the new NetPoint IP address.

Configuring the NetPoint Server by Interfacing with a PC

This procedure describes how to set a static IP address while connecting to the factory default GbE2.

1. Connect the network cable to GBE2.



2. Connect a crossover cable between interface GbE2 and a computer

   The interface of this IP configuration is:

   - IP address 10.0.10.10
   - Subnet mask 255.255.0.0
   - Gateway IP address 0.0.0.0

3. To access the NetPoint unit from another computer initially, the two systems must, at least temporarily, belong to the same network segment. That is, the first three fields of the address and the subnet mask must be identical.
   Write down the computer's current IP address and subnet mask so that you can restore them later.

4. Change the remote computer's IP configuration temporarily to the same IP address segment (10.0.10.x) and subnet mask listed in step 2.

5. On the computer, open a web browser and in the address field, enter the NetPoint's IP address/admin (10.0.10.10/admin).

6. Enter your login name and password. The default login name/password is *admin*/*admin*.

7. In the NetPoint Administrators Interface, select the **Network** tab. A list of network interfaces is displayed.

8. Click the GBE1 interface link. The Configuration page appears.

9. Assign a static IP address by entering the following information:

   - IP Address
   - Subnet Mask
   - Default Gateway

   NOTE: DNS Server is optional.

10. Click **Apply**.

11. Connect a network cable to the configured GBE1 and verify that the correct IP address appears.

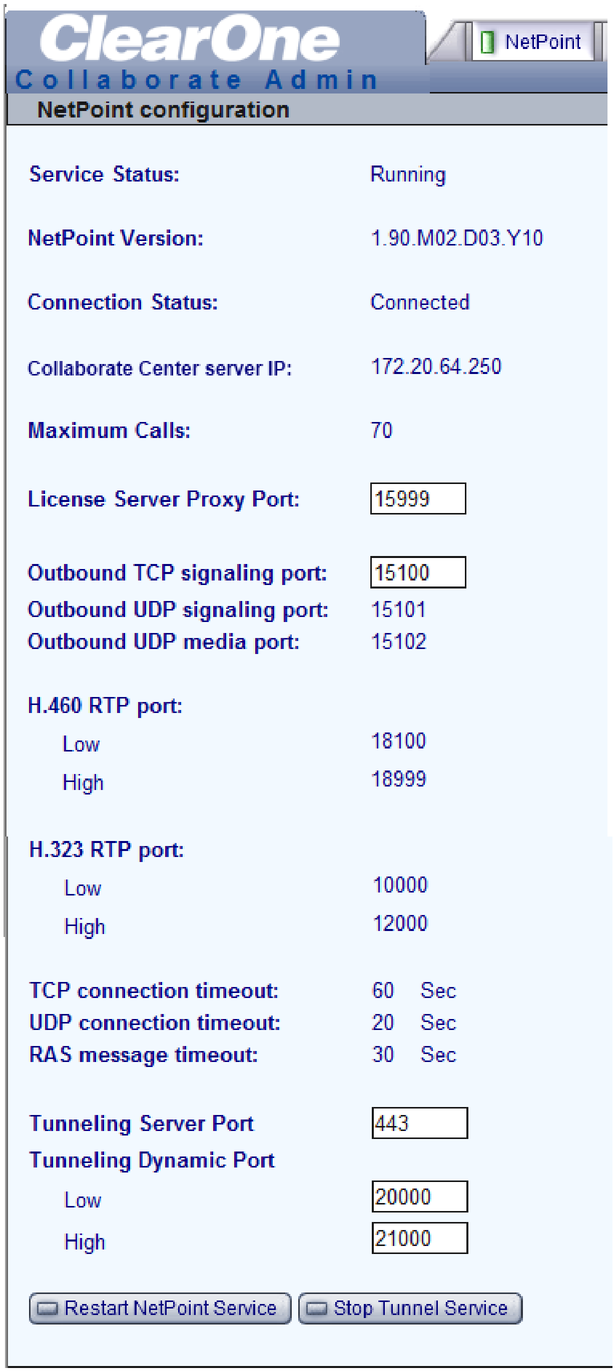
12. Restart the NetPoint server.

NOTE: In order to start working with the new IP, you must unplug the crossover cable from interface GbE2 during restart process.

LOGGING IN

Start your IE browser and point it to the NetPoint admin configuration screen at `[IP address]/admin`. The default user name/password is *admin*/*admin*.

