Policy Controller Configuration Management

What’s new in the (I)SN08 release?

The Policy Controller is a new component for the (I)SN08 release.

Configuration management overview

After a Policy Controller has been installed and commissioned into your CS 2000 network, use the procedures in this NTP to perform configuration management activities on the Policy Controller.

> ***Note:*** For procedures to install and commission a Policy Controller platform or its applications, refer to the Installation Method *Session Policy Controller Installation and Commissioning*, IM 35-0493.

You can provision and configure a Policy Controller through the Policy Controller Web GUI, or through XML procedures from...

Configuration management limitations and restrictions

The following limitations and restrictions apply when performing configuration management of the Policy Controller for all Carrier Voice over Internet Protocol (VoIP) solutions.

- The Policy Controller’s two GUIs (the Policy Controller Web GUI and the CS 2000 NCGL Platform Manager) do not support access over a NAT'd connection. Only SSPFS web proxied connections are supported. For more information about these configuration limitations, consult your site network engineering guidelines and site network administrator.
- If you are configuring the Policy Controller from the Web GUI, you cannot enter the value "0" at the start of a numerical entry unless

the value for that field is "0". For example, "089" will not be accepted, while "89" will be accepted.

- In Policy Controller release one, Premium Network Service Class is the only Network Service Class available for the SN08 release, therefore the following conditions apply:
  - — Premium is set to 100% and all four service classes are set to 0, because voice calls are tagged as Premium.
  - — In the XML commands, <NNSC> does not appear in <UpBWInfo> or <DownBWInfo>.

Tools and utilities

Re-provisioning of the Policy Controller or changing of the Policy Controller’s existing settings is performed using a number of interfaces depending on the activity required. The interface needed is described at the beginning of the applicable procedure. The following interfaces are used to perform the tasks described in this NTP:

- the Policy Controller Configuration GUI, a client Web browser application
- the CS 2000 NCGL Platform Manager GUI, a client web browser application
- the NCGL command line interface (CLI)

Client web browser requirements

For provisioning and maintaining the Policy Controller the following client web browsers are supported:

Supported web clients on a Windows 2000, XP, or 2003 based PC:

- Internet Explorer 6.0 SP1 and above
- Netscape 6.2.3+, and Netscape 7.1+

Supported web clients on a Solaris 8-based Sun workstation:

- Netscape 6.2.3+
- Mozilla 1.4+

The following browsers are NOT supported by Policy Controller:

- Any browser running on a Linux operating system
- Any browser running an OS under VMware
- Any browser running under Solaris operating system on a PC
- Any browser running on MacIntosh hardware

Accessing Policy Controller GUIs and CLIs

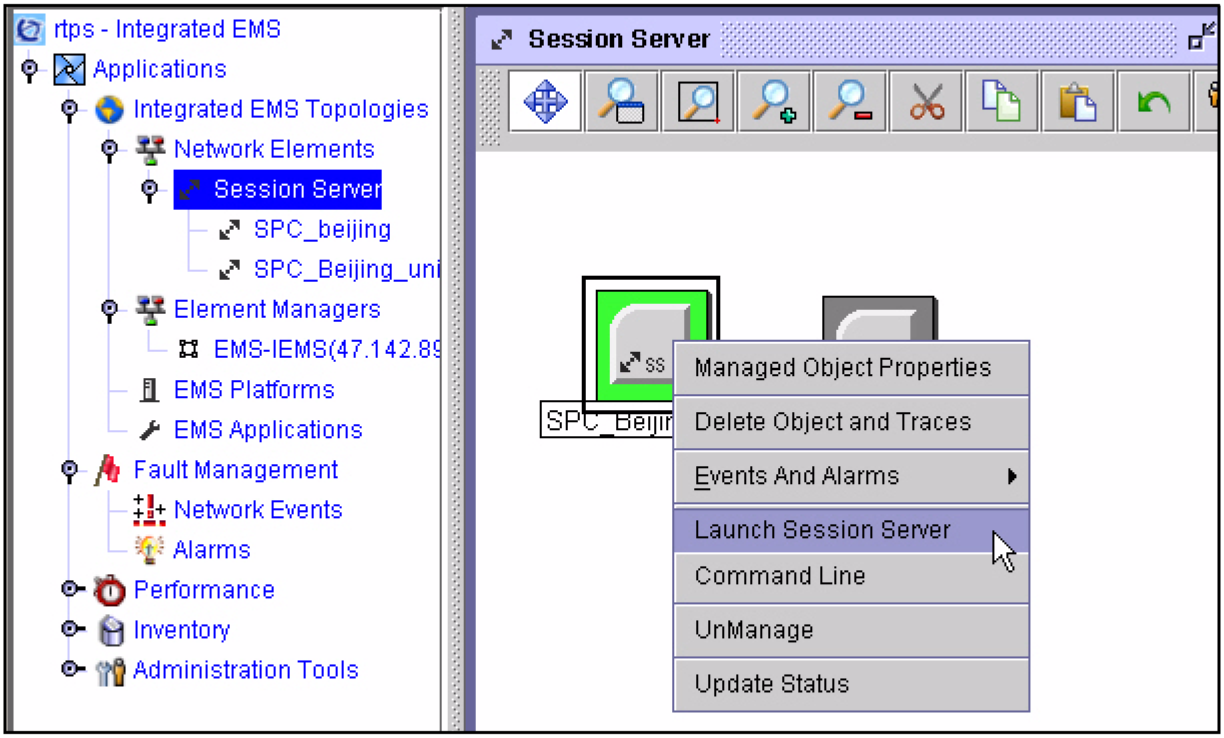
The Policy Controller can be configured so that it is accessed from the Integrated Element Manager System (Integrated EMS) between the customer operation LAN and the CS 2000 call server LAN. It can also be configured without the Integrated EMS because the Policy Controller functions as its own element manager. This means that provisioning for a Policy Controller takes place on the Policy Controller node itself.

The operating company personnel use a web-based interface to perform the provisioning and maintenance activities. The web-based interface consists of a web server, running on both Policy Controller units, that provides web pages for performing OAM&P activities.

There are three primary methods for accessing Policy Controller user interfaces:

- All GUI and CLI interfaces to the Policy Controller GUI can be accessed by selecting and right-clicking on the active Policy Controller element from the Integrated EMS expanded Network Elements view, as shown below.

Accessing Policy Controller GUIs or CLI from the Integrated EMS



For more information, refer to procedure *Access the CS 2000 Policy Controller GUIs from the Integrated EMS*, found in NTP *Policy Controller Security and Administration*, NN10346-611. For more information about using the Integrated EMS service, refer to NTP *Integrated EMS Basics*, NN10329-111.

- All GUI interfaces to the Policy Controller can be accessed from a remote system known to the proxy server (running on CS 2000 Management Tools server) on the CS-LAN.
- For commissioning purposes, the CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the Policy Controller by way of SSH/telnet access through the SSPFS server.

  The CLI can also be accessed using a console connected to the rear of the Policy Controller active unit. In some cases, this connection is wired to a terminal box. Refer to section Attach a VGA monitor and keyboard console on page 10 for more information about using this method.

ATTENTION

For all methods of GUI access, 1st party cookies (cookies that only get sent back to the originating server) must be enabled on the client system web browser to enable logging onto the Policy Controller; however, 3rd party cookies (cookies that can be read by servers other than the originating server) can be disabled.

ATTENTION

For all methods of GUI access, only HTTPS (HyperText Transport Protocol Secure) access is allowed. For security reasons, HTTP (HyperText Transport Protocol) access is not supported on the Policy Controller.

ATTENTION

Pop-Up blocking should be either disabled or restricted to only allow pop-ups from the same server. If you must use Pop-Up blocking software, add the SSPFS server’s hostname/IP address to the software’s “no block” list. Please consult technical support or local IS services for more information on browser configuration policies and restrictions.

Policy Controller configuration

Configuring the Policy Controller in the call server network

There is one Policy Controller unit per CS 2000, with the following configuration:

In (I)SN08, the Policy Controller node hardware (SAM-XTS) unit is installed in either the SAMF or Call Control frames (CCF). On the CCF frame (NTRX51TA), a Policy Controller node (made up of two hardware units) is usually mounted below the STORM units. Alternatively, it can be placed in the SAMF frame (NTRX51HA), below the BIP power distribution unit.

Each Policy Controller node is labeled for identification. Most often, the naming identification should be similar to the hostname of the node made during commissioning of the node.

Configuring Network Virtual Call Admissions Control (NVCAC)

In (I)SN08, the Policy Controller takes over responsibility for Network Virtual Call Admissions Control (NVCAC) from the Gateway Controller.

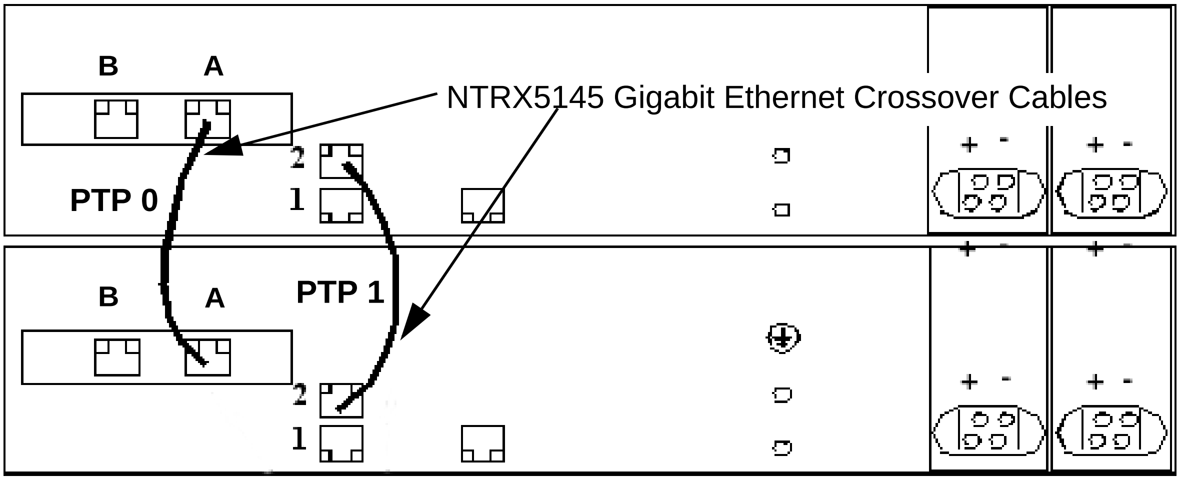
If you are already using Basic VCAC, you need to migrate to Network VCAC and configure the Policy Controller to run Network VCAC. If you are installing Network VCAC for the first time, you also need to configure the Policy Controller to run Network VCAC. For these procedures, refer to Activating Network VCAC on the Policy Controller on page 13.

Connecting Policy Controller ethernet ports to the call server network

Each of the Policy Controller unit’s two gigabit ethernet interfaces (shown as link 0 and link 1) are directed to the CS 2000 LAN switch that routes call traffic and signaling on the customer’s private central office network. In addition, two ethernet interfaces, acting as Point To Point (PTP) links, connect unit 0 to unit 1.

The following figure shows a rear view of a Session Sever unit chassis and the location of the ethernet connections.

Ethernet ports and cable connections for Policy Controller units



Notes about ethernet ports:

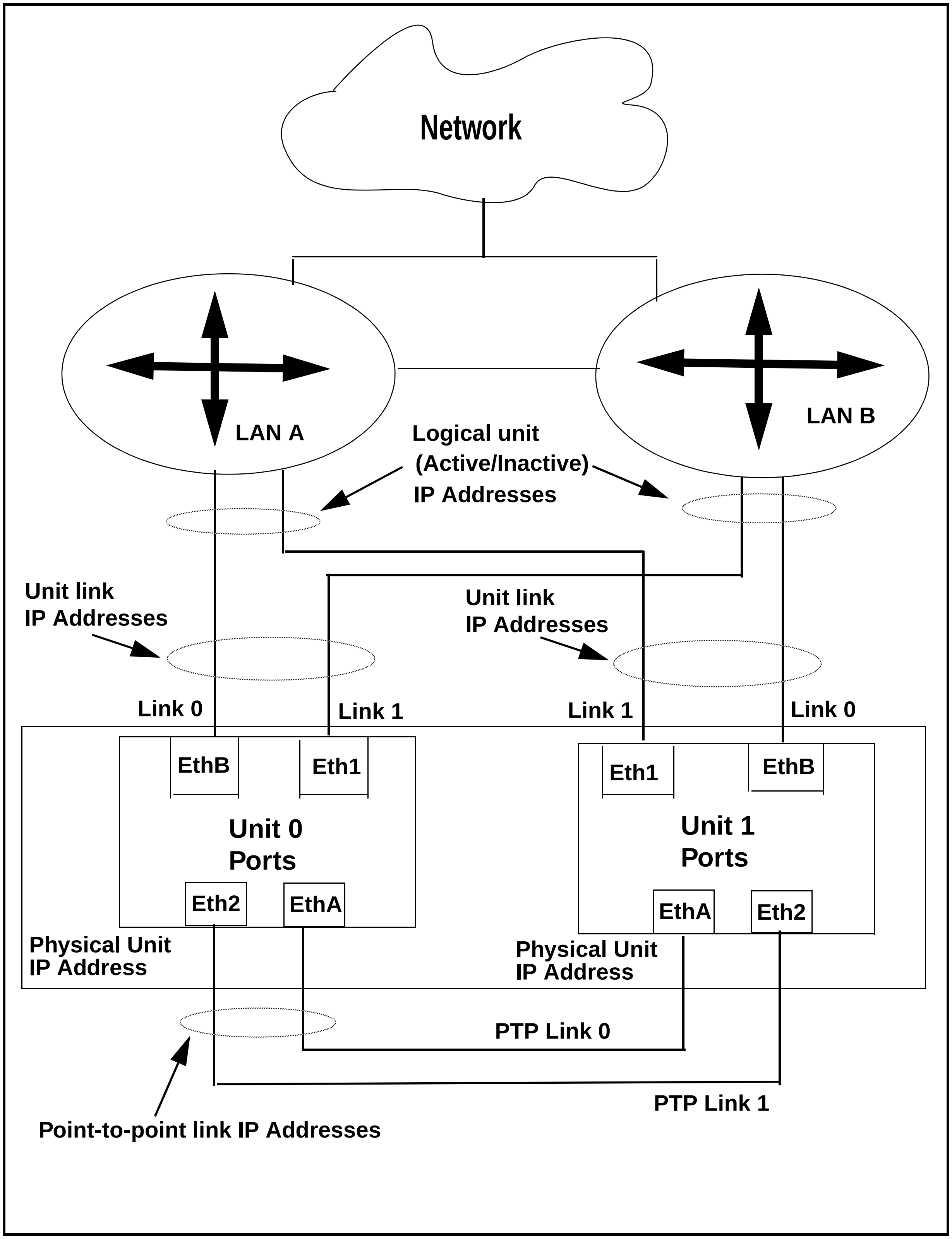
Ports 1 and B (both sets) go to CS-LAN Switch

Ports 2 (PTP1) and A (PTP0), on both units, are used for point-to-point connections between Policy Controller units

Mapping IP addresses and links to physical ethernet ports

The following figure shows the port and link configuration for both the Policy Controller units. Port ethB of each unit is connected directly to a LAN switch, while port eth1 is connected to the redundant LAN switch. Ports ethA and eth2, found on each unit, are cross-connected to the mate ports on the mate units. This configuration is used to support full network redundancy between both units and between the units and the network.

Physical map of Policy Controller ethernet links and ports to IP addresses



Understanding Policy Controller node IP addressing

All the physical ethernet ports on each unit are assigned an IP address. Together both units use a block of eight consecutive IP addresses all on the same subnet as the Call Server (CS) LAN. Address usage is assigned as follows:

- Four IP addresses, one for each physical ethernet port
- Four IP addresses, an active and inactive logical address per unit
- Two internal IP addresses, one for each end of the point-to-point connections

The unit 0 and unit 1 IP physical addresses are specified by the user during the commissioning process for that unit as determined by requirements at the customer site with assistance from the IP solution Network Engineering Guidelines. The rest of the IP addresses are generated by the system based on the unit 0 physical IP address. Note the last octet of the active IP address must be divisible by 8.

Sample IP addressing scheme for a Policy Controller node

Policy Controller IP addresses	Example unit IP address scheme	Datafilled or generated by:	Description
Active unit	172.16.16.72[a]	system	Logical unit
Inactive unit	172.16.16.71	system	Logical unit
Unit 0	172.16.16.67	user	Physical unit 0
Unit 0, Link 0	172.16.16.65	system	Physical unit link
Unit 0, Link 1	172.16.16.66	system	Physical unit link
Unit 1	172.16.16.70	user	Physical unit 1
Unit 1, Link 0	172.16.16.68	system	Physical unit link
Unit 1, Link 1	172.16.16.69	system	Physical unit link
Local PTP link 0	192.168.1.1[b]	system	Local point to point link
Mate PTP link 1	192.168.1.2	system	Mate point to point link

[a] The active node’s last set of digits must be the highest address and must be divisible by 8.

[b] The IP addresses 192.168.1.1 and 192.168.1.2 are generated by the system and assigned to the local and mate unit Point to Point (PTP) links. To avoid conflict, do not assign the same IP address to the mate PTP link on the mate unit.

Procedures for managing Policy Controller GUI access using IEMS

Most configuration activities for setting up the Policy Controller GUIs and CLI to be accessible from the Integrated EMS are performed using the Integrated EMS Configuration Management NTP, NN10330-511.

Procedures for managing Policy Controller Application software

Refer to Upgrading the Policy Controller NTP, NN10431-461, for detailed information about reinstalling the Policy Controller application as part of a maintenance release upgrade activity.

Attach a VT-100 console monitor to the RJ-45 serial port

Use the following procedure to attach a VT-100 monitor (or emulator) or input to a serial box to the rear of a Policy Controller chassis for use as a console monitor using an RJ-45 serial connector (Nortel PEC NTRX5178). This may be required to isolate faults or to assist in commissioning activities.

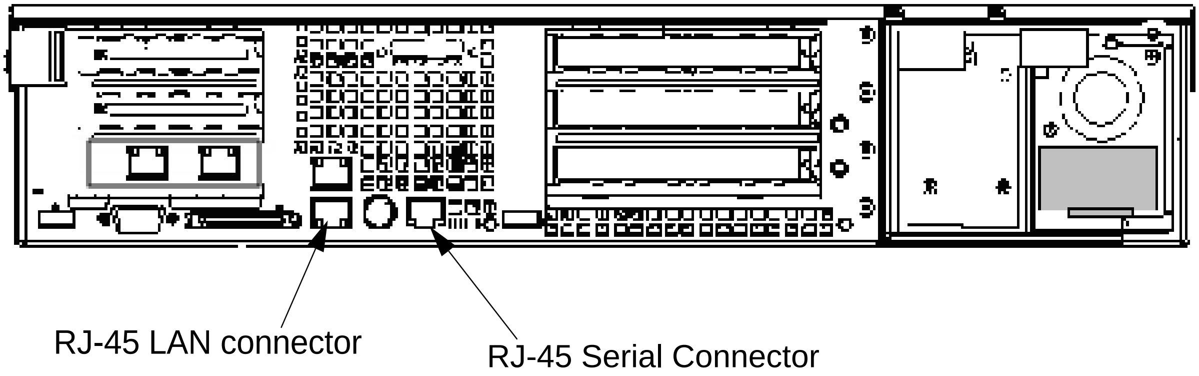
Use this procedure when the Policy Controller platform NCGL is not fully configured.

At the rear of the Policy Controller chassis.

1 Attach the VT100+ terminal to the serial port using the diagram shown below

> ***Note:*** Ensure that the Policy Controller RJ-45 Serial cable is connected to the serial port on the rear of the unit and not the RJ-45 LAN connector. It should be connected to a VT-100 capable console device such as a PC or laptop running a VT-100 terminal communications session into the RJ-45.

Rear view of Policy Controller chassis



2 The procedure is complete.

Attach a VGA monitor and keyboard console

Use the following procedure to attach a VGA monitor and PS/2 style keyboard into the rear of a Policy Controller chassis for use as a console monitor.

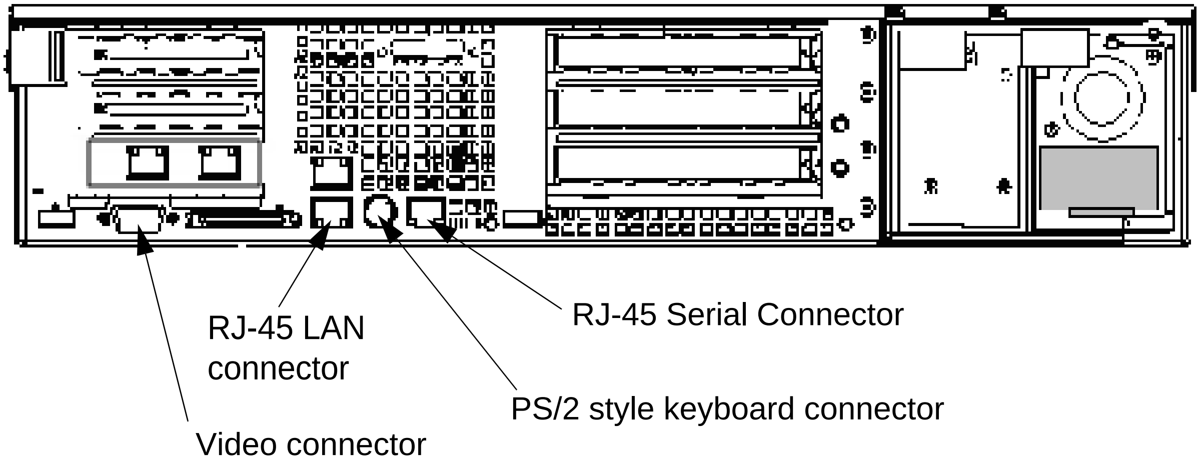
> **ATTENTION**
>
> You cannot use this method to fully commission a Policy Controller unit. Instead, use method Attach a VT-100 console monitor to the RJ-45 serial port on page 9.

At the rear of the Policy Controller chassis.

1 Plug in a PS/2 style keyboard and VGA monitor into the rear of the Policy Controller chassis using the diagram shown below.

Note: Optionally use a dongle (Y cable) to connect both keyboard and mouse to the same PS/2 mouse/keyboard port.

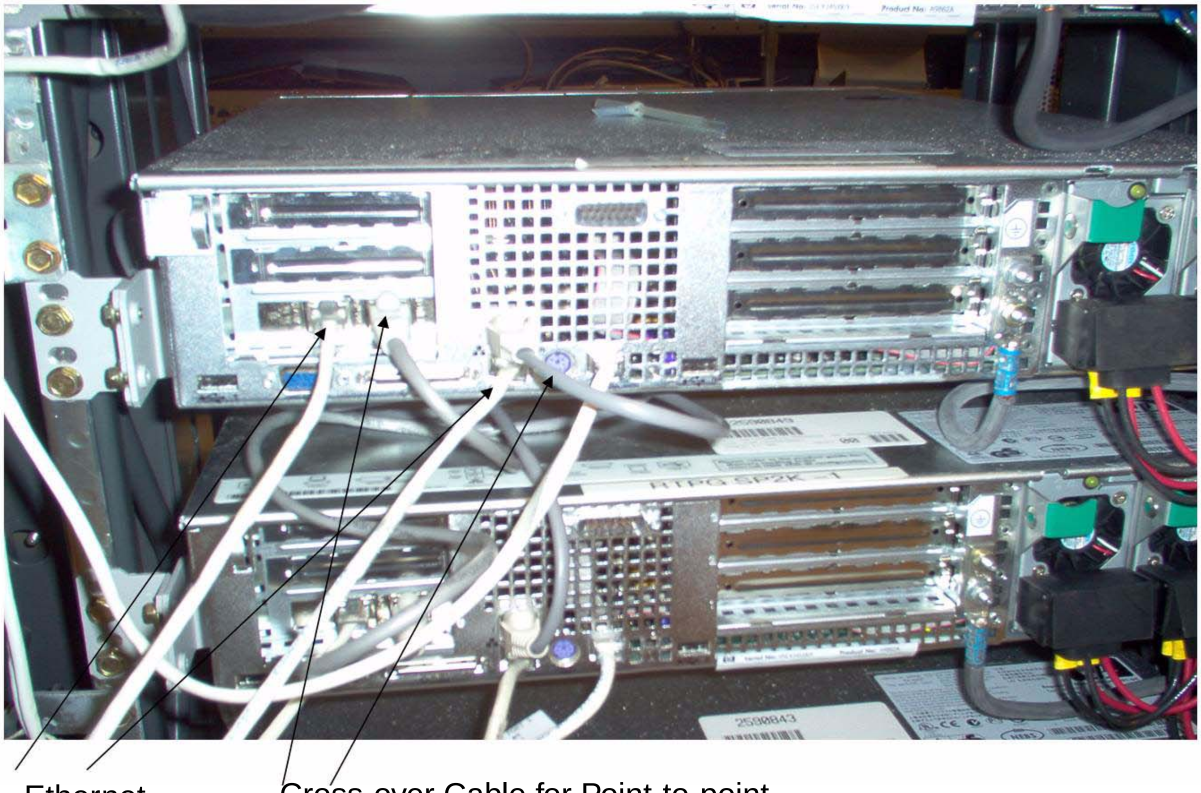
Rear view of Policy Controller chassis



2 The procedure is complete.

Checking ethernet cabling at the rear of the Policy Controller units

Each Policy Controller is configured with two 1000Mbs/100Mbs/10Mbs interfaces directed to the LAN switch, as represented by link 0 and link 1. Configuration depends on the IP router configuration. In addition, two interfaces connect unit 0 to unit 1, as shown as the Point To Point (PTP) link.