MAIN SCREEN



NetPoint configuration

Service Status: Running

NetPoint Version: 1.90.M02.D03.Y10

Connection Status: Connected

Collaborate Center server IP: 172.20.64.250

Maximum Calls: 70

License Server Proxy Port: 15999

Outbound TCP signaling port: 15100
Outbound UDP signaling port: 15101
Outbound UDP media port: 15102

H.460 RTP port:
Low 18100
High 18999

H.323 RTP port:
Low 10000
High 12000

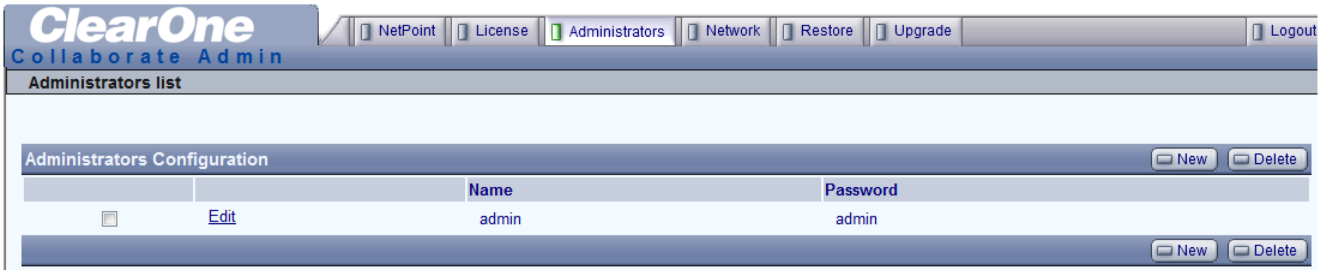
TCP connection timeout: 60 Sec
UDP connection timeout: 20 Sec
RAS message timeout: 30 Sec

Tunneling Server Port 443
Tunneling Dynamic Port
Low 20000
High 21000

Outbound TCP signaling port: If you decide to change the **Outbound TCP Signaling Port** before establishing the connection with NetPoint, click **Management Pages**, and change the port number in the NetPoint configuration page accordingly**. You also need to ask your system administrator to open new pinholes through three changed ports.**

ADMINISTRATORS

The Administrators tab enables you to manage NetPoint administrators. You can create, delete, and edit administrators' login credentials.



Administrators list

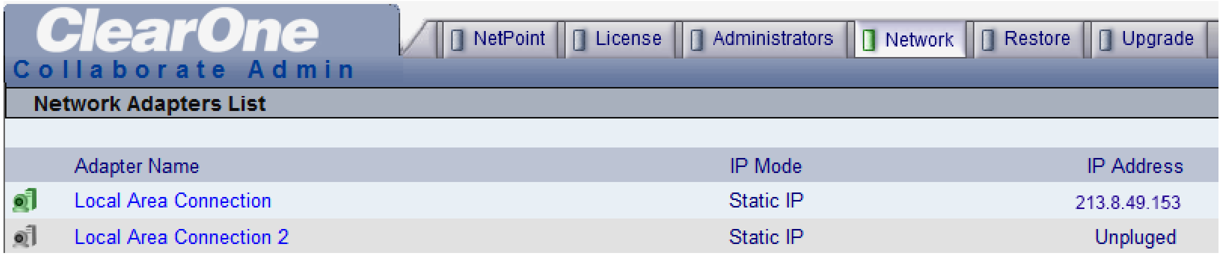
Administrators Configuration

		Name	Password
☐	Edit	admin	admin

- Click **New** to create a new admin.
- To delete an admin account, select the checkbox of the desired administrator and click **Delete**.
- To edit the login credential of an administrator, click **Edit**. Change the required parameters and then click **Update**.