Ethernet Connectivity interface to the CS LAN

Cross-over Cable for Point-to-point connectivity between two units in the same node.

Activating Network VCAC on the Policy Controller

Purpose of this procedure

Virtual Call Admissions Control (VCAC) is a quality of service (QoS) mechanism that allows the Communication Server 2000 to cancel post-dial, pre-ringing calls that would overload a segment of the packet network. The SN07 release introduced Basic VCAC using the Gateway Controller for call admissions control.

In the SN08 release, Network VCAC enhances Basic VCAC and moves call admissions control from the Gateway Controller (GWC) to the Policy Controller. To enable Network VCAC on the Policy Controller you either have to migrate from Basic VCAC to Network VCAC, or if you were not previously using Basic VCAC, activate a new installation of Network VCAC.

Network VCAC depends on a logical model of the packet network made up of network zones. A network zone represents a Limited Bandwidth Link (LBL), Network Address Translation (NAT), or a composite NAT and LBL.

Use this procedure when:

- you are using Basic VCAC on your CS 2000 system and want to migrate to Network VCAC and activate it on the Policy Controller. Refer to procedure Migrating from Basic VCAC to Network VCAC on the Policy Controller on page 15.
- you have a new installation of Network VCAC and want to activate it on the Policy Controller. Refer to Activating Network VCAC on the Policy Controller without Basic VCAC on page 17.

Limitations and restrictions

This procedure has the following limitations and restrictions:

- During the migration from Basic VCAC to Network VCAC, do not perform any network zone provisioning until you activate Network VCAC on the Policy Controller.
- Activating Network VCAC is network-wide. You cannot operate both Basic VCAC and Network VCAC on your CS 2000 network.
- There is no provisioning connection between the Policy Controller and CS 2000 GWC Manager GUI in SN08. Therefore, you must provision all topology information first into CS 2000 GWC Manager GUI and then into the Policy Controller.
- If the Policy Controller application is not available, or the TCP connection between the Gateway Controller and the Policy

Controller is down, the call will be allowed to go through without any checks on bandwidth availability. Also, if the Policy Controller topology is queried about a particular link it does not know, it will reply with an error and the Gateway Controller will allow the call to proceed without any admissions control. These types of errors can degrade the VCAC application as they allow calls access to the network without accounting for them.

- The VCAC architecture has provisioning limits that are enforced by the provisioning system:
  - There is a maximum of five network links between a Gateway and the Service provider’s core network.
  - VCAC only uses the negotiated codec values for a call. For example, if a call has been setup with a codec of G729 (compressed, low bandwidth) and fax tones are detected on the Gateway which requires a switch to a codec of G711 (uncompressed, high bandwidth) or T.38 (special fax datastream), VCAC will ignore these changes and continue modelling the call as G729.
  - There is a requirement that voice traffic is prioritized over the data traffic. Also, VCAC does not model voice traffic and non-Policy Controller controlled data traffic on the same LBL. This is set up by careful modeling of the logical network, as a part of the system engineering.
  - Interactions with codec negotiation. In a network configured to use G729 as the preferred codec and G711 as the default codec, the originator offers a list of codecs to the terminator who chooses the codec the call uses. Initially, the Network VCAC application offers the worst case codec (G711) to the originator until the negotiated SDP is returned by the terminator. However, this means that it is not always possible to get the expected codec of G729 on a link. Detection is difficult because there is no guarantee that all calls will negotiate to G729.

Prerequisites

These procedures have the following prerequisites:

- Upgrade all Communication Server 2000 (CS 2000) components to the SN08 release before you begin this procedure. The CS 2000 system continues to support Basic VCAC over the upgrade from the SN07 release to the SN08 release until you activate Network VCAC. For upgrade procedures on CS 2000 components, refer to NTP *Upgrading a Carrier Voice over IP Network*, NN10440-450.
- Install and commission the Policy Controller with the SN08 release. For Policy Controller installation and commissioning procedures,

refer to Installation Method *Session Policy Controller Installation and Commissioning* (IM 24-0493) and this NTP *Policy Controller Configuration Management* (NN10432-511)

- If you are migrating from Basic VCAC to Network VCAC, you must already be operating Basic VCAC on your CS 2000 network—ensure the Basic VCAC SOC value is set to ON. For new installations of Network VCAC, ensure that the VCAC SOC is enabled.

Action

ATTENTION

All NAT, LBL, and composite NAT-LBL zones must be configured identically and in the same order first on the CS 2000 system and then on the Policy Controller. If you change a network zone attribute on the CS 2000 system, you must immediately change it on the Policy Controller. Otherwise, Network VCAC will not function correctly.

For the CS 2000 system network zone GUI configuration information, refer to NTP *Gateway Controller Configuration Management* (NN10205-511). For the CS 2000, use this NTP to configure the network zones on the Policy Controller.

Migrating from Basic VCAC to Network VCAC on the Policy Controller

At the CS 2000 GWC Manager /OSSGate interface/Policy Controller

1 After the CS 2000 components are upgraded to the SN08 release, do not make any changes to the network zones (NAT, LBL, and composite NAT-LBL zones) on the CS 2000 system until the switch to Network VCAC on the Policy Controller is complete. This restriction maintains consistency of the topology data on the CS 2000 system and the Policy Controller and ensures Network VCAC will work correctly.

2 Ensure that you have the network zone details (all NAT, LBL, and composite NAT-LBL zones) available from the CS 2000 system.

Get a detailed list of network zones currently provisioned in the CS2000 system by querying all network zones names, IDs and network zone parents.

For the GUI procedure, refer to the procedure “View a network zone ID” from NTP *Gateway Controller Configuration*

Management (NN10205-511). For the XML procedure, use the XML command “queryNetworkZone” from NTP *OSSGate User’s Guide* (NE10004-512).

3 Use the network zone data (network zone name, ID, and parent name) that you obtained from the CS 2000 system to provision network zones on the Policy Controller. The network zone data that you enter on the Policy Controller must be identical and in the same order as the network zone data currently on CS 2000 system. You must add a parent network zone before its child network zone. To ensure a network zone match between the CS 2000 system and the Policy Controller, you must manually verify that the network zone data is identical in both.

You can use either the GUI or XML procedure to add a network zone on the Policy Controller. For more information on adding a network zone from the Policy Controller, refer to the procedure Add network zone on page 69 in this NTP.

4 Add and provision the Policy Controller into the CS 2000 system, which allows the CS 2000 system to establish connections to the Policy Controller. Confirm that the Policy Controller is functioning correctly, that its TCP links to the CS 2000 system are working, and no alarms have been generated.

For the GUI procedure, refer to procedure “Add a Policy Controller” in NTP *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure and the commands, refer to the NTP *OSSGate User’s Guide* (NE10004-512).

5

ATTENTION

To minimize disruption to the network, perform the switch to Network VCAC during a period when there are fewer calls.

Using the GUI procedure or the XML command, switch ON Network VCAC. When Network VCAC is activated, the CS 2000 system stops running Basic VCAC, and switches to using the Policy Controller for Network VCAC policy decisions.

For the GUI procedure, refer to procedure “Change the Network VCAC status” in NTP*Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, refer to the NTP *OSSGate User’s Guide* (NE10004-512).

When the Network VCAC is activated, all calls trigger bandwidth management through the Policy Controller. There is no current bandwidth status between Basic and Network VCAC so the Policy Controller will have no knowledge of existing calls that were set up under Basic VCAC. This condition can lead to temporary degradation of voice quality on some calls.

6

> **ATTENTION**
>
> The provisioning restrictions have changed in SN08. In SN08, it is possible to mix agent types (IAD, CICM, H323) behind a common link. Changes to agent types will not survive a rollback, so do not make any changes to the network zone topology until Network VCAC has had sufficient time to soak and be tested.

Verify call processing to confirm Network VCAC on the Policy Controller is functioning correctly. Monitor for logs that indicate a problem. Before making any network zone topology changes, allow the system to soak for a period of time so potential errors can appear and be corrected.

7 When the system is functioning correctly, you can then make changes to the network zone data in the CS 2000 system and the Policy Controller. Ensure that all network zone changes are entered identically first on the CS 2000 system and then on the Policy Controller to manually keep them in synchronization going forward. Otherwise, there will be a network zone topology mismatch and calls will fail.

For GUI procedures to add network zones and change network zone attributes for the CS 2000 system and the Policy Controller, refer to the latest version of NTP*Gateway Controller Configuration Management* (NN10205-511) and this NTP. For the XML procedures, refer to NTP *OSSGate User's Guide* (NE10004-512).

8 You have completed this procedure. If you have a problem with Network VCAC and need to rollback to Basic VCAC, refer to procedure Rollback Network VCAC to Basic VCAC on page 23.

Activating Network VCAC on the Policy Controller without Basic VCAC

At the CS 2000 GWC Manager/OSSGate interface/Policy Controller

1 Ensure that the prerequisites are completed for this procedure — CS 2000 components upgraded to SN08 release, Policy

Controller installed and commissioned with SN08 release, VCAC SOC enabled.

Get a detailed list of network zones (NAT, LBL, or composite NAT-LBL zones) from the customer. You will use these network zones to provision the CS 2000 GWC Manager and the Policy Controller.

2 To correctly configure the Network Blocking – Normal Traffic (NBLN) treatment that Network VCAC uses when it blocks calls, datafill the following tables:

- Table Treatment Control (TMTCNTL). Refer to step a
- Table Treatment to Cause Map (TMTMAP). Refer to step b
- Table Flexible CAUSEMAP (FLXCMAP). Refer to step c

If a call fails because VCAC fails, you need to apply an NBLN treatment to the originating call agent of the node. If VCAC blocks an originating line or trunk, a LINE138 log report or TRK138 log report generates with treatment set to NBLN. The log reports identify the call originator and the dialed digits to help you determine the problem. For more information on these log reports, refer to NTP *DMS-100 Family Log Reference Manual*, 297-8021-840.

a Datafill table Treatment Control (TMTCNTL). Table TMTCNTL consists of the Treatments subtable (TMTCNTL.TREAT) that defines treatments assigned to lines. Datafill each treatment subtable with the following tuple:

NBLN Y S <tone>

Entry	Definition
NBLN	The treatment assigned.
Y	The event must be logged.
S	The tone is defined by Common Language Location Indentifier (CLLI).
<tone>	The preferred tone which is identified by the telco and played to the call originator. Use a standard tone, or a custom tone defined through table TONES. ***Note:*** You must set a tone instead of an announcement as there is not enough bandwidth to play the announcement.

CAUTION

The tuple in subtable TMTCNTL.TREAT must be set to **tone** instead of **announcements**. Otherwise, a treatment loop can result as there is insufficient bandwidth to play the announcement.

b

CAUTION

The treatment MUST NOT be played locally (NOLOCAL in the TMTMAP datafill examples below) if any of the trunks using this node are based on SIP or H323. This can cause a treatment loop as there is insufficient bandwidth to play the announcement.

CAUTION

The release cause MUST NOT allow immediate reattempts. If the terminating line/trunk is blocked, a reattempt will create a release loop as a different incoming trunk member will be attempted.

Datafill table Treatment to Cause Map (TMTMAP). TMTMAP maps signalling protocols and treatments to call failure messages. Datafill this table to determine if the preceding exchange reports the treatment or if the switch applies the treatment locally. There is no dedicated VCAC release cause for protocols. However, each protocol does contain a number of release causes that are appropriate for VCAC. It is up to the telco to identify a release cause that will map into their signaling network.

The following examples are table TMTMAP datafill entries:

Q764 NBLN ALLBC ISUP NOLOCAL NORMUNSP LOCLNET Y

Q767 NBLN ALLBC ISUP NOLOCAL NORMUNSP LOCLNET Y

Q931 NBLN ALLBC PRI NOLOCAL NORMUNSP LOCLNET Y

In the above examples, Qxxx NBLN is the protocol pair, NOLOCAL indicates the treatment is not played locally, NORMUNSP is the release cause, and Y signals the treatment will be logged.

> ***Note:*** For more information about table TMTMAP, refer to NTP *Succession Networks Operational Configuration: Data Schema Reference*, NN10324-509.

The datafill examples above will send the release cause Normal Unspecified to the originating node. The originator of the call will hear a treatment specific to that release cause, and not the NBLN treatment used on the terminating node. It is up to the telco to arrange the mappings from the line treatment to tone and release causes to tone if they require consistent tones for both line and trunk Network VCAC failures.

c Datafill table Flexible CAUSEMAP (FLXCMAP) to map release causes to treatments. For example, if the release cause is NORMUNSP, then the datafill entry in table FLXCMAP would look like the following entry:

NORMUNSP CCITT_STANDARD RODR N

This example maps the NORMUNSP to the reorder (RODR) treatment. The RODR treatment is used to index into table TMTCNTL to identify what the user hears.

> ***Note 1:*** For more information about table FLXCMAP, refer to NTP *Succession Networks Operational Configuration: Data Schema Reference*, NN10324-509.
>
> ***Note 2:*** In multi-node scenarios, the telco is responsible for configuring the signaling to ensure the NBLN treatment can reach the originator. If any node does not support Network VCAC or does not have the SOC enabled, the NBLN treatment may be unavailable in this scenario. In this case, the originator receives a treatment based on the release cause that reaches the originating node instead.
>
> ***Note 3:*** If the originating gateway does not support the release cause or the audible signal (for example, MGCP or

H.248) that it is mapped to, the originator may not hear any tone when the NBLN treatment is provided.

ATTENTION
The datafill examples in step 2a, b and c are examples only. There are regulatory requirements for the behavior of signaling links and each customer can have different requirements for the mapping of release codes to treatments, and for the management of their signaling network.

3

ATTENTION
To minimize disruption to the network, activate Network VCAC during a period when there are fewer calls.

From the CS 2000 GWC Manager GUI or using the XML command, switch ON Network VCAC.

For the GUI procedure, refer to procedure “Change the Network VCAC status” in the latest version of NTP*Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, refer to NTP *OSSGate User’s Guide* (NE10004-512).

When Network VCAC is activated, all calls will trigger bandwidth management through the Policy Controller.

4 Use the network zone data that you obtained from the customer to provision network zones on the Policy Controller and the CS 2000 GWC Manager. The network zone data that you enter on the Policy Controller must be identical and in the same order as the network zone data you enter into the CS 2000 GWC Manager. You must add a network parent zone before its network child zone. To ensure a network zone match between the systems, you must manually verify that the network zone data is identical in both.

You can use either the GUI or XML procedure to add a network zone from the Policy Controller. For more information on adding a network zone from the Policy Controller, refer to the procedure Add network zone on page 69 in this NTP.

5 Add and provision the Policy Controller into the CS 2000 system, which allows the CS 2000 system to establish connections to the Policy Controller. Confirm that the Policy Controller is functioning correctly, that its TCP links to the CS 2000 system are working, and no alarms have been generated.

For the GUI procedure, refer to procedure “Add a Policy Controller” in the latest version of NTP *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure and the commands, refer to NTP *OSSGate User’s Guide* (NE10004-512).

6

ATTENTION

The provisioning restrictions have changed in SN08. In SN08, it is possible to mix agent types (IAD, CICM, H323) behind a common link. Changes to agent types will not survive a rollback, so do not make any changes to the network zone topology until Network VCAC has had sufficient time to soak and be tested.

Verify call processing to confirm Network VCAC on the Policy Controller is functioning correctly. Monitor for logs that indicate a problem. Before making any network zone topology changes, allow the system to soak for a period of time so potential errors can appear and be corrected.

7 When the system is functioning correctly, you can then make changes to the network zone data in the CS 2000 system and the Policy Controller. Ensure that all network zone changes are entered identically first on the CS 2000 system and then on the Policy Controller to manually keep them in synchronization going forward. Otherwise, there will be a network zone topology mismatch and calls will fail.

For GUI procedures to add network zones and change network zone attributes for the CS 2000 system and the Policy Controller, refer to the latest version of NTP*Gateway Controller Configuration Management* (NN10205-511) and this NTP. For the XML procedures, refer to NTP *OSSGate User’s Guide* (NE10004-512).

8 You have completed this procedure.

Network VCAC rollback to Basic VCAC

Use this procedure to abort the switch to Network VCAC from Basic VCAC and rollback to Basic VCAC.

> **ATTENTION**
> Only perform a rollback from Network VCAC to Basic VCAC during the period when you are preventing changes to the network zone topology in the CS 2000 system (up to step 7). Otherwise, network zone topology mismatches can occur between the CS 2000 system and the Policy Controller, causing Basic VCAC to work incorrectly.

Rollback Network VCAC to Basic VCAC

At the CS 2000 GWC Manager GUI/OSSGate interface

1 Deactivate Network VCAC in the CS 2000 system. For the GUI procedure, refer to the procedure “Change the Network VCAC status” in the latest version of NTP*Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, refer to NTP *OSSGate User’s Guide* (NE10004-512).

After Network VCAC is deactivated, the CS 2000 system will manage bandwidth. The bandwidth status does not transfer from the Policy Controller to the CS 2000, which can lead to temporary degradation of voice quality on calls. As existing calls clear, potential problems are removed.

2 You have completed this procedure.

VCAC deactivation

If there is a serious VCAC malfunction, disable the VCAC SOC functionality. Basic and Network VCAC will be not function.

Inter-domain SIP-T versus Intra-domain SIP-T

When VCAC blocks a SIP-T call, the call release can be initiated locally or from the switch on the other end of the trunk, depending on whether the trunk is intra-domain or inter-domain.

If the SIP-T trunk is intra-domain, we assume that the switch on the other end of the trunk understands VCAC. So on a call where the originator is behind an LBL with not enough bandwidth to carry the call, we would let the call continue. The is because the terminator could be behind the same LBL as the originator, therefore eliminating the need to use the failing LBL, resulting in the call completing successfully. On the other hand, if the terminator is not behind the same failing LBL as the originator, VCAC would block the call. A call release message would then be sent in a backward direction using the release cause that is datafilled in table TMTMAP for the NBLN treatment.

If the switch on the other side of the SIP-T trunk does not understand VCAC, then an inter-domain trunk should be used instead of intra-domain. Failure to do so, can result in a ring-splash/ringing problem when a call is blocked by VCAC. For example, the MCS5200 does not understand the VCAC extensions, so if it is configured with an Intra-domain trunk, a call originator to it would hear ringing until answer, and then would be routed to treatment. This is because the MCS5200 uses slow start when it provides Session Description Protocol (SDP). A Gateway that uses fast start over the same configuration would result in the originator hearing a Ring splash before being routed to treatment

If the SIP-T trunk is inter-domain, we assume that the switch on the other end of a trunk does not understand VCAC. Therefore, any inter-domain SIP-T call originating from a gateway behind a low bandwidth link with not enough bandwidth to carry the call, will be blocked by VCAC before leaving the originating switch.

Interactions

VCAC can potentially affect any call. If there is insufficient resources for a call or call leg to complete then the call will be released, and the user is directed to a treatment.

VCAC can deny call admission whenever the speech path changes as in the following scenarios.

- Call Origination. After the digits have been dialed and the CS 2000 attempts to establish a speech path prior to ringing/ringback, VCAC can deny admission to the call. This is the main VCAC scenario.
- Call Hold. The bearer path is dropped for a call placed on hold, whether as a call hold service or as a step in another service such as 3WC or consultation transfer. If other calls have consumed the available resources then an attempt to retrieve the held call will fail.
- Call Transfer. The bearer path is changed after it has been set up. Services such as call transfer, CFNA, 3WC can cause this condition. IN services use call transfer by connecting a call to announcements before routing to other destinations. This procedure fails if there is a LBL in the new path without resources for the new call leg.
- Calls that ring before negotiating the speech path. Examples are non-pilot members for simring and pre-answer call waiting attempts. In these cases, the application only calculates the bandwidth on answer, so the call will be denied if there is not enough bandwidth.

On call denial, VCAC will clear down the call that would overload the Limited Bandwidth Link (LBL).

Service limitations and restrictions

There is a best effort approach to services with the following limitations and restrictions for services below.

Lawful Intercept

There are a number of restrictions for configuring Lawful Intercept (LI):

- The parties monitoring for the Law Enforcement Agency (LEA) must not be configured behind LBLs. This restriction is similar to the restriction for NAT traversal, that the parties monitoring for the LEA must not be configured behind NAT devices. If the parties monitoring for LEA ignore this restriction, they can ring but won’t get a voice path.
- When a call leg is blocked by VCAC, C-tone can be interrupted for dedicated LI and there can be Ring splash on the LEA monitoring parties for switched LI.
- There is a transparency issue when the call parties are behind a common and full LBL. In this case, if the two parties are not subject to LI, they can call each other, but if one of the parties is subject to LI, then the call will be blocked, as the call is extended to the LI replicator device. Another example is when both parties are on the same Gateway and cannot be blocked, therefore making LI monitoring very obvious.This problem can be solved by the Public Network Interception (PNI) feature which prevents calls from being monitored unless the LEA chooses to take the risk of the monitoring action being discovered.

For more information about Lawful Intercept, refer to NTP *Lawful Intercept Technology and Product Fundamentals (NA)*, NN10190-113.

Emergency and other priority calls

There is no guarantee that emergency or priority calls will get through. These calls are subject to the same VCAC process as any other voice traffic. The Network VCAC application does not give extra precedence to these calls over other voice traffic.

Service failure and behavior

If there is insufficient bandwidth then one or more call legs will fail and the service attempt will fail. The following examples are common service failures and their behavior when Network VCAC denies calls.

This is not an exhaustive list of services or ways in which the service can fail.

- Three Way Call. Three Way Call can be blocked at a number of points - when retrieving someone from hold, on contacting the second party, and when connecting the three members to the conference bridge. If the second party cannot be reached, the controller hears the NBLN treatment and can flash back to the first party. If one party cannot reach the conference bridge due to bandwidth restrictions, then the controller receives three seconds of NBLN treatment to alert them to the problem before being connected to the other party.
- Call Waiting. Transfer to a waiting call only applies Network VCAC when the switch to the waiting call occurs. This transfer can fail if there is insufficient bandwidth for the two parties to reach each other. In this case, the waiting party hears ringing, then the NBLN treatment, and the called party hears three seconds of BUSY before being reconnected to their original call.
- Call Hold. A party put on hold releases its bandwidth until a reconnect attempt is made. This reconnection can fail if other calls have consumed the bandwidth in the meantime. In this case, the party on hold drops to dialtone and the retrieving party hears the NBLN treatment.
- Call Forward No Answer. Call Forward No Answer can fail when the call is made to the first party or when the call is forwarded onto the second party. If the failure occurs on the connection to the second party then the originator will have heard several seconds of ringing before receiving the NBLN treatment.
- Music On Hold. Music on hold is played when a party is put on hold. If there is insufficient bandwidth for the on hold part to reach the audio server then the held party will drop out of the service and hear dial tone.
- SIMRING. SIMRING only reserves bandwidth to the pilot DN. If there is insufficient bandwidth to reach the pilot DN then ring splash is heard on the non-pilot DN. If there is enough bandwidth to reach the pilot DN, but the call is answered on a non-pilot DN without enough bandwidth, then the originator hears the NBLN treatment followed by DISC treatment, and the answering party drops back to dial tone.
- CICM EBS secondary DN services. The CICM secondary DN service can maintain two bearer channels. Some service failures will not occur because the speech path is maintained and the

bandwidth is not released. However, holding multiple bearer channels will exhaust the bandwidth more quickly on links.

- Meet-Me Conference. The Meet-Me service applies a short ring tone to existing conferees when a party attempts to join, even if Network VCAC actually blocks that party. The denied party hears NBLN treatment but existing conferees hear no indication that the joining attempt failed. If the Network VCAC-denied party was first or second to dial into the Meet-Me bridge, the remaining party is disconnected as if the conference had ended normally. Calls to a Meet-Me bridge denied by VCAC are recorded as answered but with no elapsed time for billing purposes.

Add a Policy Controller application

Purpose of this procedure

From the Policy Controller Web GUI, use this procedure to add a Policy Controller application to the system.

Limitations and restrictions

There are no limitations or restrictions for this procedure.

Prerequisites

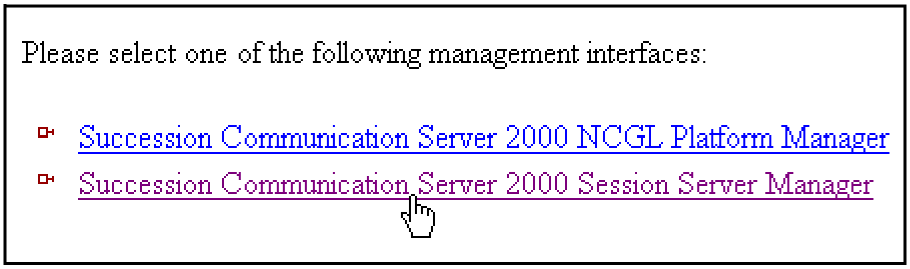
There are no prerequisites for this procedure.

Action

Add a Policy Controller Application

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

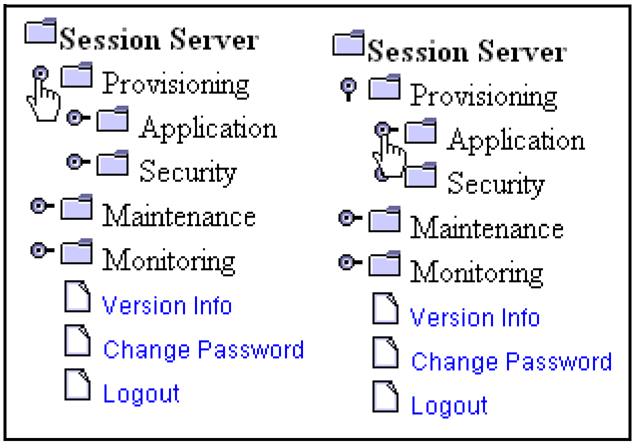


Please select one of the following management interfaces:

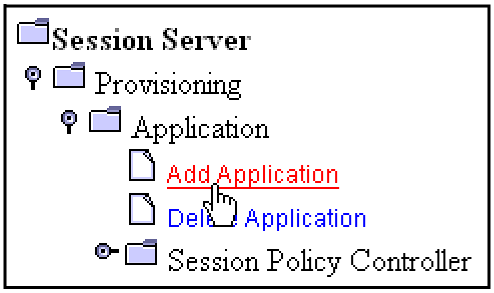
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

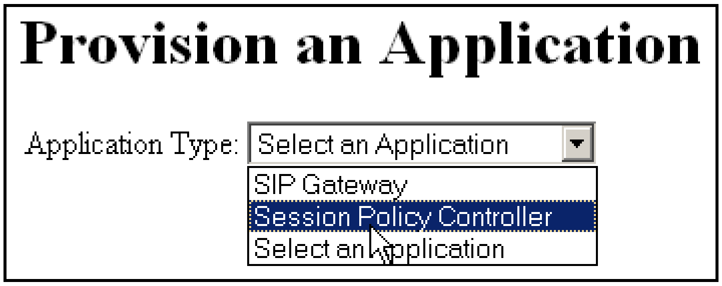
2 Under the **Session Server** folder, select the **Provisioning** folder, and then select the **Application** folder.



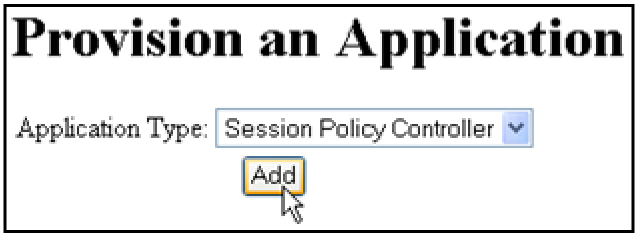
3 Click **Add Application**



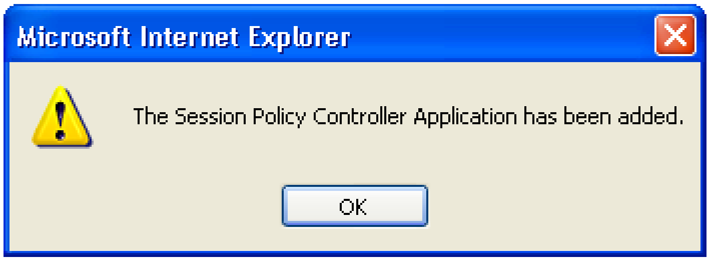
4 From the **Provision an Application** window, go to the **Application Type** drop-down menu and select **Session Policy Controller**.



5 To add a Policy Controller application to the system, click the **Add** button.

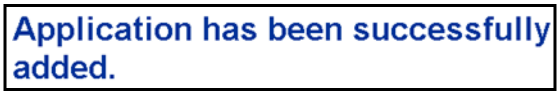


6 A message box displays telling you that the Policy Controller Application has been added to the system. Click the **OK** button to confirm.



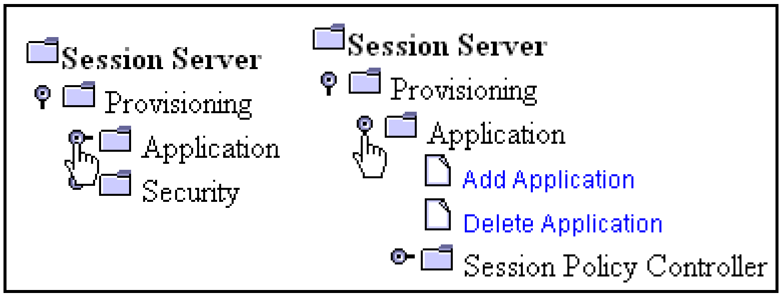
The Session Policy Controller Application has been added.

The following confirmation message displays telling you the Policy Controller Application has been successfully added to the system.



Application has been successfully added.

7 To confirm the addition of the Policy Controller Application, close and then open the **Application** folder: select the **Application** folder to close it, then select it again to open it.



The Policy Controller Application has been added to the system.

8 To begin provisioning the Policy Controller that you have just added, go to **Session Policy Controller** folder.

9 You have completed this procedure.

Delete a Policy Controller Application

Purpose of this procedure

Use this procedure to delete a Policy Controller Application from the system.

Limitations and restrictions

There are no limitations or restrictions for this procedure

Prerequisites

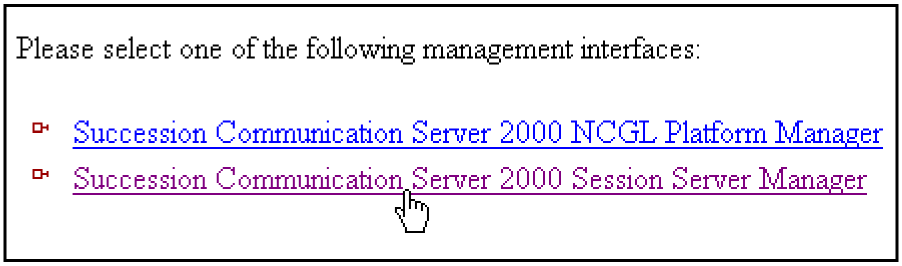
There are no prerequisites for this procedure.

Action

Delete a Policy Controller Application

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

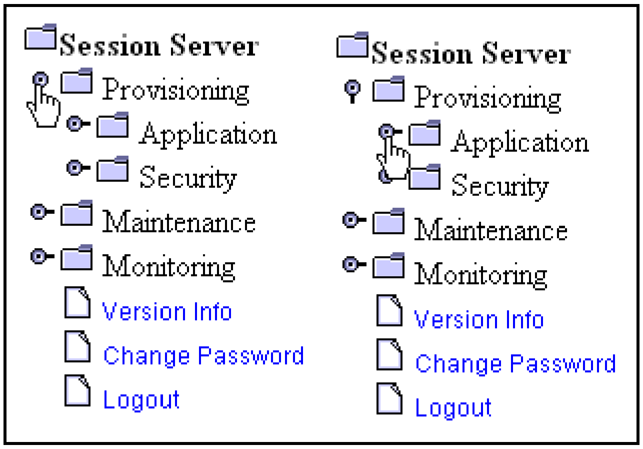


Please select one of the following management interfaces:

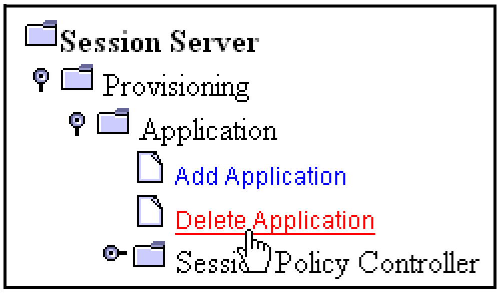
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

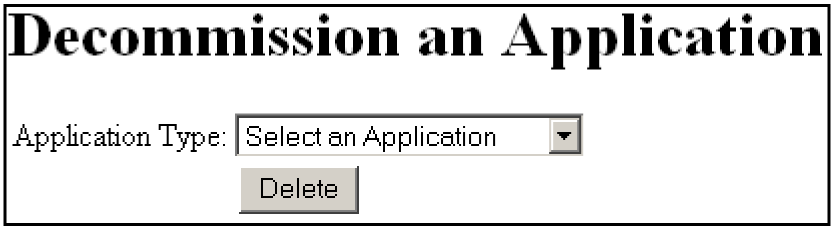
2 At the **Session Server** folder, select the **Provisioning** and then select **Application** folder.



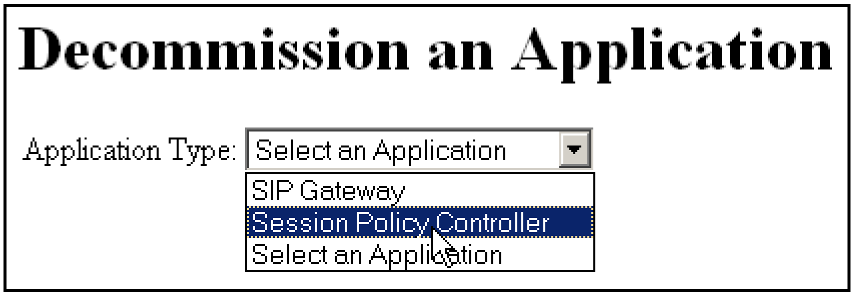
3 Select **Delete Application**



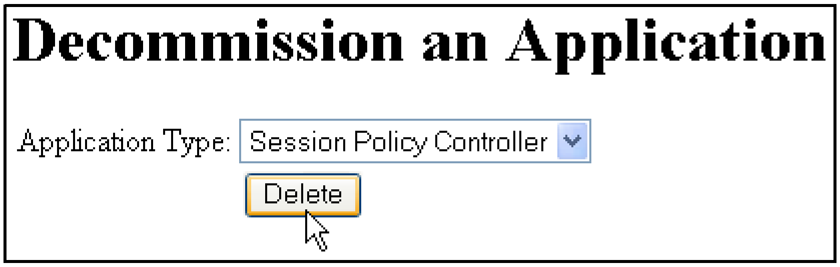
The **Decommission an Application** window opens.



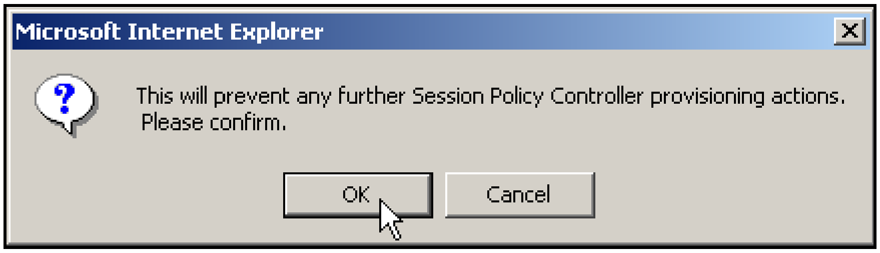
4 From the **Decommission an Application** window, locate the **Application Type** drop-down menu and select **Session Policy Controller**.



5 To delete a Policy Controller application, click the **Delete** button.



6 The following message box displays.



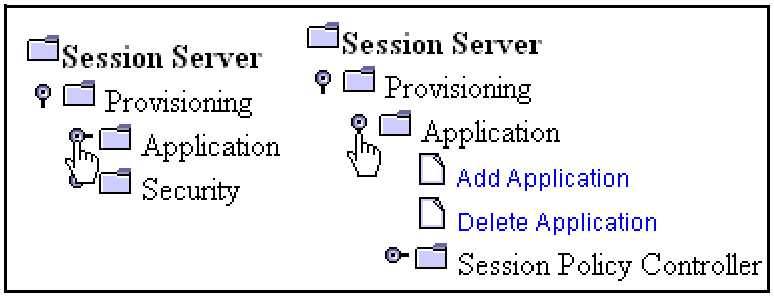
Microsoft Internet Explorer

This will prevent any further Session Policy Controller provisioning actions.
Please confirm.

Click the **OK** button to confirm the deletion of the Policy Controller Application. Or, click the **Cancel** button to stop the deletion and close the message box.

7 To confirm the deletion of Session Policy Controller Application, close and open the **Application** folder:

Select the **Application** folder to close it, and then select it again to open it.



The Policy Controller Application has been deleted from the system.

8 You have completed this procedure.

List/Modify Topology Manager (TM) parameters

Purpose of this procedure

Use this procedure to list and modify the Topology Manager (TM) parameters.

Limitations and restrictions

The fields in the **Topology Manager Parameter Change** window are read-only until you click the **Modify** button.

If the Primary Port and the Second Port are both occupied by other processes, then the Topology Manager process will not start.

Changes to Topology parameters will not take effect until you restart the Topology Manager.

Prerequisites

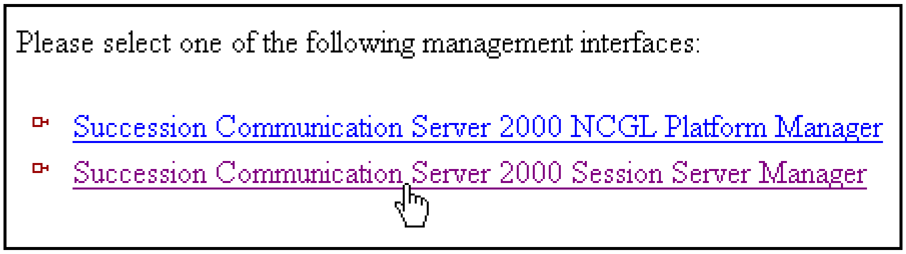
There are no prerequisites for this procedure.

Action

List/Modify TM Parameters

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

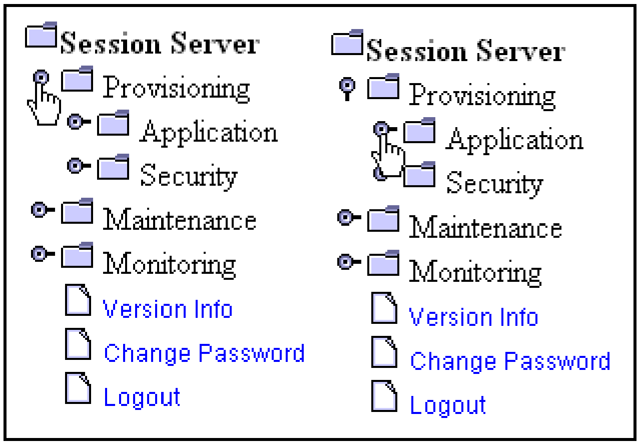


Please select one of the following management interfaces:

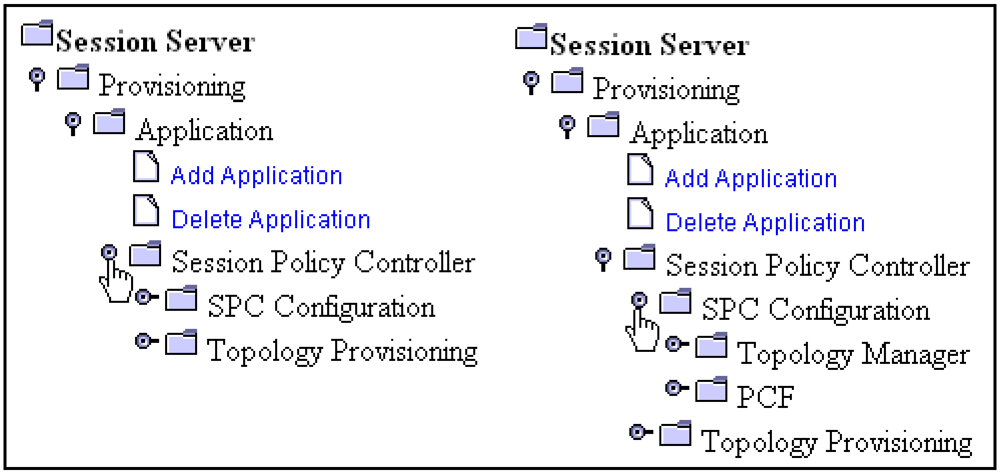
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

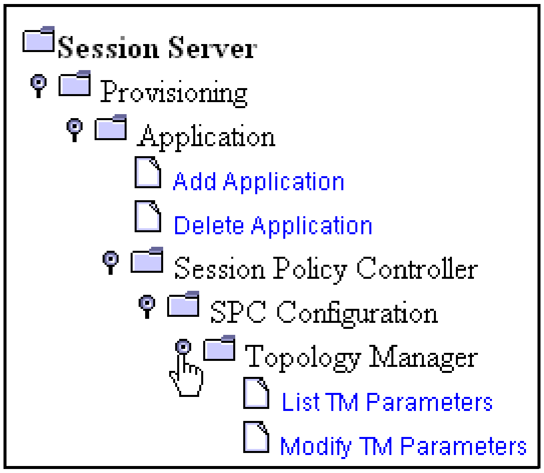
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



3 Select the **Session Policy Controller** folder, and then select the **SPC Configuration** folder.



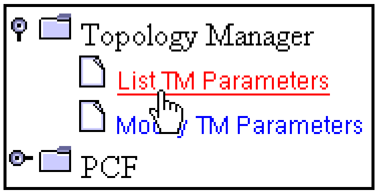
4 Select the **Topology Manager** folder.



5

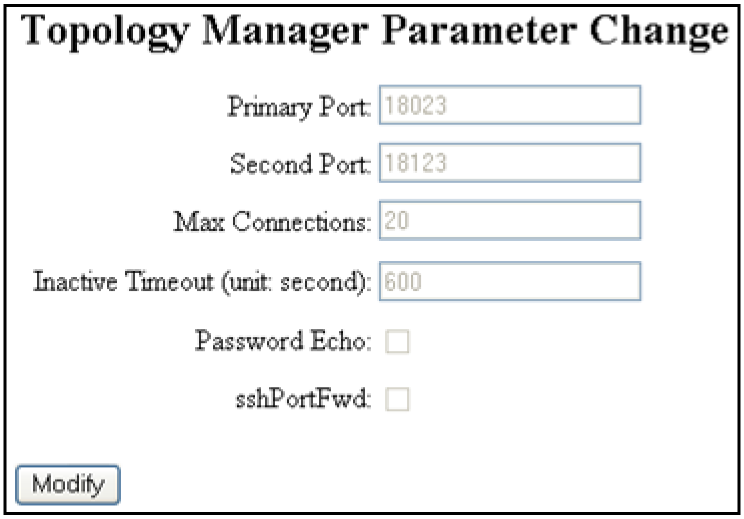
If	Do
you want **to list and view** the TM parameters	step 6
you want **to modify** the TM parameters	step 7

6 Click **List TM parameters**.



The **Topology Manager (TM) Parameter Change** window opens. To modify the TM parameters, go to step 7.

> ***Note:*** The entry fields are read-only until you click the **Modify** button.



Topology Manager Parameter Change

Primary Port: 18023

Second Port: 18123

Max Connections: 20

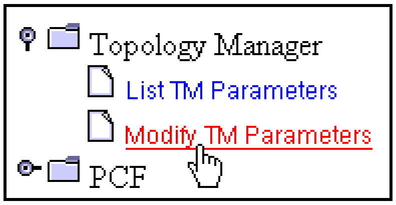
Inactive Timeout (unit: second): 600

Password Echo: □

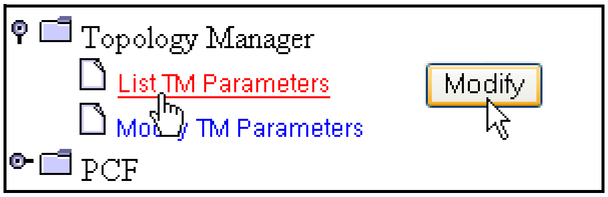
sshPortFwd: □

7 To modify the TM Parameters, use one of the following methods:

- Select the **Topology Manager** folder and then select **Modify TM Parameters.**



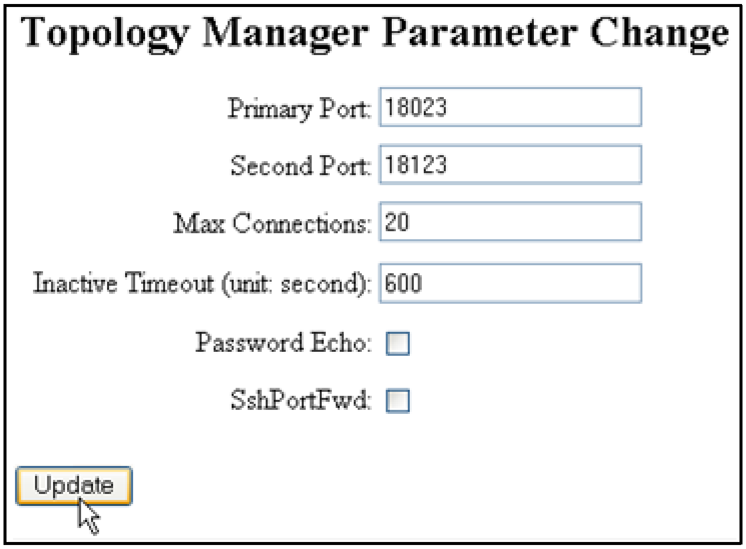
- Or, select the **Topology Manager** folder, and then select **List TM Parameters**. Then from the **Topology Manager Parameter Change** window (right frame), click the **Modify** button.



The **Topology Manager Parameter Change** window, containing an **Update** button, opens.

8 From the **Topology Manager Parameter Change** update window, modify the parameters in the desired fields, and then click the **Update** button to save the new values.

Use table TM Parameter Change window field descriptions on page 41 to help you fill out the fields for the **TM Parameter Change** update window.



Topology Manager Parameter Change

Primary Port: 18023

Second Port: 18123

Max Connections: 20

Inactive Timeout (unit: second): 600

Password Echo: □

SshPortFwd: □

TM Parameter Change window field descriptions (Sheet 1 of 2)

Field	Entry	Description
Primary Port	Default=18023	The primary port that the TM listens on for the OSS client to connect to.
Second Port	Default=18123	The secondary port that the TM listens on for the OSS client to connect to when the primary port is occupied by other processes.

Max Connections	Default=20
	Range=1to 20
		The maximum number of concurrent connections.

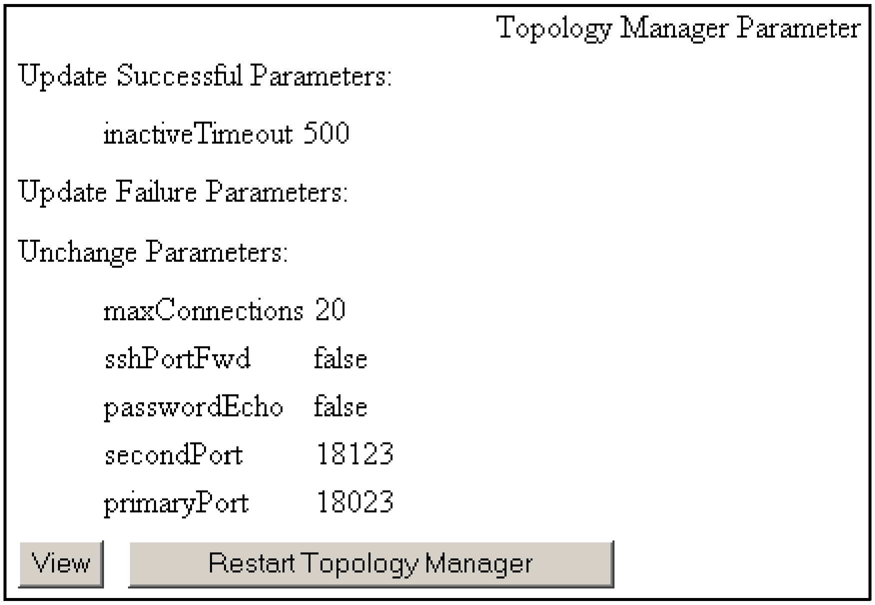
Inactive Timeout	Default=600 seconds
	Range=1to 3600 seconds
		The maximum idle time of the session. When the set time in this field expires, the TM will disconnect the session.

TM Parameter Change window field descriptions (Sheet 2 of 2)

Field	Entry	Description
Password Echo	Default= Unselected	When connecting to the Topology Manager from an OSS interface, this field determines whether the password is echoed on the screen or not. **Selected**=true The password is echoed on screen. **Unselected**=false The password is not echoed on screen and is invisible.
SshPortFwd	Default= Unselected	**Selected**=true The OSS can only access TM by setting a SSH port forwarding on the IEMS server. **Unselected**=false The OSS can directly access TM using a Telnet-compatible client.

The saved results display in the **Topology Manager Parameter** results window. This window shows the parameters that were successfully updated, failed to update, or remain unchanged.

> ***Note:*** You need to restart the Topology Manager for the parameter changes to take effect. Go to step 9 for this information.