NETWORK

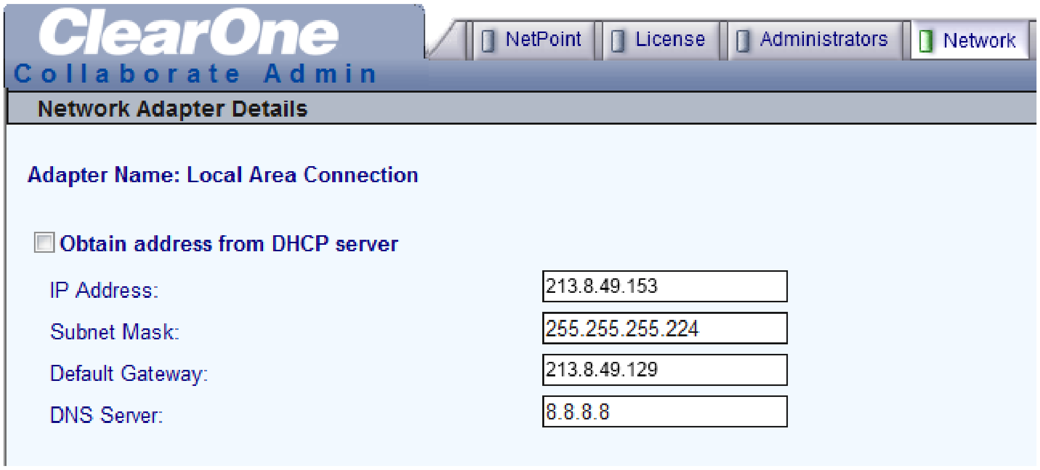
The Network tab displays a list of available networks (marked green), and enables you to set a static IP address when NetPoint is connected to the network and has acquired a DHCP address.



Network Adapters List

	Adapter Name	IP Mode	IP Address
🟩	Local Area Connection	Static IP	213.8.49.153
	Local Area Connection 2	Static IP	Unpluged

1. Click the desired Network to open it for editing.
2. To set a static IP address, uncheck **Obtain address from DHCP server**.



Network Adapter Details

Adapter Name: Local Area Connection

□ Obtain address from DHCP server

IP Address:	213.8.49.153
Subnet Mask:	255.255.255.224
Default Gateway:	213.8.49.129
DNS Server:	8.8.8.8

3. Assign a static IP address by entering the following information:
   - IP Address
   - Subnet Mask
   - Default Gateway.

   NOTE: DNS Server is optional, however, if configured it will allow you to switch between the EVC web applications without needing to login each time.

4. When you are done click **Apply**.

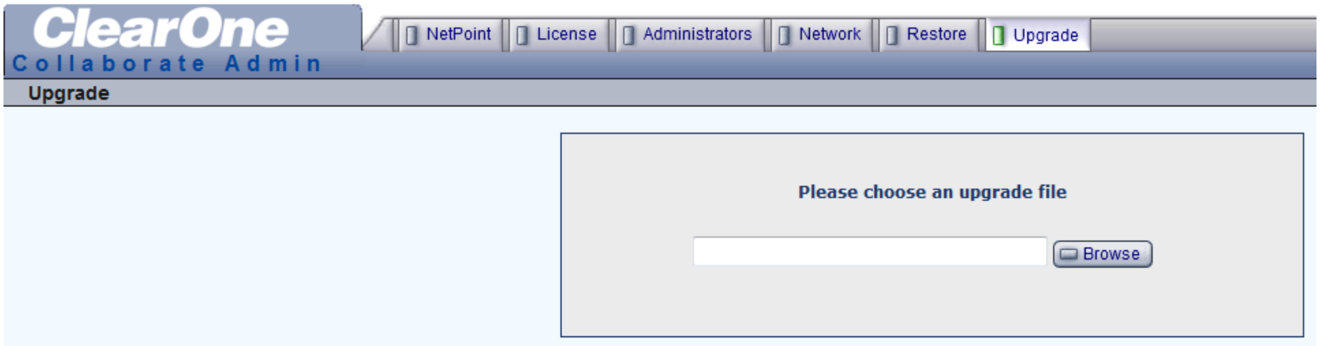
   NOTE: The configured NIC can be the one you are currently connected to or a different one.

UPGRADING

This feature enables upgrading the current NetPoint server version.