Topology Manager Parameter

Update Successful Parameters:

inactiveTimeout	500

Update Failure Parameters:

Unchange Parameters:

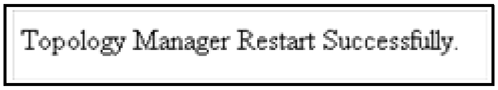
maxConnections	20
sshPortFwd	false
passwordEcho	false
secondPort	18123
primaryPort	18023

9 From the **Topology Manager Parameter** results window, perform the following tasks:

- Click the **View** button which returns you to the **Topology Manager Parameter Change** window, where you can see the updated TM parameters.

  OR

- Click the **Restart Topology Manager** button which restarts the Topology Manager and commits the changes you made to the system. If successful, the following message displays.



Topology Manager Restart Successfully.

If unsuccessful, an error message displays giving instructions. Follow the instructions to solve the error. Then go back to the **Topology Manager Parameter Change** window and click the **Restart Topology Manager button** again.

10 You have completed this procedure.

List/Modify Policy Control Framework (PCF) parameters

Purpose of this procedure

The Policy Control Framework (PCF) processes requests for resources and applies the necessary policy enforcements to the requests.

Use this procedure to list and modify the current Policy Control Framework parameters.

Limitations and restrictions

The fields in the **PCF Parameter Change** window are read-only until you click the **Modify** button.

Prerequisites

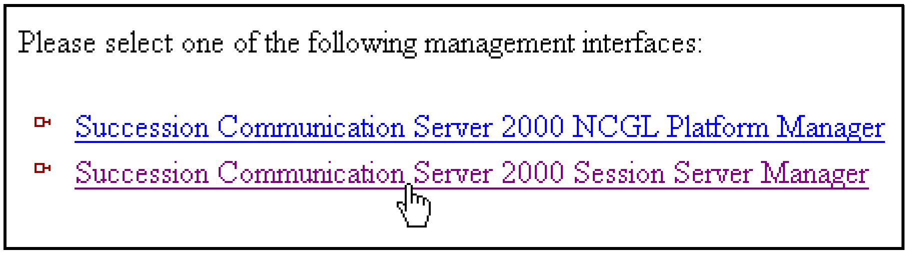
There are no prerequisites for this procedure.

Action

List/Modify Policy Control Framework (PCF) Parameters

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

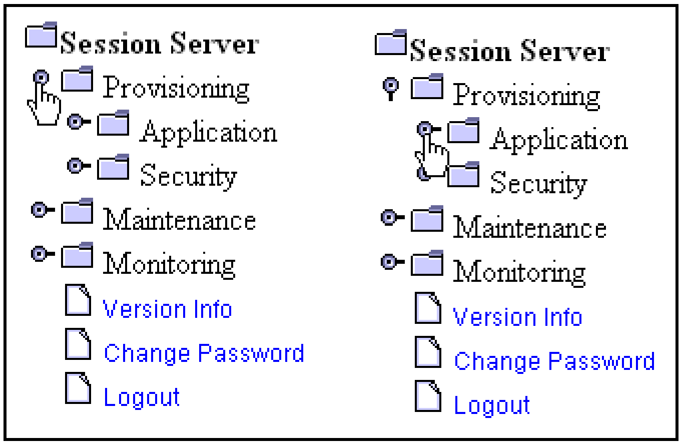


Please select one of the following management interfaces:

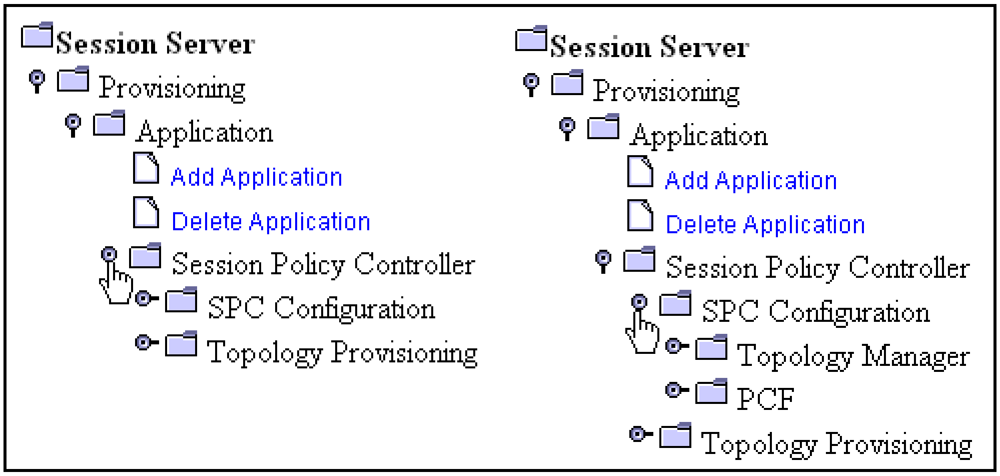
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

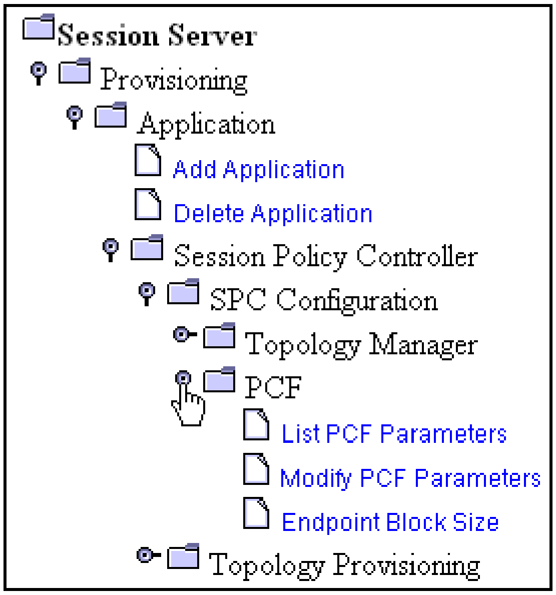
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



3 Select the **Session Policy Controller** folder, and then select the **SPC Configuration** folder.



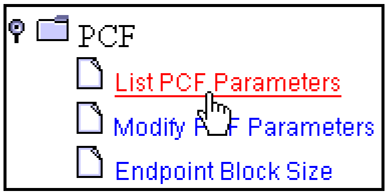
4 Select the **PCF** folder.



5

If	Do
you want **to list and view** the PCF parameter field values	next step
you want **to modify** the PCF parameter field values	step 7

6 Select **List PCF parameters**.

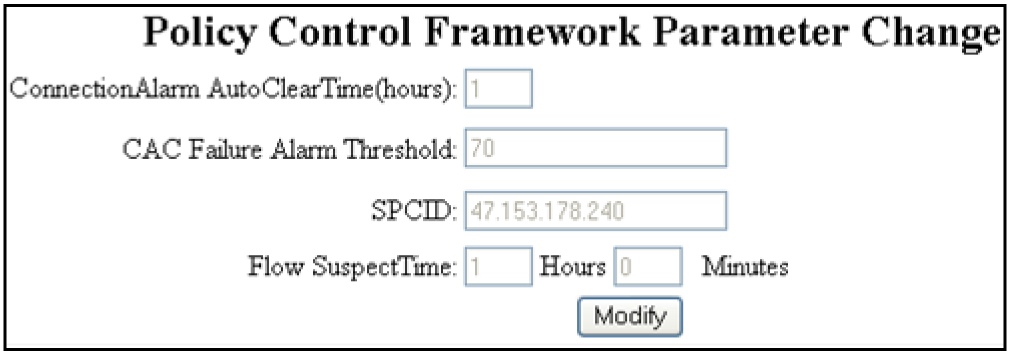


The **Policy Control Framework (PCF) Parameter Change** window opens.

> ***Note:*** The fields are read-only until you click the **Modify** button.

Refer to table PCF Parameter Change window field descriptions on page 48 for descriptions of the fields for the **PCF Parameter Change** window.

To modify the PCF field values, go to step 7.



Policy Control Framework Parameter Change

ConnectionAlarm AutoClearTime(hours): 1

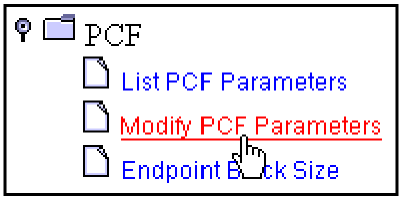
CAC Failure Alarm Threshold: 70

SPCID: 47.153.178.240

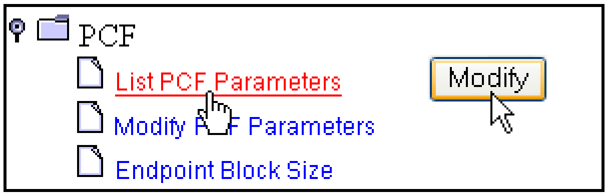
Flow SuspectTime: 1 Hours 0 Minutes

7 To modify the PCF Parameters, use one of the following methods:

- Select the **PCF** folder and then select **Modify PCF Parameters**.



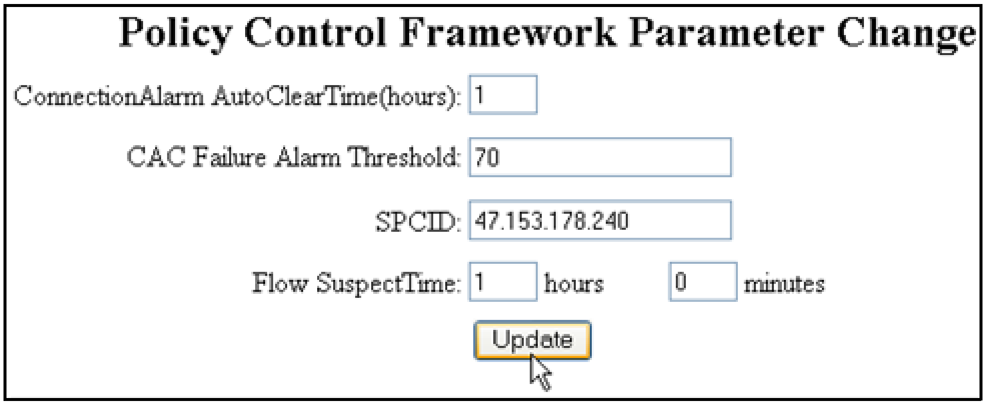
- Or, select the **PCF** folder and then select **List PCF Parameters**. Then from the **Policy Control Framework Parameter Change** window, click the **Modify** button.



The **Policy Control Framework Parameter Change** window, containing an **Update** button, opens.

8 From the **Policy Control Framework Parameter Change** update window, modify the parameters in the desired PCF fields, and then click the **Update** button to save the modified values.

Use table PCF Parameter Change window field descriptions on page 48 to help you fill out the fields in the **PCF Parameter Change** window.



Policy Control Framework Parameter Change

ConnectionAlarm AutoClearTime(hours): 1

CAC Failure Alarm Threshold: 70

SPCID: 47.153.178.240

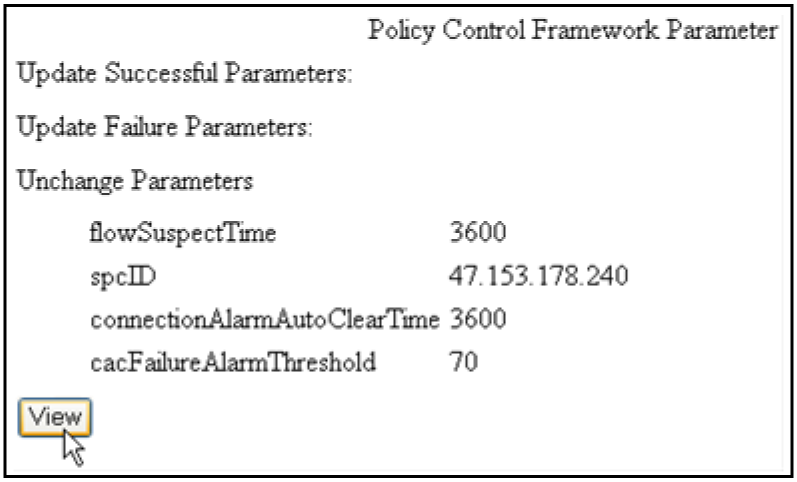
Flow SuspectTime: 1 hours 0 minutes

PCF Parameter Change window field descriptions

Field	Entry	Description
ConnectionAlarm AutoClearTime (hours)	Default= 1 hour Range= 1-24 hours	The time it takes to automatically clear a connection alarm.
CAC Failure Alarm Threshold	Default=70% Range= 1-100%	The Policy Controller will show an alarm on the console if the percentage of failed calls is equal to this value.
SPCID	logical IP address of the Policy Controller	Uses an IP address to identify the Policy Controller uniquely.
Flow SuspectTime	Default= 1 hour Range= 23 hours 59 minutes	Monitors the relevant resources for calls made via the Policy Controller which have lasted longer than the Flow Suspect time. The Policy Controller will audit calls and if the Gateway Controller returns an error for the call, the call flow will be deleted. The Policy Controller will then recover the associated resources for any deleted call flows.

After you click the **Update** button, the parameter change is immediate. The saved results appear in the **Policy Control**

Framework Parameter results window. This window indicates the parameters that were successfully updated, failed to update, or remain unchanged.



Policy Control Framework Parameter

Update Successful Parameters:

Update Failure Parameters:

Unchange Parameters

flowSuspectTime	3600
spcID	47.153.178.240
connectionAlarmAutoClearTime	3600
cacFailureAlarmThreshold	70

9 From the **Policy Control Framework Parameter results** window, click the **View** button to return to the **Policy Control Framework Parameter Change** window, where the updated PCF parameter values are visible.

10 You have completed this procedure.

Purpose of this procedure

Use this procedure to perform the following tasks:

- List and modify Endpoint Block Size.
- After the Policy Controller is initially installed, add the software license key to enable the PCF to start.

> **ATTENTION**
> Before modifying the Endpoint Block Size, you need a valid software license key. If you do not have a valid software license key, contact Nortel Networks customer support to obtain one.

Limitations and restrictions

This procedure has the following limitations and restrictions:

- Endpoints are in blocks of 5000.
- The Endpoint Warning Size depends on the Endpoint Block Size.

  Note: The **Endpoint Block Size** field is read-only and cannot be modified.

- For (I)SN08, only the location of the endpoint is important.
- You must have a software license key to change the Endpoint Block Size.

Prerequisites

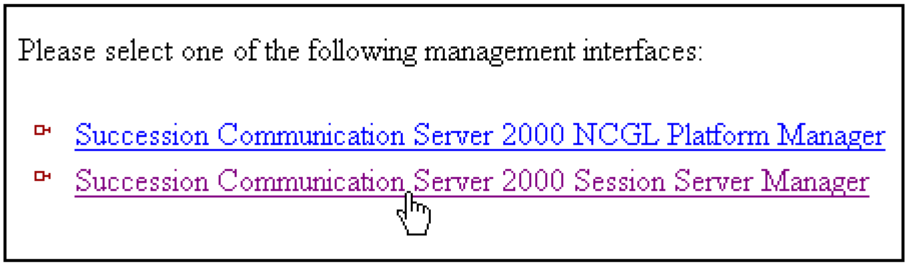
There are no prerequisites for this procedure.

Action

List/Modify an Endpoint Block Size

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

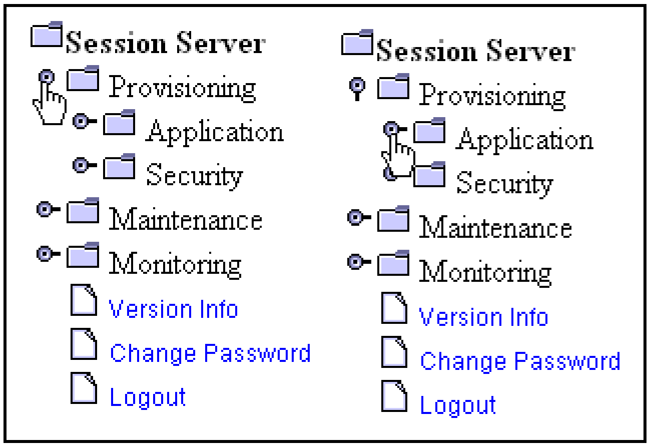


Please select one of the following management interfaces:

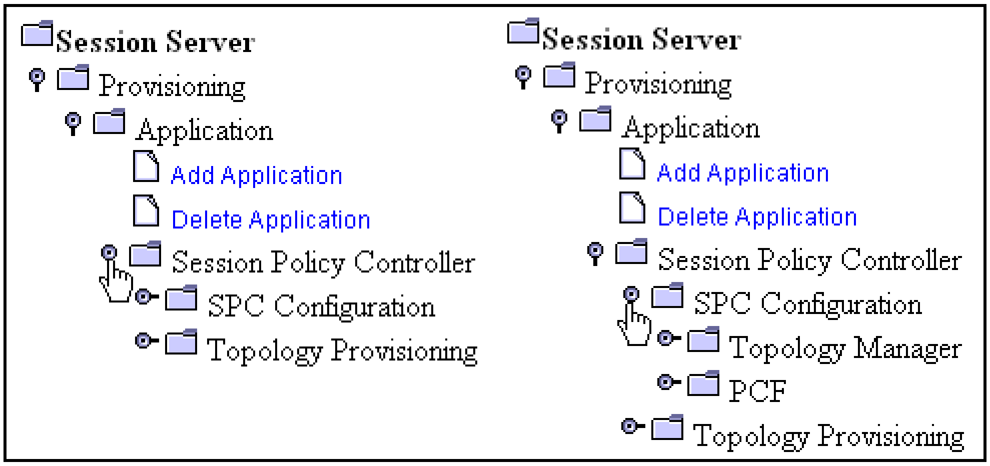
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

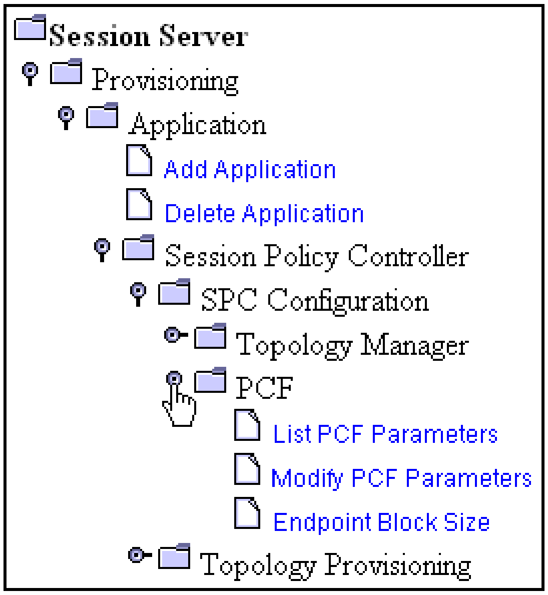
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



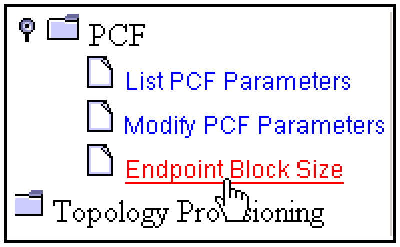
3 Select the **Session Policy Controller** folder, and then select the **SPC Configuration** folder.



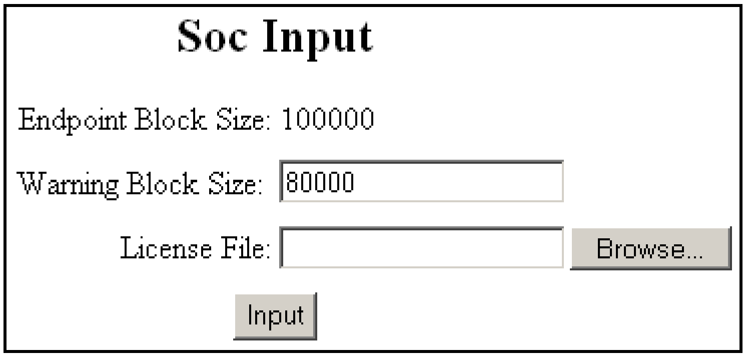
4 Select the **PCF** folder.



5 Select **Endpoint Block Size**.



The **Software Optionality Control** (**SOC) Input** window opens.



Soc Input

Endpoint Block Size: 100000

Warning Block Size: 80000

License File:

Use the following table to help you fill out the fields in the **SOC Input** window.

To modify the **Warning Block Size**, go to step 6.

SOC Input window field descriptions

Field	Entry	Description
Endpoint Block Size	Default= 5000	The current Endpoint Block Size.

Warning Block Size	Default= 4000
	Range= 50% to 95% of Endpoint Block Size
		If the Endpoint Block Size equals or exceeds the value in this field, the Policy Controller raises an alarm.

License File		The software license file allows you to increase the Endpoint Block Size. Change the Endpoint Block Size by entering the software license key into this field. ***Note:*** Contact Nortel customer support to obtain a software license key.
Browse		Click the **Browse** button and locate the software license key.
Input		Click the **Input** button to modify the endpoint block size.

6 To modify the Warning Block Size, click the **Warning Block Size** field and enter a new warning block size.

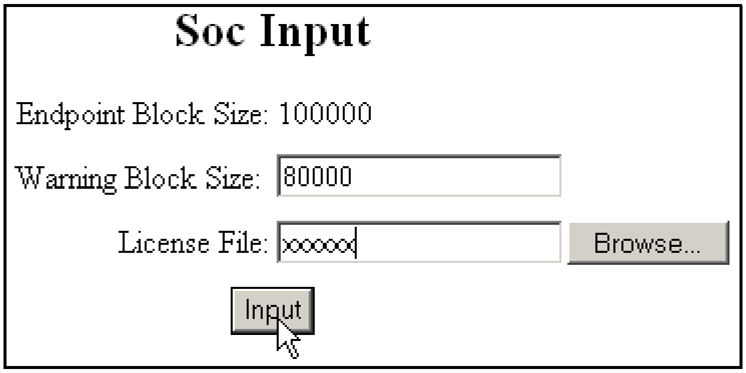
7 Enter the software license key in the **License File** field using one of the following methods:

- Click the **License File** field and enter the path to the software license key.

  OR

- Click the **Browse** button, locate the software license key, and select it. The path to the software license key displays in the **License File** field.

8 Click the **Input** button to change the Endpoint Block Size and/or the Warning Block Size.



Soc Input

Endpoint Block Size: 100000

Warning Block Size: 80000

License File: xxxxxx

The **Endpoint Block Size** changes and takes effect immediately.

9 You have completed this procedure.

Purpose of this procedure

Use this procedure to perform the following tasks for each network zone:

- View the details of a network zone.
- Modify and update the parameters for a network zone.

Limitations and restrictions

The fields in the **Detail Network Zone** window are read-only.

A valid **Network Zone ID** value is numeric between 2 and 16777215.

After you provision a network zone ID, this field cannot be modified.

A valid network zone name must follow the DNS convention and the following rules:

- The name cannot start or end with "." or "-"
- The name does not support consecutive ".."
- The name does not support "_"
- The name is case insensitive.
- The name supports a maximum of 32 characters.

Premium is the only Network Service Class available for SN08. All voice calls are tagged as Premium.

In Policy Controller release one, Premium Network Service Class is the only Network Service Class available for the SN08 release, therefore the following conditions apply:

- Premium is set to 100% and all four service classes are set to 0, because voice calls are tagged as Premium.
- In the XML commands, <NNSC> does not appear in <UpBWInfo> or <DownBWInfo>.

A valid **EncapsOverHead** parameter is numerical in the range of 0 to 1000000.

A valid **UnitSize** parameter is numerical in the range of 1 to 1000000.

A valid **UnitOverHead** parameter is numerical in the range of 0 to 1000000.

The **UnitSize** value must be bigger than the **UnitOverHead** value, or an error will display when you click the **Save** button.

If the **isFixedPDU** field is selected, you must fill out the **UnitSize** field and the **UnitOverHead** field.

Prerequisites

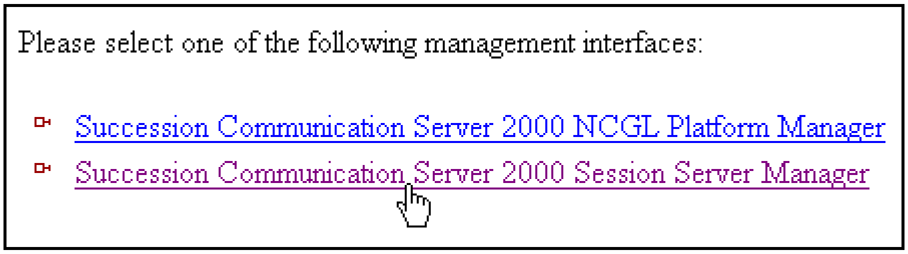
There are no prerequisites for this procedure.

Action

Display/Modify network zone

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

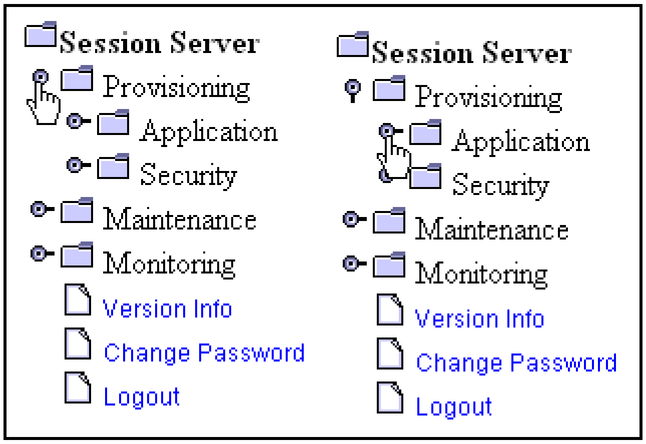


Please select one of the following management interfaces:

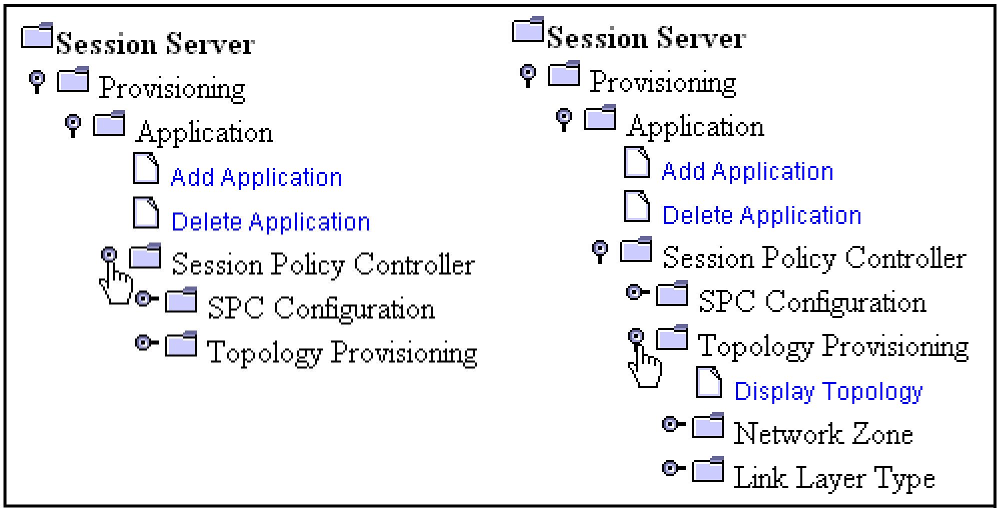
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

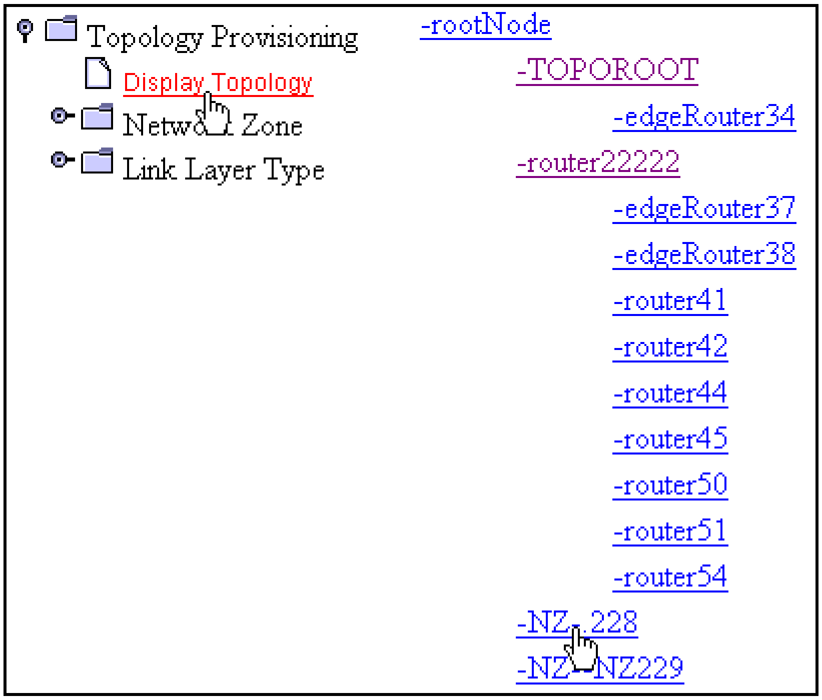
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



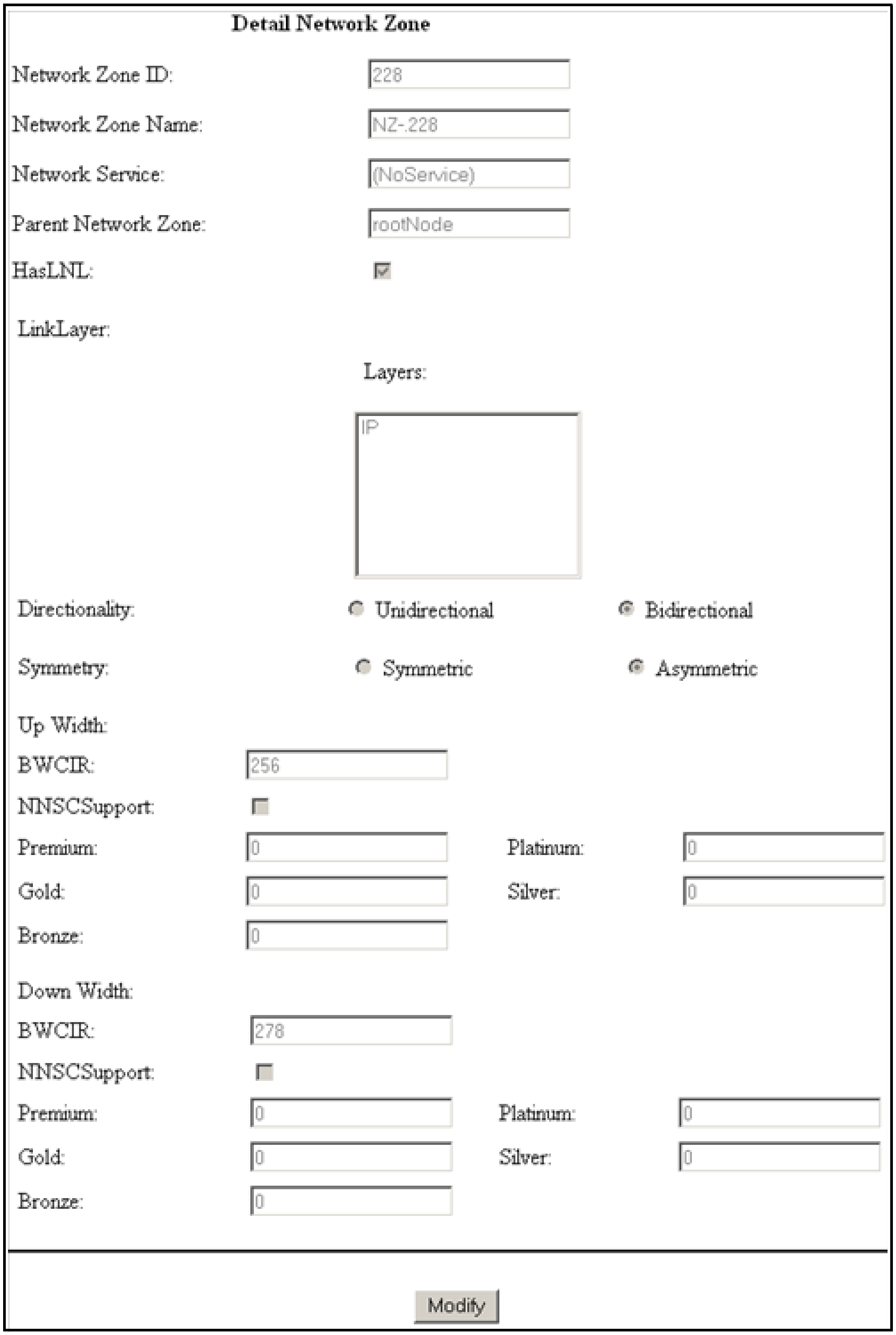
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



4 Select **Display Topology**. The **Topology** window opens and displays the network zone topology in tree format. Select a network zone to view its details.



The **Detail Network Zone** window opens with the details of the chosen network zone. The fields are read-only until you click the **Modify** button. The fields are described in the table Detail Network Zone window field descriptions on page 60. To modify the network zone field values, go to step 5.



Detail Network Zone

Network Zone ID:	228		
Network Zone Name:	NZ-228		
Network Service:	(NoService)		
Parent Network Zone:	rootNode		
HasLNL:	☑		
LinkLayer:			
	Layers:		
	IP		
Directionality:	○ Unidirectional	● Bidirectional	
Symmetry:	○ Symmetric	● Asymmetric	
Up Width:			
BWCIR:	256		
NNSCSupport:	□		
Premium:	0	Platinum:	0
Gold:	0	Silver:	0
Bronze:	0		
Down Width:			
BWCIR:	278		
NNSCSupport:	□		
Premium:	0	Platinum:	0
Gold:	0	Silver:	0
Bronze:	0		

Detail Network Zone window field descriptions (Sheet 1 of 3)

Field	Entry	Description
Network Zone ID	Range= numbers between 2 and 16777215	Identifies the network zone.
Network Zone Name	Range= 1 to 32 characters	Identifies the name of the network zone.

Network Service	Default= NoService
	Range= NAT or NoService
		Identifies the type of network service. There are two types of network service:
		• Network Address Translation (NAT)
		• Limited Bandwidth Links
		(LBL)
		NoService means LBL

Parent Network Zone		Identifies the name of the parent zone that this network zone belongs to.

HasLNL	Default= Selected
	Range= Selected or Unselected
		The network zone has a Logical Network Link (LNL)
		Selected=True The network zone has a LNL
		Unselected=False The network zone does not have a LNL
		Note: If the **Network Service** field is set to "NoService" then this option is mandatory and the check box will not be present. If the **Network Service** field is set to "NAT" then this field can be modified.

Link Layer		Lists all the Link Layers that the system supports in the **Layers** box.

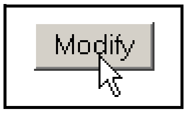
Detail Network Zone window field descriptions (Sheet 2 of 3)

Field	Entry	Description
Directionality		This is a required field. Defines whether the logical link is Bidirectional or Unidirectional. **Bidirectional**= Two sets of Bandwidth objects **Unidirectional**= One set of Bandwidth objects
Direction		Defines whether the logical link is Up width or down width. **Up** Width= defines an up link **Down** Width= defines a down link These two fields only display if you select the **Unidirectional** field.
Symmetry		Defines whether the logical link is symmetric or asymmetric. **Symmetrical**= One set of identical bandwidth objects are created. **Asymmetrical**=Two sets of bandwidth objects must be defined (Not necessarily identical). These two fields display only if the **Bidirectional** field is selected.
BWCIR	Range= 0 to 2^63-1	**BWICR**=Bandwidth Committed Rate is the bandwidth of the network zone link in bits per second (bps). The Policy Controller uses BWICR to count the required bandwidth of the endpoints to determine when the call can be set up.

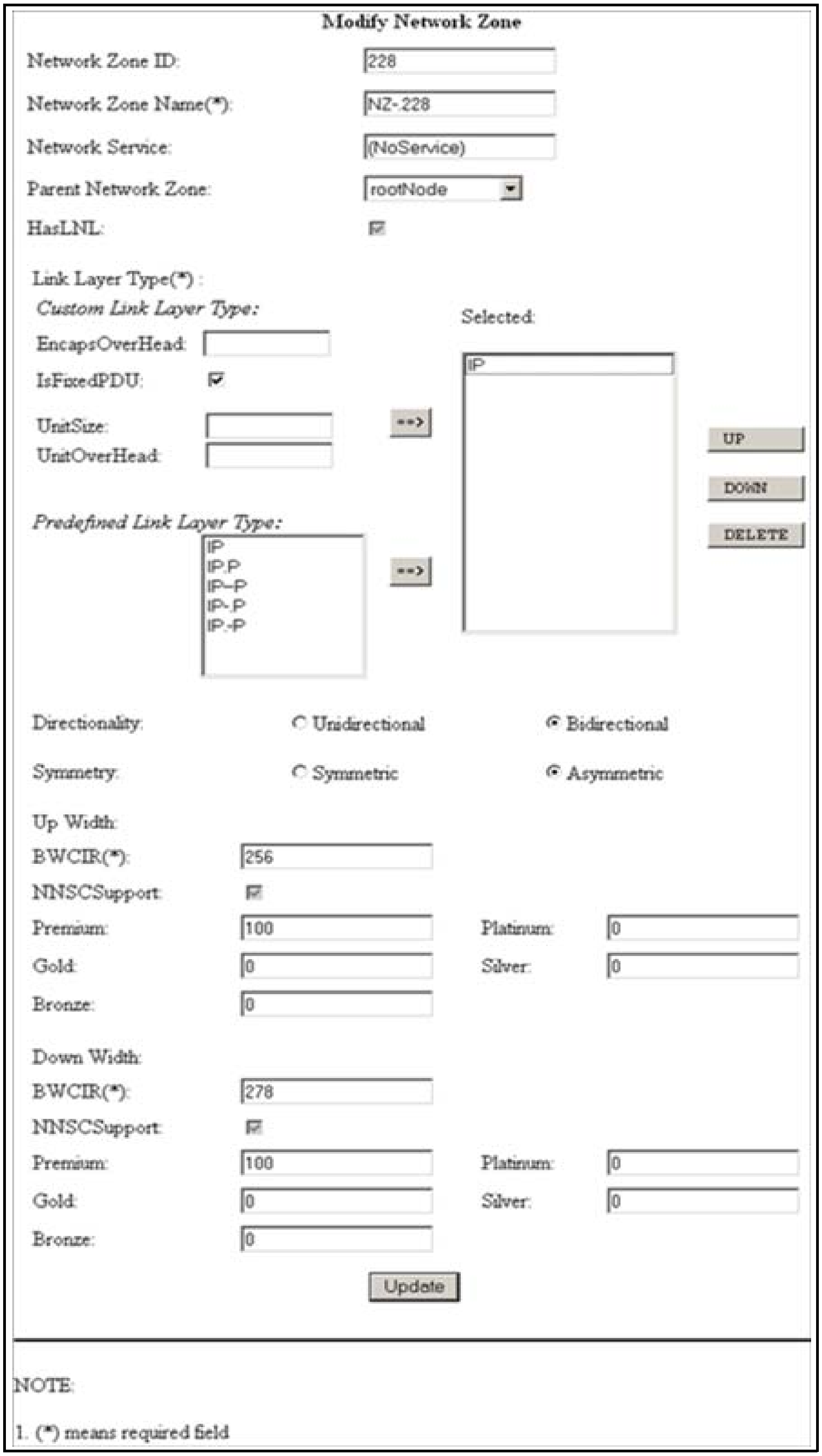
Detail Network Zone window field descriptions (Sheet 3 of 3)

Field	Entry	Description
NNSCSupport		Nortel Networks Service Classifier indicates the subscriber service class. In SN08, only voice calls are supported from the CS2000.
Premium		Indicates the level of Nortel Networks Service Class. ***Note:*** **Premium** is the only Network Service Class available for SN08. All voice calls are tagged as Premium.
Modify		Takes you to the **Modify Network Zone** window where you can change and save the parameters of a network zone.

5 To modify the field values for a network zone, click the **Modify** button at the bottom of the **Detail Network Zone** window.



The **Modify Network Zone** window opens. Use table Modify Network Zone window field descriptions on page 64 to help you modify a network zone.



Modify Network Zone

Network Zone ID:	228
Network Zone Name(*):	NZ-228
Network Service:	(NoService)
Parent Network Zone:	rootNode ▾
HasLNL:	☑

Link Layer Type(*) :

Custom Link Layer Type:

EncapsOverHead:	
IsFixedPDU:	☑
UnitSize:	
UnitOverHead:	

Predefined Link Layer Type:

IP
IP.P
IP~P
IP-.P
IP.-P

Selected:

IP

Directionality:	○ Unidirectional	● Bidirectional
Symmetry:	○ Symmetric	● Asymmetric

Up Width:

BWCIR(*):	256		
NNSCSupport:	☑		
Premium:	100	Platinum:	0
Gold:	0	Silver:	0
Bronze:	0		

Down Width:

BWCIR(*):	278		
NNSCSupport:	☑		
Premium:	100	Platinum:	0
Gold:	0	Silver:	0
Bronze:	0		

NOTE:

1. (*) means required field

Modify Network Zone window field descriptions (Sheet 1 of 4)

Field	Entry	Description
Network Zone ID	Range= numbers between 2 and 16777215	Identifies the network zone.
Network Zone Name	Range= 1 to 32 characters	Identifies the name of the network zone.

Network Service	Default= NoService
	Range= NAT or NoService
		Identifies the type of network service. There are two types of network service:
		• Network Address Translation (NAT)
		• Limited Bandwidth Links
		(LBL)
		NoService means LBL

Parent Network Zone		This is a required field. Identifies the name of the parent system that this network zone belongs to.
HasLNL		The network zone has a Logical Network Link (LNL) **Selected**=True The network zone has a LNL **Unselected**=False The network zone does not have a LNL ***Note:*** If the **Network Service** field is set to "NoService" then this option is mandatory and the check box will not be present. If the **Network Service** field is set to "NAT" then this field can be modified.

Modify Network Zone window field descriptions (Sheet 2 of 4)

Field	Entry	Description
Link Layer Type		Lists the Link Layer Types that the system supports. **Custom Link Layer Type**= Allows you to create a custom Link Layer Type. Fill out the following fields to create a custom Link Layer Type: **EncapsOverHead** **IsFixedPDU** **UnitSize** **UnitOverHead** **Predefined Link Layer Type**=Select a Link Layer Type that has already been defined.
Selected		Lists the Link Layer Types that you have added from either the **Custom Link Layer Type** fields or the **Predefined Link Layer Type** box**.** These Link Layer Types will be included in the network zone.
UP DOWN DELETE		Moves the layers up or down in the **Selected** box for the network zone. Or, deletes them from the **Selected** box.
Directionality		This is a required field. Defines whether the logical link is Bidirectional or Unidirectional. **Bidirectional**= Two sets of Bandwidth objects. **Unidirectional**= One set of Bandwidth objects.

Modify Network Zone window field descriptions (Sheet 3 of 4)

Field	Entry	Description
Direction		Defines whether the logical link is Up width or down width. **Up** Width= defines an up link **Down** Width= defines a down link These two fields only display if you select the **Unidirectional** field.
Symmetry		Defines whether the logical link is symmetric or asymmetric. **Symmetrical**= One set of identical bandwidth objects are created. **Asymmetrical**=Two sets of bandwidth objects must be defined (not necessarily identical). These two fields display only if the **Bidirectional** field is selected.
BWCIR	Range= 0 to 2^63-1	**BWICR**=Bandwidth Committed Rate is the bandwidth of the network zone link in bits per second (bps). The Policy Controller uses BWICR to count the required bandwidth of the endpoints to determine when the call can be set up.
NNSCSupport		Nortel Networks Service Classifier indicates the subscriber service class. In SN08, only voice calls are supported from the CS2000.

Modify Network Zone window field descriptions (Sheet 4 of 4)

Field	Entry	Description
Premium		Indicates the level of Nortel Networks Service Class. ***Note:*** **Premium** is the only Network Service Class available for SN08. All voice calls are tagged as Premium.
Update		Updates the modified parameters for the network zone to the system.

6 You can modify the following field parameters on the **Modify Network Zone** window:

- **Network Zone Name**: Click this field and enter a network zone name.
- **Parent Network Zone**: Click open the drop-down box next to this field and select a parent network zone.
- **HasLNL**: Click to select or deselect this field.

  Note: If the **Network Service** field is set to "NoService" then this option is mandatory and the check box will not be present. If the **Network Service** field is set to "NAT" then this field can be modified.

- **Link Layer Type**:
  - — From the Custom Link Layer Type fields, modify the fields **EncapsOverHead, IsFixedPDU**, **UnitSize**, and **UnitOverHead** to create or modify a Custom Link Layer Type. Click the arrow button to the right of the **UnitSize** field to move the Link Layer Type to the **Selected** box. The Link Layer Type will be added to the network zone after you click the **Update** button.

    OR

  - — From the **Predefined Link Layer Type** box, click the arrow key to the right of the box to move the selected Link Layer Type to the **Selected** box. The Link Layer Type will be added to the network zone after you click the **Update** button.
- **Selected**: Click a Link Layer Type in the **Selected** box to select it. Click the **DELETE** button to the right of the **Selected**

box to remove the selected Link Layer Type from the **Selected** box.

You can also change the position of a Link Layer Type in the **Selected** box: Click a Link Layer Type in the **Selected** box to select it. Click the **UP** or **DOWN** button to the right of the **Selected** box to move the selected Link Layer Type either up or down in position.

- **Directionality**: Choose whether the logical link is unidirectional or bidirectional. Click either the **Unidirectional** or **Bidirectional** radio button.

  — **Unidirectional**: If you choose **Unidirectional**, the **Direction** field displays with the **Up** width and **Down** width fields.

  Click either the **Up** or **Down** radio buttons to define whether the logical link width is up or down.

  — **Bidirectional**: If you choose **Bidirectional**, the Symmetry field displays with the **Symmetrical** and **Asymmetrical** fields visible.

  Click either the **Symmetrical** or **Asymmetrical** radio button to define whether the logical link is symmetrical or asymmetrical. If you click the **Symmetrical** radio button, the Up and Down Width display together. If yo click the **Asymmetrical** radio button, the Up and Down Width display separately.

- **BWCIR**: Click the **BWICR** field and enter the Bandwidth Committed Rate (BWICR) in bits per second (bps) for the network zone.

7 Click the **Update** button. If the save is successful, the **Detail Network Zone** window opens displaying the network zone with the modified parameters. If the save is not successful, an error message appears giving you instructions. Follow the instructions and then click the **Update** button again.

8 You have completed this procedure.

Add network zone

Purpose of this procedure

Use this procedure to provision network zone parameters and add a network zone to the system.

Limitations and restrictions

A valid **Network Zone ID** parameter is numeric between 2 and 16777215.

A valid network zone name or network zone parent name must follow the DNS convention and the following rules:

- The name cannot start or end with "." or "-"
- The name does not support consecutive ".."
- The name does not support "_"
- The name is case insensitive.
- The name supports a maximum of 32 characters.

A valid **EncapsOverHead** parameter is numerical in the range of 0 to 1000000.

A valid **UnitSize** parameter is numerical in the range of 1 to 1000000.

A valid **UnitOverHead** parameter is numerical in the range of 0 to 1000000.

The **UnitSize** value must be bigger than the **UnitOverHead** value, or an error will display when you click the **Save** button.

If the **isFixedPDU** field is selected, you must fill out the **UnitSize** field and the **UnitOverHead** field.

Prerequisites

If a network zone is going to be added to the Policy Controller ensure that it has first been added to the CS 2000 GWC Manager. Only then can a network zone be added to the Policy Controller. This synchronization ensures the network zone ID is consistent between both the CS 2000 GWC Manager and the Policy Controller.

Refer to the GUI procedure “Add a Policy Controller” in NTP *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure and the commands, refer to the NTP *OSSGate User’s Guide* (NE10004-512).

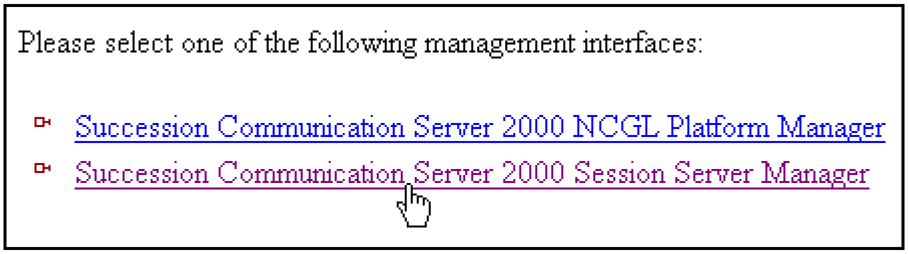
If adding a Predefined Link Layer Type, the Link Layer Type must have first been created using procedure Add a Link Layer Type on page 98.