To upgrade the current NetPoint server version:

1. Log into **NetPoint Admin** and click the **Upgrade** tab.



Upgrade

Please choose an upgrade file

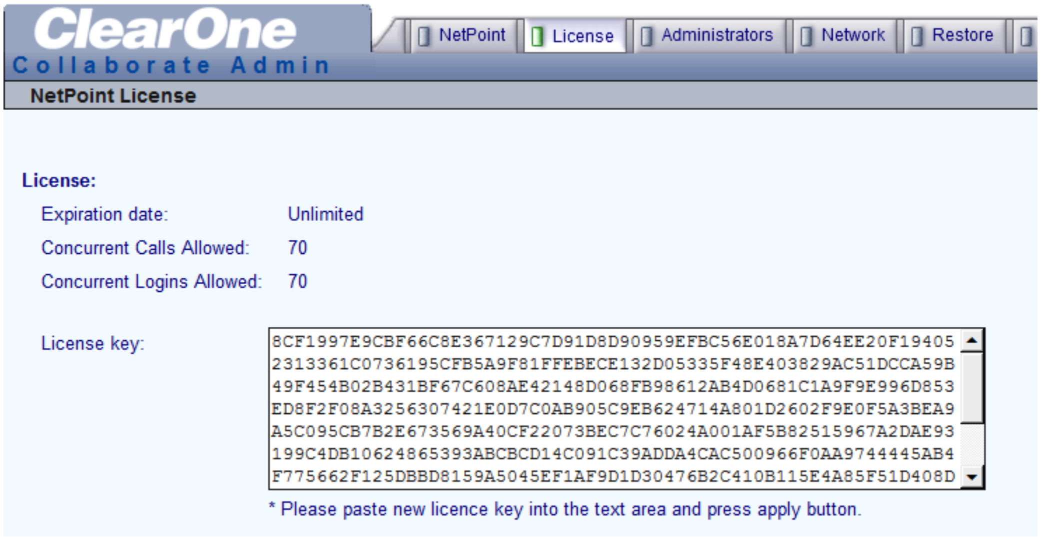
2. Select the upgrade file you previously received from ClearOne. (The extension of the file is .evc.)

3. Obtain and install a new license. For details on how to obtain and install a new license, see License on page 31.

LICENSE

To install a license:

1. Select the **License** tab.



NetPoint License

License:

Expiration date: Unlimited

Concurrent Calls Allowed: 70

Concurrent Logins Allowed: 70

License key:

```
8CF1997E9CBF66C8E367129C7D91D8D90959EFBC56E018A7D64EE20F19405
2313361C0736195CFB5A9F81FFEBECE132D05335F48E403829AC51DCCA59B
49F454B02B431BF67C608AE42148D068FB98612AB4D0681C1A9F9E996D853
ED8F2F08A3256307421E0D7C0AB905C9EB624714A801D2602F9E0F5A3BEA9
A5C095CB7B2E673569A40CF22073BEC7C76024A001AF5B82515967A2DAE93
199C4DB10624865393ABCBCD14C091C39ADDA4CAC500966F0AA9744445AB4
F775662F125DBBD8159A5045EF1AF9D1D30476B2C410B115E4A85F51D408D
```

* Please paste new licence key into the text area and press apply button.

2. Copy the temporary license key and send it by mail to your ClearOne sales representative.
3. You will receive a permanent license key form ClearOne. Delete the temporary license, and then copy and paste the permanent license key instead. When you are done, click **Apply**. The application will confirm the acceptance of the new license key.

LOG OUT

- Click the **Logout** tab to log out of NetPoint.

SHUT DOWN

- Click the **Shut Down** tab to shut down the NetPoint server.

RESTART

- Click the **Restart** tab to restart the NetPoint server.

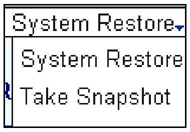
BACKUP / RESTORE

Netpoint provides a system backup and restore functionality to help recover the system if necessary.

The backup and restore functionality saves the baseline (factory default) configuration, creates a new snapshot of the Netpoint configuration once a week for 10 weeks, and enables you to manually create snapshots according to configuration changes.

At any time you can easily restore the default Netpoint configuration (as was set at ClearOne) or return to a specific configuration state.

Select the Action you want to perform:



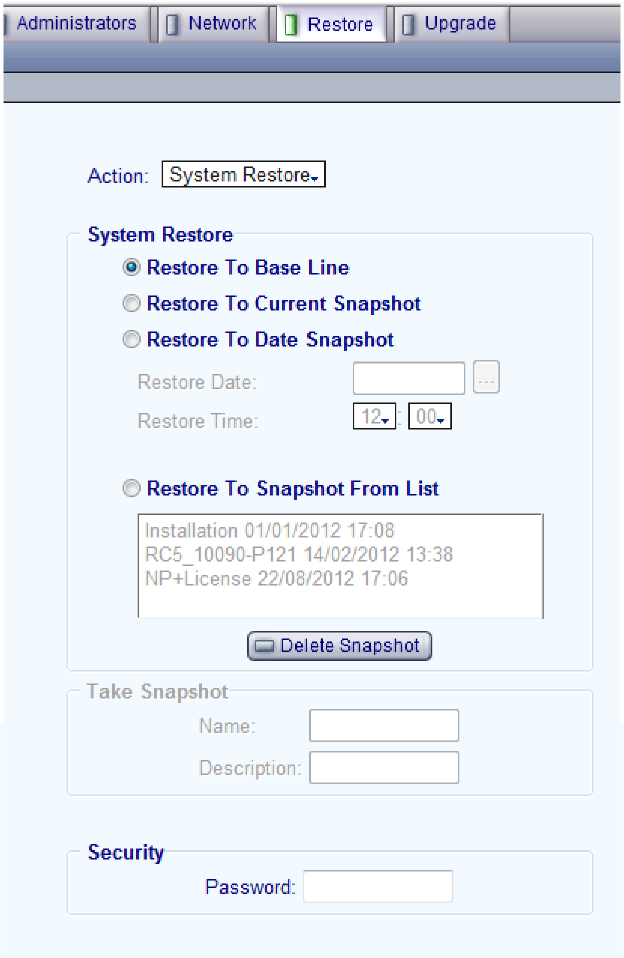
System Restore Restore the system configuration to the previously saved snapshot. A snapshot can be a baseline (factory default), a periodic snapshot created automatically by Netpoint, or a snapshot that was previously created by the system administrator.

Take Snapshot Take a snapshot of the current Netpoint configuration. It is recommended to take snapshots every time a configuration change is mad, e.g., adding new services, scheduling new meetings, etc.

SYSTEM RESTORE

To configure your restore options:

1. From the Action dropdown list, select **System Restore**.



Action: System Restore

System Restore

● Restore To Base Line

○ Restore To Current Snapshot

○ Restore To Date Snapshot

Restore Date:

Restore Time: 12 : 00

○ Restore To Snapshot From List

Installation 01/01/2012 17:08
RC5_10090-P121 14/02/2012 13:38
NP+License 22/08/2012 17:06

Take Snapshot

Name:

Description:

Security

Password:

2. Select the Restore option:

Restore To Base Line Restore the system configuration to the factory default snapshot (base line), or a newly created base line snapshot. The base line snapshot is the basic snapshot to which the system can be restored at any time.

Restore To current Snapshot Restore the system configuration to the latest snapshot.

Restore To Date

Restore the system configuration to a snapshot that was taken on a specific date. For example, if configuration changes were made and you want to restore the Netpoint configuration to the state before these changes.

Restore To Snapshot From List

Restore system configuration to a specific snapshot that was created previously. Each snapshot represents a different configuration state.

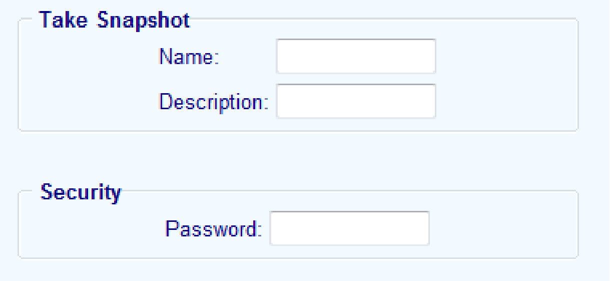
Password

Enter the password for the Netpoint backup and restore actions to ensure that only authorized administrators can restore the Netpoint configuration. The default password is 1234.

3. Click **Apply**.

Take Snapshot

After making configuration changes to Netpoint (e.g., changing network settings, updating license, or performing a periodic backup) it is recommended to take a snapshot of the Netpoint configuration.



To take a snapshot:

1. Enter a name for the snapshot. This name appears in the **Restore to Snapshot From List** area.
2. Enter a snapshot description which describes the configuration state of Netpoint.
3. Enter a password in order to ensure that only authorized administrators can backup and restore Netpoint. The default password is 1234.

DELETE SNAPSHOT

This option enables you to delete a snapshot from the list.

Select the desired snapshot and click **Delete**.

> NOTE: Some snapshots (i.e., base line snapshots and snapshots that are automatically created by the upgrade process) are locked, and cannot be deleted.