Action

Add network zone

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

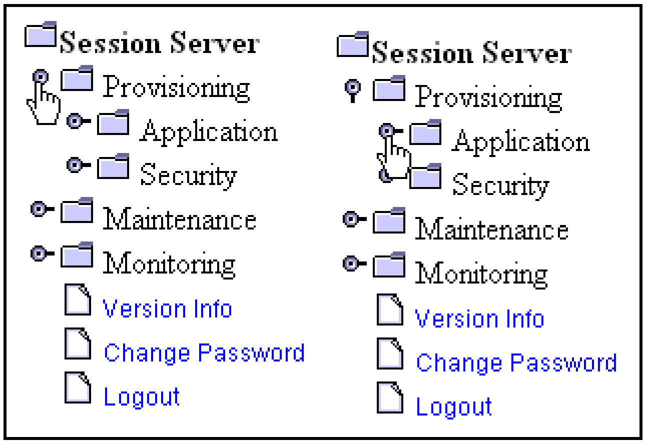


Please select one of the following management interfaces:

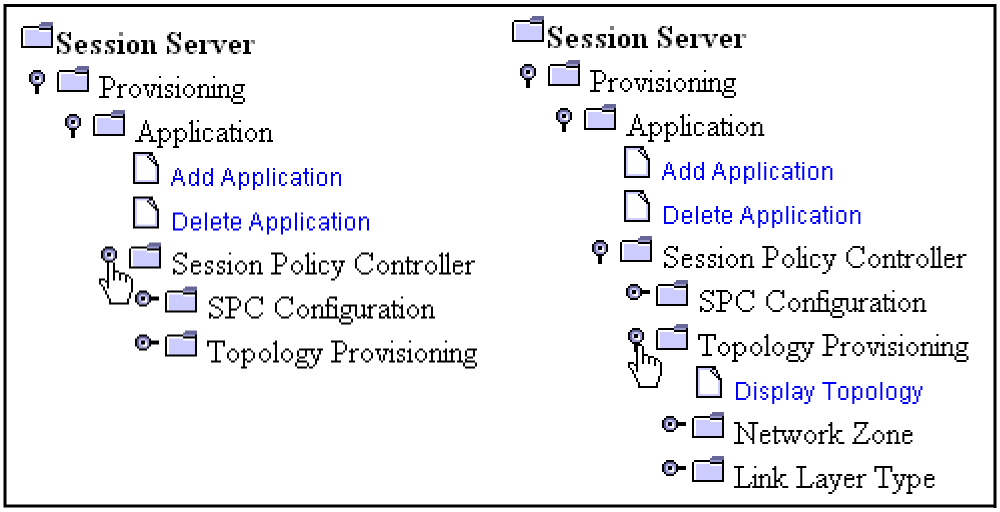
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

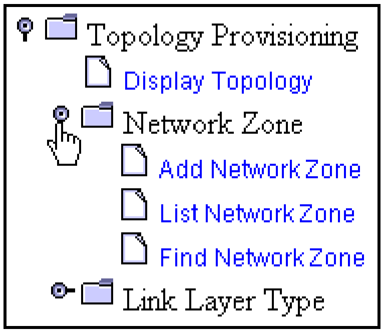
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



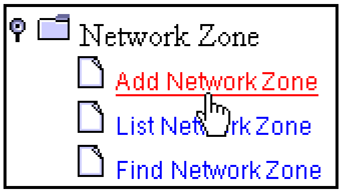
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



4 Select **Network Zone**.

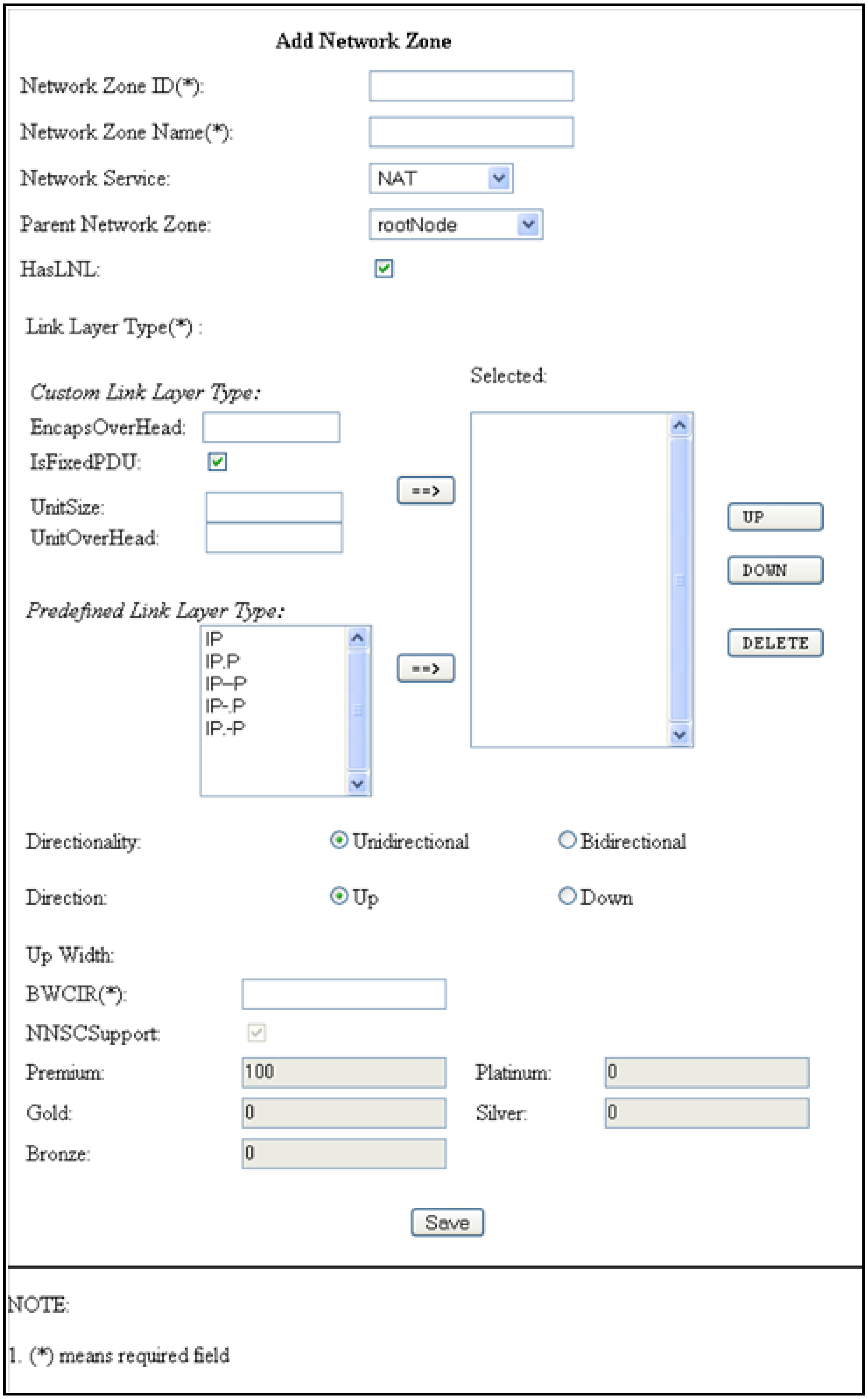


5 Select **Add Network Zone**



The **Add Network Zone** window opens.

Use table Add Network Zone window field descriptions on page 73 to help you fill out the fields in the **Add Network Zone** window.



Add Network Zone

Network Zone ID(*):

Network Zone Name(*):

Network Service: NAT

Parent Network Zone: rootNode

HasLNL: ☑

Link Layer Type(*) :

Custom Link Layer Type:

EncapsOverHead:

IsFixedPDU: ☑

UnitSize:

UnitOverHead:

Predefined Link Layer Type:

IP
IP.P
IP–P
IP-.P
IP.-P

Selected:

Directionality: ● Unidirectional ○ Bidirectional

Direction: ● Up ○ Down

Up Width:

BWCIR(*):

NNSCSupport: ☑

Premium: 100 Platinum: 0

Gold: 0 Silver: 0

Bronze: 0

NOTE:

1. (*) means required field

Add Network Zone window field descriptions (Sheet 1 of 4)

Field	Entry	Description
Network Zone ID	Range= numbers between 2 and 16777215	This is a required field. Identifies the network zone.
Network Zone Name	Range= 1 to 32 characters	This is a required field. Identifies the name of the network zone.

Network Service	Default= NoService
	Range= NAT or NoService
		Identifies the type of network service. There are two choices for this field:
		• NAT=Network Address Translation (NAT)
		• LBL=Limited Bandwidth Links (LBL)
		NoService is LBL.

Parent Network Zone		This is a required field. Select the parent zone from the drop-down box. Identifies the name of the parent zone that this network zone will belong to.

HasLNL	Default= Selected
	Range= Selected or Unselected
		The network zone uses a Logical Network Link (LNL).
		Selected=True The network zone uses a LNL
		Unselected=False The network zone does not use a LNL.
		Note: If the **Network Service** field is set to "NoService" then this option is mandatory and the check box will not be present. If the **Network Service** field is set to "NAT" then this field can be modified.

Add Network Zone window field descriptions (Sheet 2 of 4)

Field	Entry	Description
Link Layer Type		Lists the Link Layer Types that the system supports. **Custom Link Layer Type**= Allows you to create a custom Link Layer Type. Fill out the following fields to create a custom Link Layer Type: **EncapsOverHead** **IsFixedPDU** **UnitSize** **UnitOverHead** **Predefined Link Layer Type**=Select a Link Layer Type that has already been defined.
EncapsOverHead		This is the layer specific overhead required to encapsulate the layer payload within the next higher layer.
IsFixedPDU		Indicates if the layer has a fixed or variable unit size. **Selected**= True The layer has a fixed unit size. **Unselected**= False The layer has a variable unit size.
UnitSize		Indicates the application packet size.
UnitOverHead		Indicates the application packet over head.
Selected		Lists the Link Layer Types that you have added from either the **Custom Link Layer Type** fields or the **Predefined Link Layer Type** box**.** These Link Layer Types will be included in the network zone.

Add Network Zone window field descriptions (Sheet 3 of 4)

Field	Entry	Description
UP DOWN DELETE buttons		Use the UP, DOWN, and DELETE buttons to change the order of the layers in the **Selected** box, or delete them from this box.
Directionality		This is a required field. Defines whether the logical link is Bidirectional or Unidirectional. **Bidirectional**= Two sets of Bandwidth objects **Unidirectional**= One set of Bandwidth objects
Symmetry		Defines whether the logical link is symmetric or asymmetric. **Symmetrical**= One set of identical bandwidth objects are created. **Asymmetrical**=Two sets of bandwidth objects must be defined (Not necessarily identical). These two fields display only if the **Bidirectional** field is selected.
Direction		Defines whether the logical link is Up width or down width. **Up**=defines an up link **Down**=defines a down link These two fields only display if the **Unidirectional** field is selected.

Add Network Zone window field descriptions (Sheet 4 of 4)

Field	Entry	Description
BWCIR	Range= 0 to 2^63-1	**BWICR**=Bandwidth Committed Rate is the bandwidth of the network zone link in bits per second (bps). The Policy Controller uses BWICR to count the required bandwidth of the endpoints to determine when the call can be set up.
NNSCSupport	Default= Selected	Nortel Networks Service Classifier indicates the subscriber service class. In SN08, only voice calls are supported from the CS2000.
Premium		Indicates the level of Nortel Networks Service Class. **Premium** is the only Network Service Class available for SN08. All voice calls are tagged as Premium.
Save		**Saves** the network zone to the system.

6 Click the **Network Zone ID** field and enter a number that will identify the network zone in the system. The identifier must be unique and be between the number 2 and 16777215. This field is required.

7 Click the **Network Zone Name** field and enter a unique name for the network zone you want to add to the system. The name must be unique and meet the requirements listed in the section Limitations and restrictions on page 69. This field is required.

8 Select a network service for the network zone. From the **Network Service** drop-down box, select NAT or LBL.

9 Select a parent zone that the network zone will belong to. From the **Parent Network Zone** drop-down box, select one of the choices. This is a required field.

10 If the network zone has a Logical Layer Link (LNL), leave the box next to the **HasLNL** field selected (default). If the **HasLNL** field is unselected, then the fields below it will not be visible.

11 Under Link Layer Type, you can create a **Customer Link Layer Type**, or select a **Predefined Link Layer Type**.

If	Do
you want to create a **Custom Link Layer Type**	next step
you want to select a **Predefined Link Layer Type**	step 16

> ***Note:*** It is possible to combine the Predefined Link Layer Types with the Custom Link Layer Types. However, Nortel does not recommend this configuration. Use one Link Layer Type or the other.

12 Click the **EncapsOverHead** field and enter the size of the encapsulated overhead.

13 At the **IsFixedPDU** field:

If	Do
the **PDU is fixed**	next step
the **PDU is variable**	step 15

14 If the PDU is fixed:

a Click the box next to the **isFixedPDU** field to select this option.

> ***Note:*** The **UnitSize** and **UnitOverHead** fields are not enabled unless the **IsFixedPDU** field is selected.

The **UnitSize** and **UnitOverHead** fields display.

> ***Note:*** You must fill out both of these fields when the **isFixedPDU** option is selected.

b Click the **UnitSize** field and enter the unit size.

c Click the **UnitOverHead** field and enter the unit overhead. Go to step 16.

15 If the PDU is variable, unselect the **isFixedPDU** field, or leave it blank, and continue to the next step.

16 Select the layers you want included in the network zone.

- When you have created a Custom Link Layer Type, click the arrow button to the right of the **UnitSize** field to add the layer to the **Selected** box.

  OR

- If you are selecting a Predefined Link Layer Type, go to the the **Predefined Link Layer Type** box, highlight the layer, and click the arrow button to the right of this box to add the layer to the **Selected** box. Repeat this step to add more layers.

17 Change the order of the layers for the network zone, or prevent them from being added to the network zone by deleting them from the **Selected** box.

- To change the position of a layer:
  Select a layer from the **Selected** box, click the **UP** button to move the layer up in position, click the **DOWN** button to change the order of the layers for the network zone.

- To delete a layer:
  Select a layer from the **Selected** box, click the **DELETE** button to delete a layer from the **Selected** box.

18 Choose whether the logical link is unidirectional or bidirectional. Click either the **Unidirectional** or **Bidirectional** radio button.

If	Do
you choose **Unidirectional**	step 19
you choose **Bidirectional**	step 20

19 If you choose **Unidirectional**, the **Direction** field displays with the **Up** and **Down** fields. Click either the **Up** or **Down** radio button to define whether the logical link width is up or down. Go to step 21.

20 If you choose **Bidirectional**, the Symmetry field displays with the **Symmetrical** and **Asymmetrical** fields visible. Click either the **Symmetrical** or **Asymmetrical** radio button to define whether the logical link is symmetrical or asymmetrical.

21 Click the **BWICR** field and enter the Bandwidth Committed Rate (BWICR) in bits per second (bps) for the network zone.

22 Click the **Save** button to add the network zone to the system.

If the save is successful, the **List Network Zone** window opens, displaying the network zone that you just added.

If the save is not successful, an error message appears giving you instructions. Follow the instructions and then click the **Save** button again.

Repeat the steps above to add another network zone to the system.

23 If you were forwarded to this procedure from procedure Activating Network VCAC on the Policy Controller on page 13, return to that procedure and continue. You have completed this procedure.

24 You have completed this procedure.

List/Delete network zones

Purpose of this procedure

Use this procedure to perform the following tasks:

- List the provisioned network zones in the system
- Get the details for each provisioned network zone in the system
- Delete a provisioned network zone from the system

Limitations and restrictions

CAUTION
Deleting a network zone can be service impacting and can result in call failures. Take care when performing this procedure.

Prerequisites

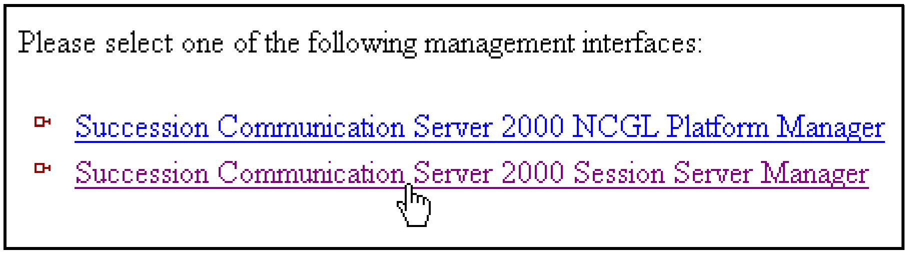
If you delete a network zone from the Policy Controller, ensure that it has first been deleted from the CS 2000 GWC Manager. Refer to the GUI procedure “Delete a Policy Controller” in NTP *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure and the commands, refer to the NTP *OSSGate User’s Guide* (NE10004-512).

Action

List/Delete network zones

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

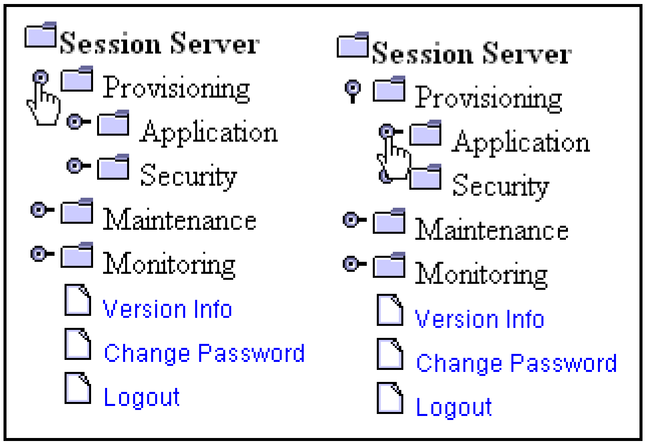


Please select one of the following management interfaces:

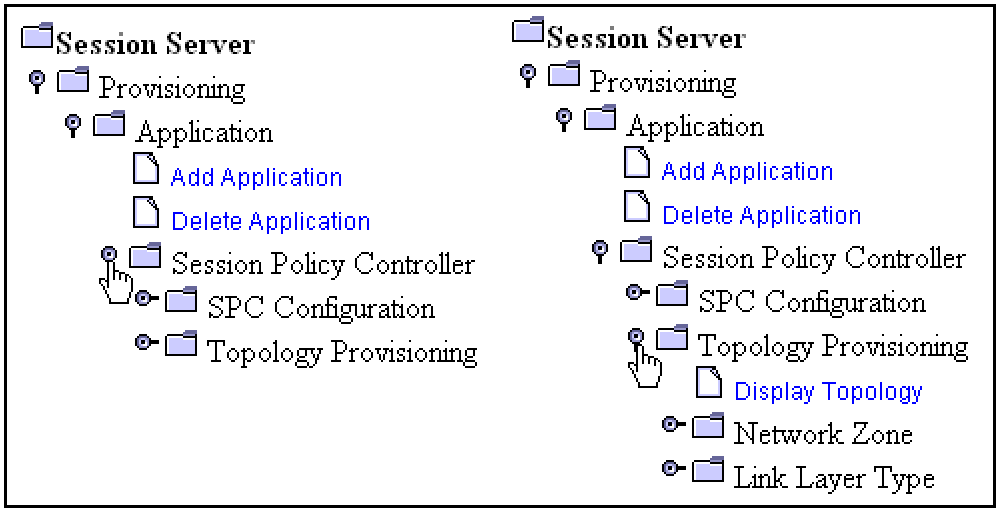
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

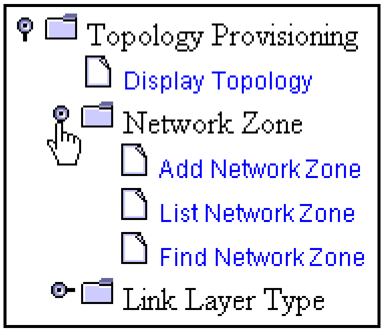
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



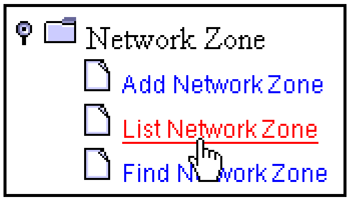
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



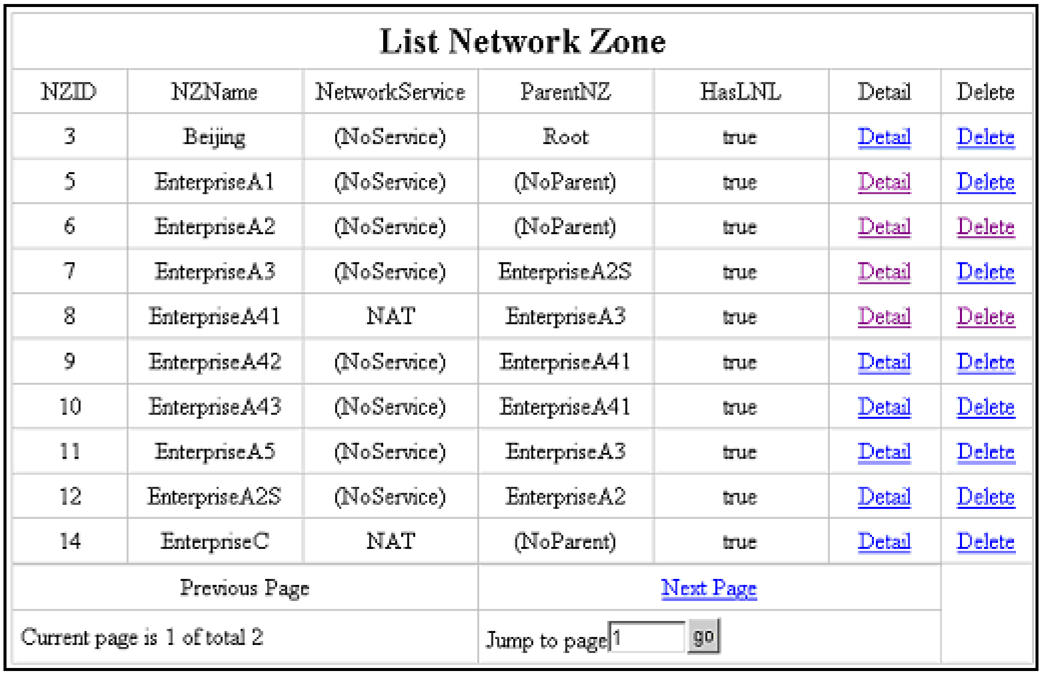
4 Select **Network Zone**.



5 Select **List Network Zone**



The **List Network Zone** window opens. The field descriptions are described in List Network Zone window field descriptions on page 82.



List Network Zone

NZID	NZName	NetworkService	ParentNZ	HasLNL	Detail	Delete
3	Beijing	(NoService)	Root	true	Detail	Delete
5	EnterpriseA1	(NoService)	(NoParent)	true	Detail	Delete
6	EnterpriseA2	(NoService)	(NoParent)	true	Detail	Delete
7	EnterpriseA3	(NoService)	EnterpriseA2S	true	Detail	Delete
8	EnterpriseA41	NAT	EnterpriseA3	true	Detail	Delete
9	EnterpriseA42	(NoService)	EnterpriseA41	true	Detail	Delete
10	EnterpriseA43	(NoService)	EnterpriseA41	true	Detail	Delete
11	EnterpriseA5	(NoService)	EnterpriseA3	true	Detail	Delete
12	EnterpriseA2S	(NoService)	EnterpriseA2	true	Detail	Delete
14	EnterpriseC	NAT	(NoParent)	true	Detail	Delete

Previous Page Next Page

Current page is 1 of total 2 Jump to page 1 go

List Network Zone window field descriptions (Sheet 1 of 3)

Field	Default	Description
NZID		Identifies the network zone by number.
NZName		Identifies the name of the network zone.

List Network Zone window field descriptions (Sheet 2 of 3)

Field	Default	Description
NetworkService	NoService	Identifies the type of network service. There are two types of network service: • Network Address Translation (NAT) • Limited Bandwidth Links (LBL) **NoService** means LBL.
ParentNZ		Identifies the name of the parent system that this network zone belongs to.
HasLNL		The network zone uses a Logical Network Link (LNL).
Detail		Click this link to get the details of a specific network zone.
Delete		Click this link to delete a specific network zone.
Previous Page Next Page		These navigation links display only when the number of network zones listed does not fit on one page. **Next Page**= Click this link to go to the next page that lists network zones. **Previous Page**= Click this link to go back to the previous page that lists network zones.

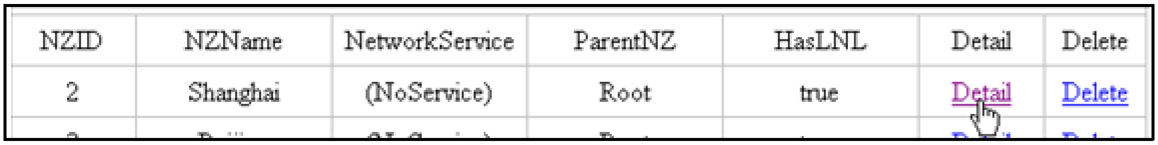
List Network Zone window field descriptions (Sheet 3 of 3)

Field	Default	Description
Current page is # of total #		This text displays only when the number of listed network zones does not fit on one page. It indicates your current page number and the total number of pages that list network zones.
Jump to Page #		This text displays only when the number of listed network zones does not fit on one page. It allows you to go to a specific page that lists network zones. To go to a specific page, click the entry box and enter the page number you want to go to and then click the **go** button. That specific page opens.

6

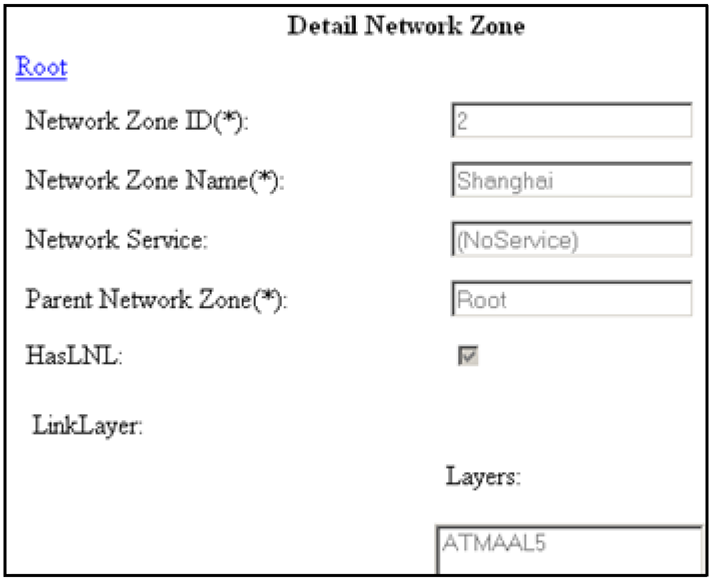
If	Do
you want **to view** the details of a specific network zone	step 7
you want **to delete** a network zone	step 8

7 To get the details of a specific network zone, click the **Details** link next to the network zone you want to see.



NZID	NZName	NetworkService	ParentNZ	HasLNL	Detail	Delete
2	Shanghai	(NoService)	Root	true	Detail	Delete

The **Detail Network Zone** window opens displaying read-only parameters for that specific network zone.



Detail Network Zone

Root

Network Zone ID(*):	2
Network Zone Name(*):	Shanghai
Network Service:	(NoService)
Parent Network Zone(*):	Root
HasLNL:	☑

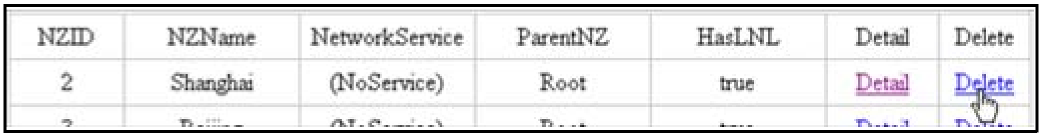
LinkLayer:

Layers:

ATMAAL5

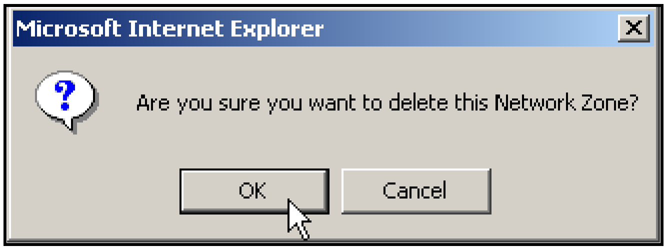
8 To delete a network zone:

a Click the **Delete** link next to the network zone you want to delete.



NZID	NZName	NetworkService	ParentNZ	HasLNL	Detail	Delete
2	Shanghai	(NoService)	Root	true	Detail	Delete

The following message window displays.



Microsoft Internet Explorer

Are you sure you want to delete this Network Zone?

b To delete the network zone, click the **OK** button, or click the **Cancel** button to cancel the deletion and close the message window.

Find network zones

Purpose of this procedure

The **Find Network Zone** window allows you to search for a specific provisioned network zone by one of the following methods:

- Numerical identifier of the network zone
- Name of the network zone
- Name of the network zone parent

Use procedure this procedure to find a provisioned network zone.

Limitations and restrictions

A valid **Network Zone ID** parameter is numeric between 2 and 16777215.

You cannot use wildcards in the any of the search fields.

A valid network zone name or network zone parent name must follow the DNS convention and the following rules:

- The name cannot start or end with a "." or "-"
- The name does not support consecutive ".."
- The name does not support "_"
- The name is case insensitive.
- The name supports a maximum of 32 characters.

Prerequisites

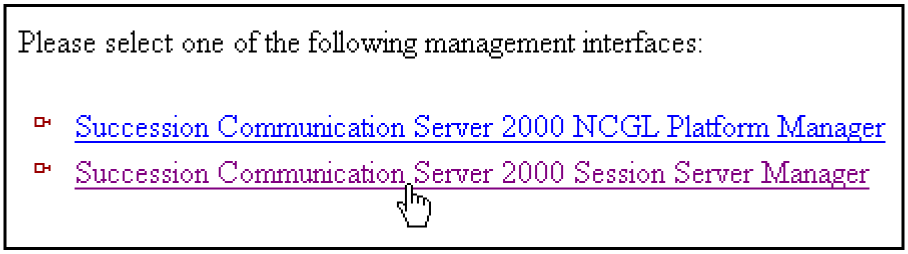
There are no prerequisites for this procedure.

Action

Find network zones

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

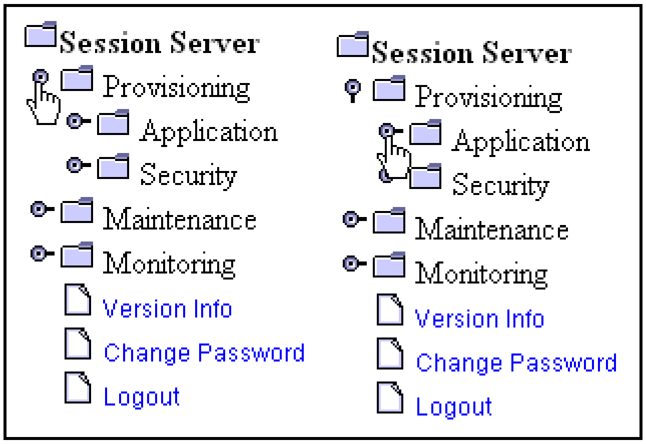


Please select one of the following management interfaces:

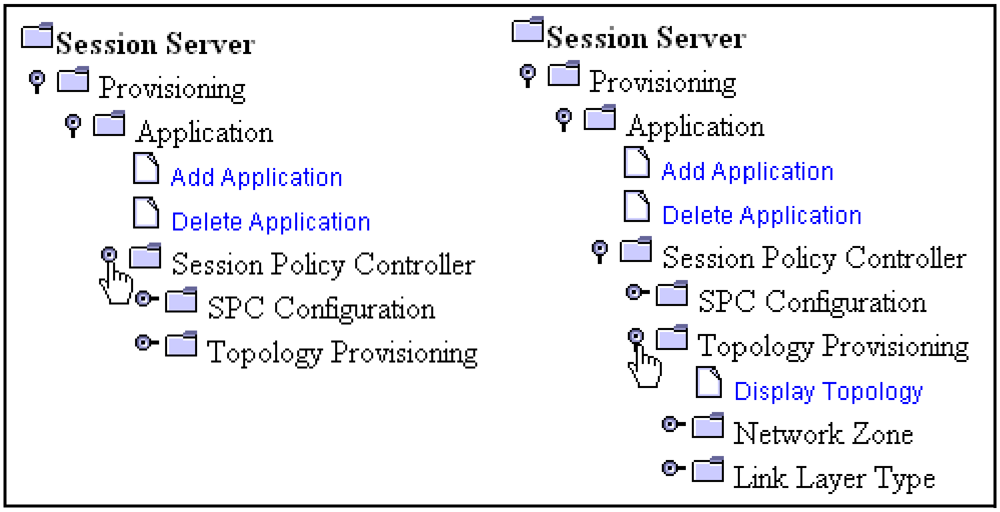
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

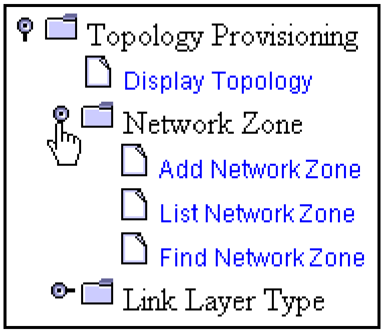
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



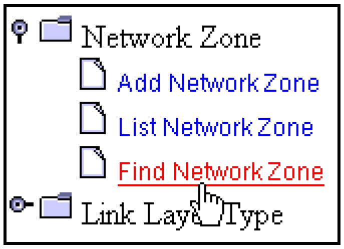
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



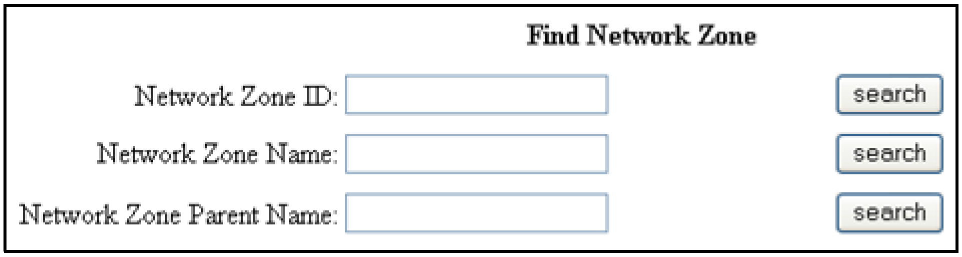
4 Select **Network Zone**.



5 Select **Find Network Zone**



The following **Find Network Zone** window opens.



Use table Find Network Zone window field descriptions on page 89 to help you fill out the fields for the **Find Network Zone** window.

Find Network Zone window field descriptions

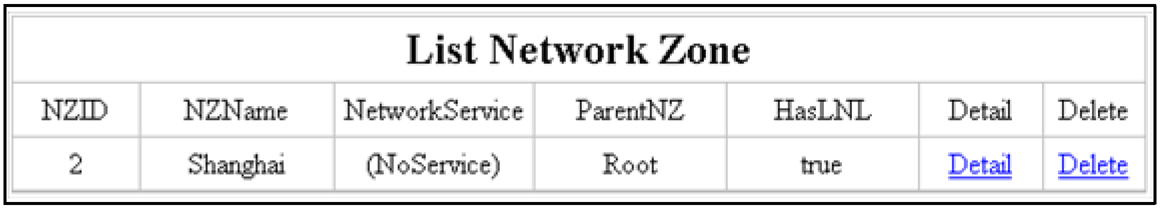
Field	Default	Description
Network Zone ID		The numerical identifier of the network zone.
Network Zone Name		The name of the network zone.
Network Zone Parent Name		The name of the parent zone that the network zone belongs to
Search		**Searches** the system by the field that you filled out. ***Note:*** If you leave all the fields blank and click any **Search** button, a list of all provisioned network zones displays.

6 To search for a provisioned network zone, use one of the following methods:

- Search for a network zone by its identifier. Click the **Network Zone ID** field and enter the identifier of the network zone you want to searching for. Then, click the **Search** button next to this field.
- Or, search for a network zone by its name. Click the **Network Zone Name** field and enter the name of the network zone you are searching for. Then, click the **Search** button next to this field.
- Or, search for a network zone by its parent name. Click the **Network Zone Parent Name** field and enter the name of the network zone parent you are searching for. Then, click the **Search** button next to this field.
- Or, list all provisioned network zones. Leave all fields blank and click on any **Search** button.

Note: You cannot use wildcards in the search fields.

The **List Network Zone** window opens (see following example) listing the parameters of the network zone that you searched on.



List Network Zone

NZID	NZName	NetworkService	ParentNZ	HasLNL	Detail	Delete
2	Shanghai	(NoService)	Root	true	Detail	Delete

Purpose of this procedure

From the **Link Layer Type** window you can perform the following tasks:

- List the Link Layer Type
- Modify the parameters of a Link Layer Type
- Delete a Link Layer Type

Use this procedure to list, modify, or delete a Link Layer Type.

Limitations and restrictions

You cannot delete or modify the parameters of a Link Layer Type if a network zone is using it.

When listing Link Layer Types, it is only possible to view the Predefined Link Layer Types. These link layers can be added across multiple network zones.

Custom Link Layer Types are network zone specific and can only be created and associated with a specific network zone. They will not be viewable from the List Link Layer Type option.

The maximum number of Link Layer Types supported is 500.

A valid Link Layer Type name must follow the DNS convention and the following rules:

- The name cannot start or end with a "." or "-"
- The name does not support consecutive ".."
- The name does not support "_"
- The name is case insensitive.
- The name supports a maximum of 32 characters.

A valid **EncapsOverHead** parameter is numerical in the range of 0 to 1000000.

A valid **UnitSize** parameter is numerical in the range of 1 to 1000000.

A valid **UnitOverHead** parameter is numerical in the range of 0 to 1000000.

The **UnitSize** parameter must be greater than the **UnitOverHead** parameter.

If the **isFixedPDU** field is selected, you must fill out the **UnitSize** field and the **UnitOverHead** field.

Prerequisites

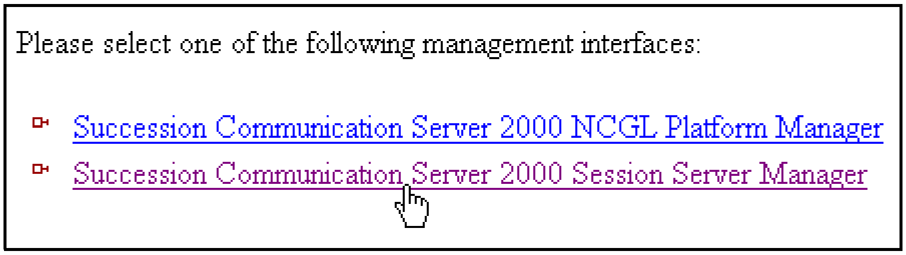
There are no prerequisites for this procedure.

Action

List/Modify/Delete a Link Layer Type

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

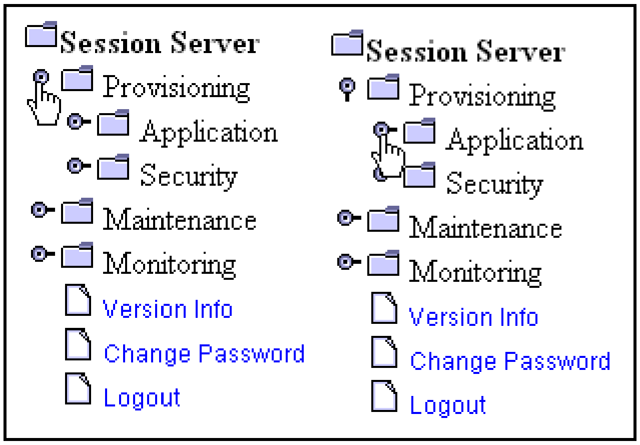


Please select one of the following management interfaces:

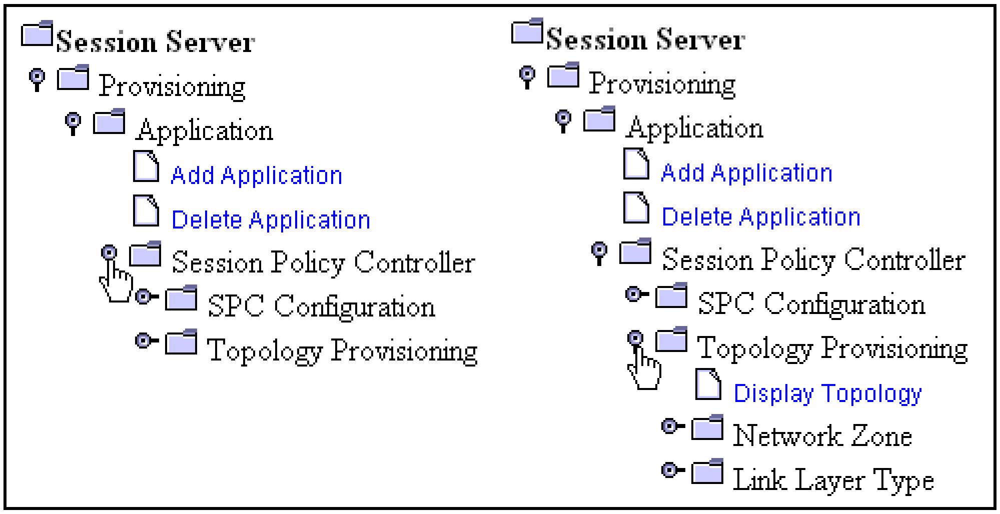
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

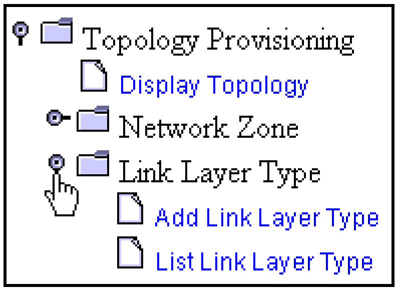
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



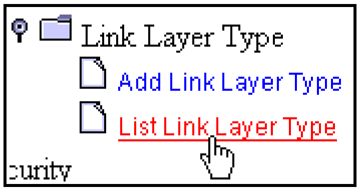
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



4 Select the **Link Layer Type** folder.



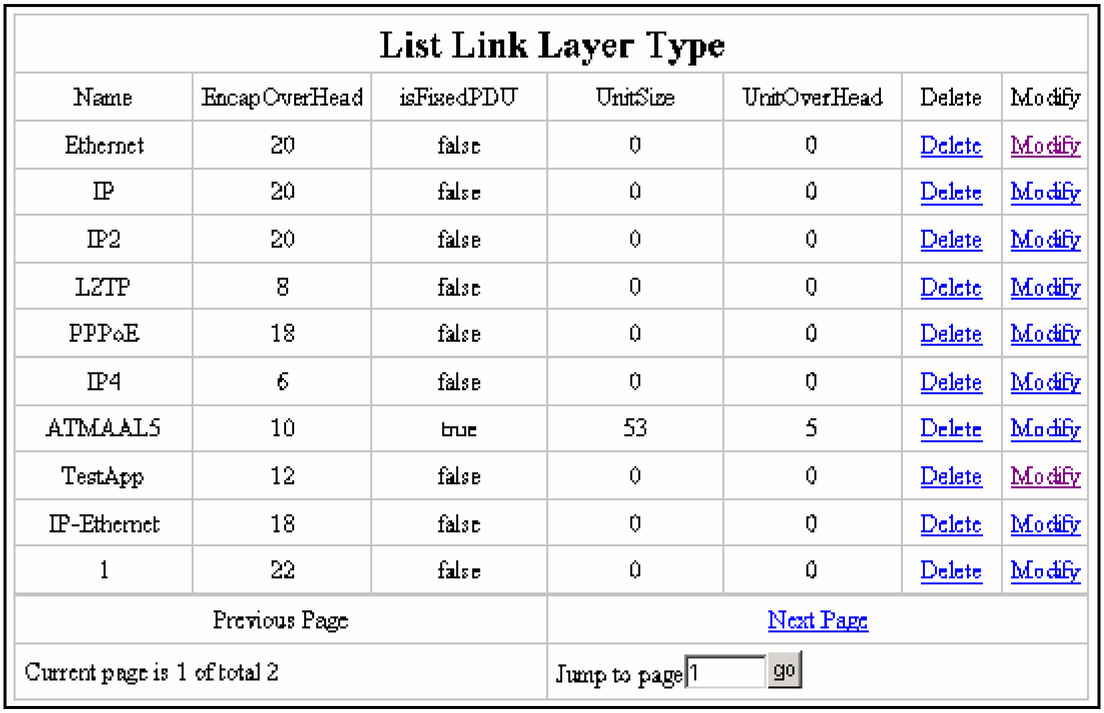
5 Click **List Link Layer Type**.



The **List Link Layer Type** window opens (see following example). This window contains the parameters for the Link Layer Types in the system.

Field descriptions for the **List Link Layer Type** window are in table List Link Layer Type window field descriptions on page 94.

To modify or delete the parameters of the Link Layer Type, go to step 6.



List Link Layer Type

Name	EncapOverHead	isFixedPDU	UnitSize	UnitOverHead	Delete	Modify
Ethernet	20	false	0	0	Delete	Modify
IP	20	false	0	0	Delete	Modify
IP2	20	false	0	0	Delete	Modify
L2TP	8	false	0	0	Delete	Modify
PPPoE	18	false	0	0	Delete	Modify
IP4	6	false	0	0	Delete	Modify
ATMAAL5	10	true	53	5	Delete	Modify
TestApp	12	false	0	0	Delete	Modify
IP-Ethernet	18	false	0	0	Delete	Modify
1	22	false	0	0	Delete	Modify

Previous Page Next Page

Current page is 1 of total 2 Jump to page 1 go

List Link Layer Type window field descriptions (Sheet 1 of 2)

Field	Entry	Descriptions
Name	Range= 1 to 32 characters	Specifies the Link Layer Type. The Link Layer Type Name should be unique.
EncapsOverHead	Range= 0 to 1000000	This is the layer specific overhead required to encapsulate the layer payload within the next higher layer.
isFixedPDU	Default= Unselected	Indicates if the layer has a fixed or variable unit size.
	Range= Unselected or Selected	**Selected**= True The layer has a fixed unit size. **Unselected**= False The layer has a variable unit size.
UnitSize	Range= 1 to 1000000	Indicates the application packet size.

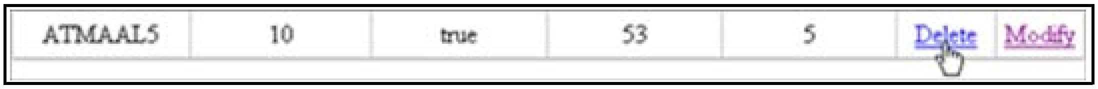
List Link Layer Type window field descriptions (Sheet 2 of 2)

Field	Entry	Descriptions
UnitOverHead	Range= 0 to 1000000	Indicates the application packet overhead.
Delete		Deletes the specific Link Layer Type.
Modify		Allows you to modify the parameters of the Link Layer Type.
Previous Page Next Page		These navigation links display only when the number of Link Layer Types listed does not fit on one page. **Next Page**= Click this link to go to the next page that lists Link Layer Types. **Previous Page**= Clink this link to go back to the previous page that lists Link Layer Types.
Current page is # of total #		This text displays only when the number of listed Link Layer Types does not fit on one page. It indicates your current page number and the total number of pages that list Link Layer Types.
Jump to Page #		This text displays only when the number of listed Link Layer Types does not fit on one page. It allows you to go to a specific page that lists Link Layer Types. To go to a specific page, click the entry box and enter the page number you want to go to and then click the **go** button. That specific page opens.

6

If	Do
you want **to delete** a Link Layer Type	step 7
you want **to modify** a Link Layer Type	step 10

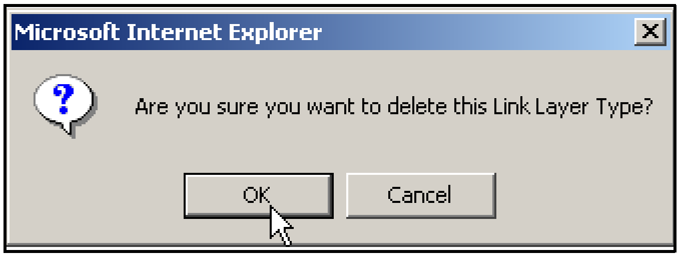
7 To delete a specific Link Layer Type, from the **Link Layer Type** window, click the **Delete** link next to the Link Layer Type that you want to delete.



ATMAAL5	10	true	53	5	Delete	Modify

Note: You can only delete the Link Layer Type if that Link Layer Type is not associated with another network zone. If a Link Layer is associated with another network zone, when you click the **Delete** link, an error message will display.

8 The following message box displays asking you to confirm the deletion of the Link Layer Type. Click the **OK** button to delete the Link Layer Type. Click the **Cancel** button to cancel the delete and close the message box.

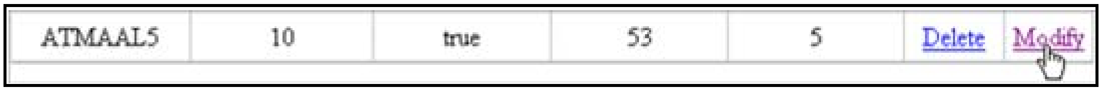


Microsoft Internet Explorer

Are you sure you want to delete this Link Layer Type?

9 If you clicked the **OK** button:
From the **List Link Layer Type** window, confirm that the Link Layer Type you just deleted is no longer there. If it is not visible, you have deleted the Link Layer Type.

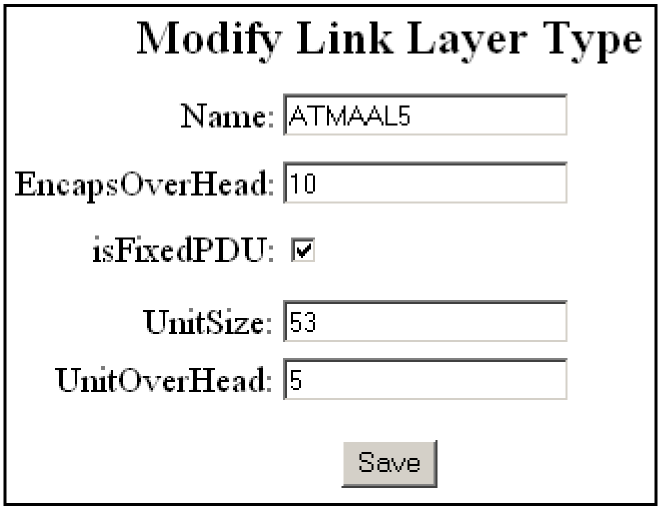
10 To modify a specific Link Layer Type:
From the **List Link Layer Type** window, click the **Modify** link next to the Link Layer Type that you want to modify.



ATMAAL5	10	true	53	5	Delete	Modify

The **Modify Link Layer Type** window displays with the parameters for that specific Link Layer Type ready to be modified (see following example).

> ***Note:*** The **UnitSize** and **UnitOverHead** fields are only visible when the **isFixedPDU** field is selected.



Modify Link Layer Type

Name: ATMAAL5

EncapsOverHead: 10

isFixedPDU: ☑

UnitSize: 53

UnitOverHead: 5

11 Modify the desired parameters and click the **Save** button to save the changes.

> ***Note:*** You can only modify parameters for the Link Layer Type if that Link Layer Type is not associated with another network zone. If a Link Layer is associated with another network zone, when you try to save the modified parameters, an error message will display.

If the save is successful, the **List Link Layer Type** window opens and displays the Link Layer Type that you have just modified.

If the save is not successful, an error message appears giving you instructions. Follow the instructions and then click the **Save** button again.

Add a Link Layer Type

Purpose of this procedure

Use this procedure to add a Link Layer Type to the system.

Limitations and restrictions

The maximum number of Link Layer Types supported is 500.

A valid Link Layer Type name must follow the DNS convention and the following rules:

- The name cannot start or end with a "." or "-"
- The name does not support consecutive ".."
- The name does not support "_"
- The name is case insensitive.
- The name supports a maximum of 32 characters.

A valid **EncapsOverHead** parameter is numerical in the range of 0 to 1000000.

A valid **UnitSize** parameter is numerical in the range of 1 to 1000000.

A valid **UnitOverHead** parameter is numerical in the range of 0 to 1000000.

The **UnitSize** value must be greater than the **UnitOverHead** value.

If the **isFixedPDU** field is selected, you must fill out the **UnitSize** field and the **UnitOverHead** field.

Prerequisites

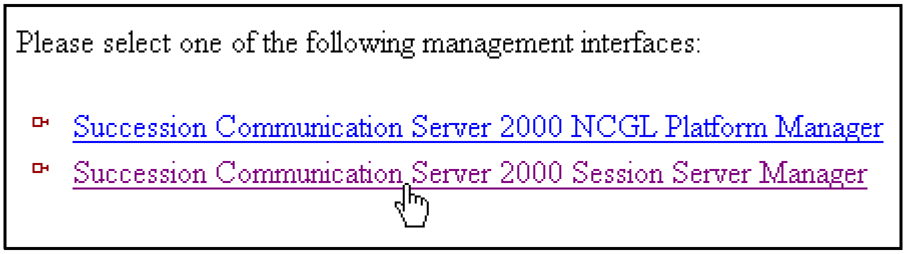
There are no prerequisites for this procedure.

Action

Add a Link Layer Type

At the Launch Point

1 From the launch point menu, select ***Succession Communication Server 2000 Session Server Manager***.

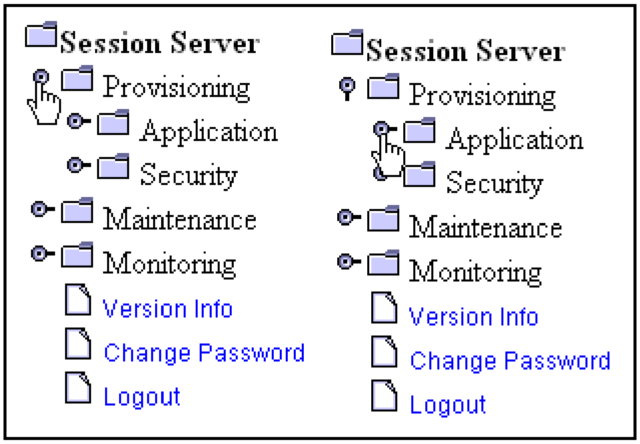


Please select one of the following management interfaces:

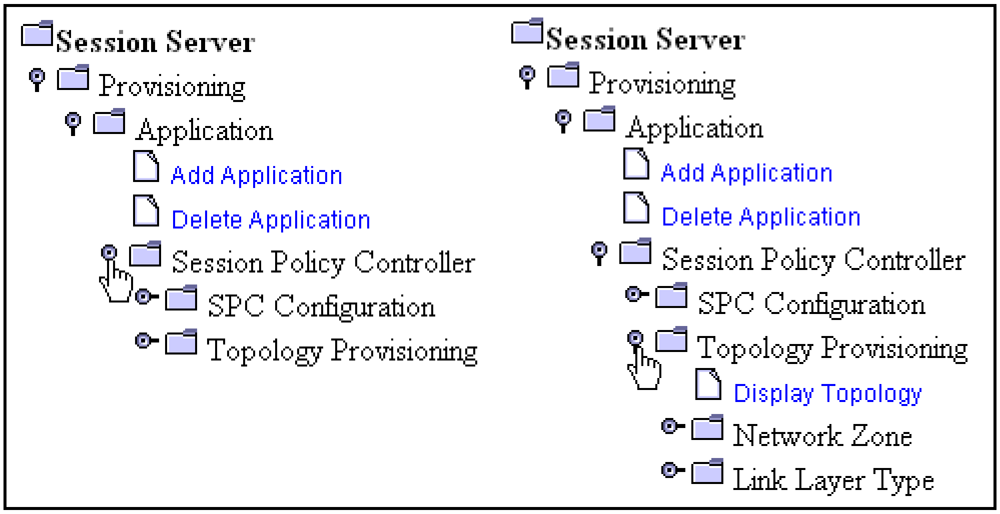
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

The Session Server Manager GUI opens in your Web browser.

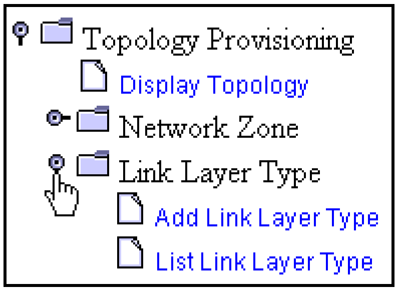
2 Under the **Session Server** folder, select the **Provisioning** folder and then select the **Application** folder.



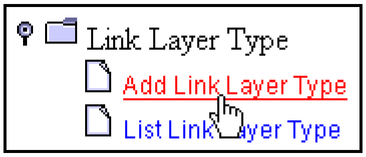
3 Select the **Session Policy Controller** folder, and then select the **Topology Provisioning** folder.



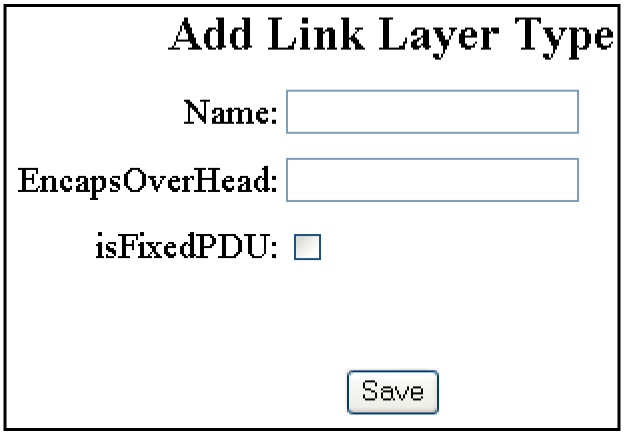
4 Select the **Link Layer Type** folder.



5 Click **Add Link Layer Type.**



The **Add Link Layer Type** window opens.



Use table Add Link Layer Type window field descriptions on page 101 to help you fill out the fields for the **Add Link Layer Type** window.

Add Link Layer Type window field descriptions

Field	Entry	Description
Name	Range= 1 to 32 characters	Specifies the Link Layer Type
EncapsOverHead	Range= 0 to 1000000	This is the layer specific overhead required to encapsulate the layer payload within the next higher layer.
isFixedPDU	Default= Unselected	Indicates if the layer has a fixed or variable unit size.
	Range= Unselected or Selected	**Selected**= True The layer has a fixed unit size. **Unselected**= False The layer has a variable unit size.
UnitSize	Range= 1 to 1000000	Indicates the application packet size.
UnitOverHead	Range= 0 to 1000000	Indicates the application packet over head.
Save		Saves the Link Layer Type to the system.

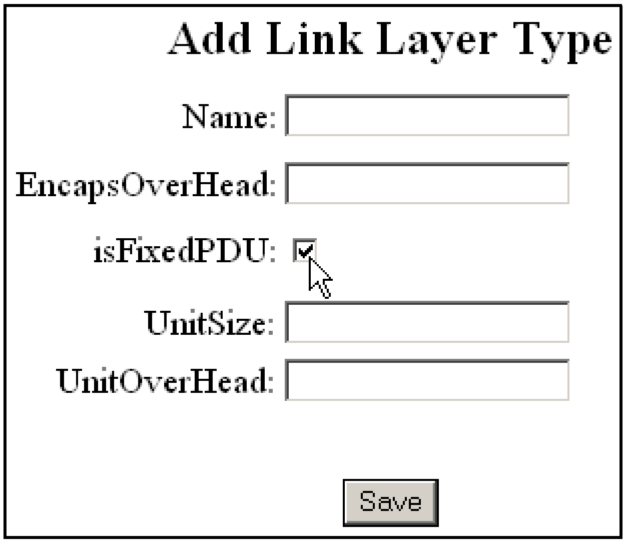
6 Click the **Name** field and enter the name of the Link Layer Type.

7 Click the **EncapsOverHead** field and enter the size of the encapsulated overhead.

8 At the **isFixedPDU** field:

If	Do
the **PDU is fixed**	step 9
the **PDU is variable**	step 12

9 If the PDU is fixed, click the box next to the **isFixedPDU** field to select this option. The **UnitSize** and **UnitOverHead** fields display (see graphic below). You must fill out both of these fields when the **isFixedPDU** option is selected.



Add Link Layer Type

Name:

EncapsOverHead:

isFixedPDU: ☑

UnitSize:

UnitOverHead:

10 Click the **UnitSize** field and enter the unit size. Click the **UnitOverHead** field and enter the unit overhead. Go to step 12.

> ***Note:*** The **UnitSize** value must be greater than the **UnitOverHead** value.

11 If the PDU is variable, unselect the **isFixedPDU** field, or leave it unselected, and continue to the next step.

12 Click the **Save** button to add a Link Layer Type to the system.

If the save is successful, the **List Link Layer Type** window opens and displays the Link Layer Type that you have just added.

If the save is not successful, an error message appears giving you instructions. Follow the instructions and then click the **Save** button again.

13 You have completed this procedure.

XML commands for the Policy Controller Topology Manager

Purpose of this procedure

The Policy Controller Topology Manager provides a provisioning interface for OSS, which you can log into by telnet and provision topology data using Extensible Markup Language (XML) commands. The XML commands are compared against the rules from a set of XML Schema (XSD) files for the Policy Controller Topology Manager.

Use the XML commands in the following table to configure and manage the Policy Controller Topology Manager.

XML command	Definition
addNetworkZone	Add a network zone to the system
deleteNetworkZone	Delete a network zone from the system
changeNetworkZone	Changes attributes of a network zone
queryNetworkZone	Retrieves detailed network zone information
AddLinkLayerType	Add a Link Layer Type to the system
deleteLinkLayerType	Delete a Link Layer Type from the system
changeLinkLayerType	Change a Link Layer Type
queryLinkLayerType	Retrieves detailed Link Layer Type information

Login to the Topology Manager

The Topology Manager implements a telnet protocol over a simple TCP/IP socket connection to allow clients to connect to the Topology Manager. While the connection is based on telnet, it does not implement a complete set of telnet capabilities, and does not require the client to support all the telnet options. The client or OSS establishes a TCP/IP socket connection to a specific port number (that is user configurable) on the server running the Policy Controller application.

The Topology Manager continuously listens for incoming connection requests. For each connection request, it starts a session after the username and password authentication, which you can use to send XML provisioning commands.

Connecting to the Topology Manager

When the Topology Manager is configured to set **sshPortFwd=true** (on), you can connect to the Topology Manager using procedure “Setting up a connection to the Topology Manager using ssh” in NTP *Policy Controller Security and Administration*, NN10434-611.

When the Topology Manager is configured to set **sshPortFwd=false** (off), a telnet client or OSS can connect to the Topology Manager by initiating a telnet session to the correct host name (or IP address) and port number. Users must belong to the primary authentication group “succcssn” to login to Topology Manager with the following command:

```
$ telnet <spc_host_name or IP address> <tm_primary_port>
```

> ***Note:*** The customer network administrator assigns a host name or IP address to the server where the Topology Manager is configured during installation and setup. Refer to your local network administrator for the correct address. The default primary port is 18023, which is configurable from the Policy Controller Web GUI.

The following is an example of a Topology Manager login:

```
$ telnet 47.153.178.243 18023

Trying 47.153.178.243...

Connected to 47.153.178.243.
Escape character is '^]'.
Enter username and password

> topoadm topoadm

topoadm logged in at 24/11 2004 11:58.

*****************************************
**                                     **
**                                     **
**       SPC Topology Manager          **
**                                  **
**                                     **
**  This is the SPC topology        **
**  managment tool.                 **
**                                  **
*****************************************
```

Supported Topology Manager control commands

After you have logged into the Topology Manager, it is in XML mode ('>' prompt) and only XML commands are accepted. To change from XML mode ('>' prompt) to Control mode ('?' prompt), enter **Ctrl+B** at '>' prompt.

The following commands are supported in Control mode:

- **logout:** Log out of the Topology Manager. The current or new user can login after a logout.

```
>^B
enter control mode.
?logout
topoadm logged out.


Enter username: topomtc
Enter passwd:
topomtc logged in at 24/11 2004 12:08.


*****************************************************
**                           **
**   SPC Topology Manager    **
**                           **
**  This is the SPC topology **
** managment tool.           **
**                            **
**                            **
******************************************************
```

- **mode xml:** Allows the user to change from Control mode to XML mode.

```
>^B
?mode xml
enter xml mode!
>
```

- **quit/exit/clearconv:** Allows the user to end the Topology Manager session.

```
>^B
```

```
?exit

Connection closed by foreign host.
```

Topology Manager access privileges

The Topology Manager reuses the OSSGate application access level. The Topology Manager user must belong to the “succssn” primary group and to one of the following Topology Manger user groups listed below:

- mgcadm
- mgcrw
- mgcsprov
- mgcmtc
- mgcro

Note: For more information on access privileges, refer to NTP *Policy Controller Security and Administration*, NN10434-611.

Topology Manager user group

User authentication is complete during the login process. The user needs the correct primary and secondary group privileges to login to the Topology Manager. Otherwise, the login will fail.

The following table shows the relationship between the XML Topology Manager commands and the user groups.

	User groups				
XML command	**mgcadm**	**mgcrw**	**mgcsprov**	**mgcmtc**	**mgcro**
addNetworkZone	X	X			
deleteNetworkZone	X	X			
changeNetworkZone	X	X			
queryNetworkZone	X	X	X	X	X
addLinkLayerType	X	X			
deleteLinkLayerType	X	X			
(Sheet 1 of 2)					

	User groups				
XML command	mgcadm	mgcrw	mgcsprov	mgcmtc	mgcro
changeLinkLayerType	X	X			
queryLinkLayerType	X	X	X	X	X
(Sheet 2 of 2)					

Topology Manager XML return codes

For each XML command, the Topology Manager will return an XML response formatted like the following example:

Example

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
      <MethodName usn="1" version="1.0">
        <ReturnData>
       <ReturnCode text="Successful operation value="0"/>
        </ReturnData>
      </MethodName>
   </Methods>
 </Response>
 </CommandList>
```

The following table lists all the Topology Manager XML return codes and the corresponding message.

Return code	Message
0	Successful operation
2	Request Rejected due to Resource Limits Reached
3	Application was Commanded to Abort
4	Database connection failed
5	Unknown internal error
(Sheet 1 of 3)	

Return code	Message
6	Database is now in read only state
7	Successful operation, but there is no data in the database currently
8	Database SQL operation failed
301	Incorrect command version
400	ID of NetworkZone is duplicated
401	Name of Network Zone is duplicated
402	Specified Network Zone’s Parent does not exist
403	Levels of Network Zone on the chain has exceeded the maximum 5 levels limitation
404	Network Zone chain should not contain a loop
405	Required UpBWInfo or DownBWInfo is missing
406	Invalid NZ or LLT name. Name should be DNS compliant
407	NNSC allocation number error
408	UnitSize should be bigger than UnitOverhead
409	Network Zone deletion failed due to existing Network Zone association
410	Specified Network Zone does not exist
411	Specified LinkLayerType does not exist
412	Name of LinkLayerType is duplicated
413	Operation failed as another Network Zone is associated with this LinkLayerType
414	Successful operation and more results need to be returned
416	Logical network link should be provided in non-NAT Network Zone
(Sheet 2 of 3)	

Return code	Message
417	Deleting the logical network link from the current Network Zone is not allowed
418	The maximum supported Network Zone number has been reached
419	The maximum supported Link Layer Type number has reached
501	The Security Privilege is not sufficient to perform this action

(Sheet 3 of 3)

When return code 414 is returned during querying the network zone or Link Layer Type from the topology manager XML interface

Although this return code is not zero, return code 414 does not mean it is an error response. The corresponding return text to the code 414 is “Successful operation and more results need to be returned”, which means there is more data in the database to meet the query condition. Additional queries can be issued by operating personnel to retrieve this data.

The code 414 may be returned in the following situations:

- There are more NetworkZones (NZ) in the topology database than the number (500 network zones for Policy Controllers in SN08) of NZs that can be returned in one XML response. Operating personnel can do additional queries to get the remainder of information when the code 414 is returned. The following XML commands can return code 414.

```
<?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
              <Command>
              <Interface>ITransIf</Interface>
                    <Methods>
                      <queryNetworkZone usn="1" version="1.0">
                        <Parameters>
                        </Parameters>
                      </queryNetworkZone>
                    </Methods>
              </Command>
        </CommandList>

    <?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
            <Command>
            <Interface>ITransIf</Interface>
                <Methods>
                  <queryNetworkZone usn="1" version="1.0">
                    <Parameters>
             <IDMin>101</IDMin>
                    </Parameters>
                  </queryNetworkZone>
                </Methods>
            </Command>
        </CommandList>

<?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
            <Command>
            <Interface>ITransIf</Interface>
                <Methods>
                  <queryNetworkZone usn="1" version="1.0">
                    <Parameters>
             <IDMax>1200</IDMax>
                    </Parameters>
                  </queryNetworkZone>
                </Methods>
            </Command>
        </CommandList>

<?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
            <Command>
            <Interface>ITransIf</Interface>
                <Methods>
                  <queryNetworkZone usn="1" version="1.0">
                    <Parameters>
             <IDMin>101</IDMin>
```

```
          <IDMax>1200</IDMax>
               </Parameters>
              </queryNetworkZone>
             </Methods>
         </Command>
     </CommandList>
```

- There are more NetworkZones whose ID is between IDMin and IDMax in the topology database than the value of <MaxZones>. Operating company personnel can do additional queries to get the remainder of information when the code 414 is returned. The following XML command can return code 414.

```
<?xml version="1.0" encoding="UTF-8"?>
     <CommandList>
         <Command>
         <Interface>ITransIf</Interface>
             <Methods>
              <queryNetworkZone usn="1" version="1.0">
               <Parameters>
          <IDMin>101</IDMin>
          <IDMax>120</IDMax>
          <MaxZones>5</MaxZones>
               </Parameters>
              </queryNetworkZone>
             </Methods>
         </Command>
     </CommandList>
```

- There are more NetworkZones whose ID is larger than or equal to <IDMin> in the topology database than the value of <MaxZones>. Operating company personnel can do additional queries to get the remainder of information when the code 414 is returned. The following XML command can return code 414.

```
<?xml version="1.0" encoding="UTF-8"?>
     <CommandList>
         <Command>
         <Interface>ITransIf</Interface>
             <Methods>
              <queryNetworkZone usn="1" version="1.0">
```

```
                       <Parameters>
               <IDMin>101</IDMin>
               <MaxZones>5</MaxZones>
                       </Parameters>
                      </queryNetworkZone>
                    </Methods>
              </Command>
        </CommandList>
```

- There are more NetworkZones whose ID is less than or equal to <IDMax> in the topology database than the value of <MaxZones>. Operating company personnel can do additional queries to get the remainder of information when the code 414 is returned. The following XML command can return code 414.

```
<?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
              <Command>
              <Interface>ITransIf</Interface>
                    <Methods>
                      <queryNetworkZone usn="1" version="1.0">
                       <Parameters>
               <IDMax>120</IDMax>
               <MaxZones>5</MaxZones>
                       </Parameters>
                      </queryNetworkZone>
                    </Methods>
              </Command>
        </CommandList>
```

- There are more LinkLayerTypes in the topology database than the value of <MaxTypes>. Operating company personnel can do additional queries to get the remainder of information when the code 414 is returned. The following XML command can return code 414.

```
<?xml version="1.0" encoding="UTF-8"?>
        <CommandList>
              <Command>
              <Interface>ITransIf</Interface>
                    <Methods>
                      <queryLinkLayerType usn="1" version="1.0">
```

```
            <Parameters>
      <MaxTypes>5</MaxTypes>
            </Parameters>
           </queryLinkLayerType>
          </Methods>
      </Command>
</CommandList>
```

XML NetworkZone commands

Provisioning NetworkZones

Provision a network zone according to the following rules:

- A valid network zone ID is in the range 2 to 16777215
- A valid network zone name follows the DNS convention and the following rules:
    1) Name can not start with a "." or "-"
    2) Name can not end with a "." or "-"
    3) Consecutive ".." are not supported.
- The network zone name is case insensitive.
- The maximum number of network zones supported is 32000.
- The maximum layers of a logical network link are 10.
- A valid <BWCIR> value should be in the range 0 to 2^63-1.
- If all the 5 NNSC allocations are provisioned, they should sum up to 100. If parts of the 5 NNSC allocations are provisioned, they should sum up to less or equal to 100.

  In Policy Controller release one, Premium Network Service Class is the only Network Service Class available for the SN08 release, therefore the following conditions apply:

  — Premium is set to 100% and all four service classes are set to 0, because voice calls are tagged as Premium.

  — In the XML commands, <NNSC> does not appear in <UpBWInfo> or <DownBWInfo>.
- A valid <Overhead> value is in the range 0 to 1000000.
- A valid <UnitSize> value is in the range 1 to 1000000
- A valid <UnitOverhead> value is in the range 0 to 1000000.
- The <UnitSize> value has to be bigger than the <UnitOverhead> value.

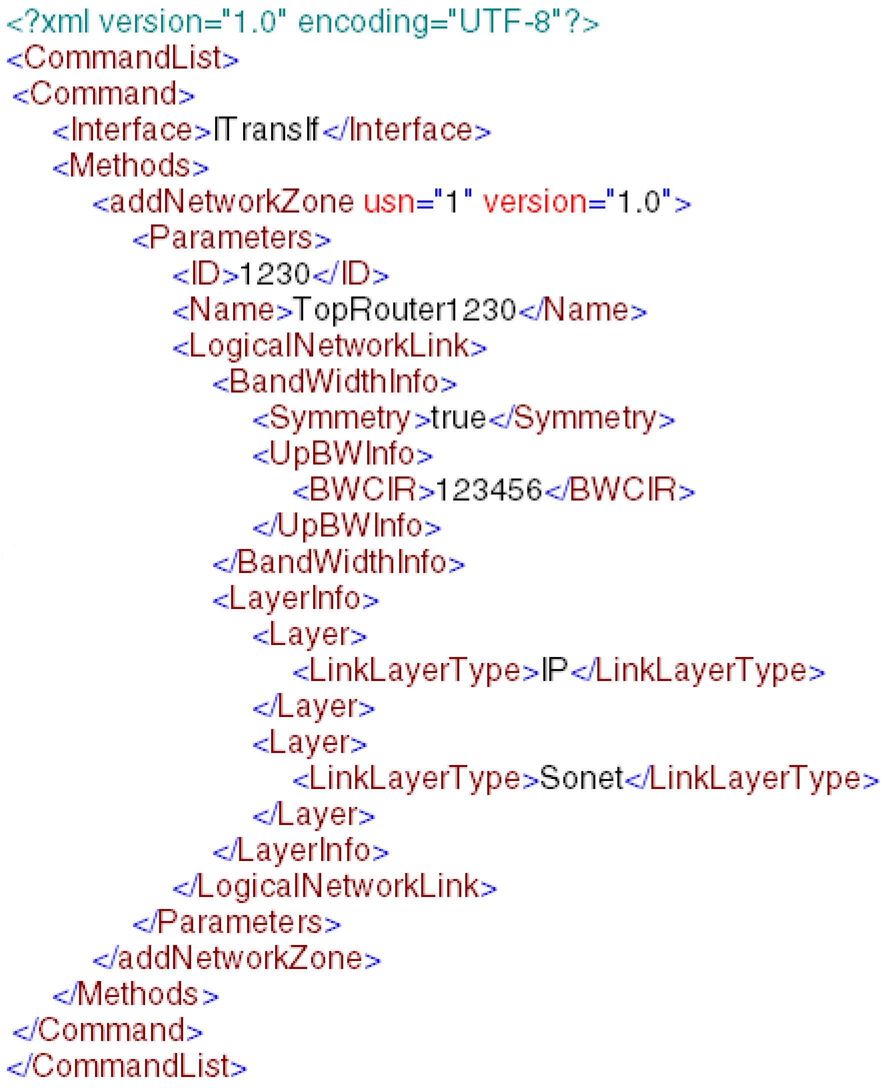
addNetworkZone

You can add a root NetworkZone if the <Parent> attribute is not present or the <ParentID> is set to zero.

You can add a non-root NetworkZone by specifying the <ParentID> or the <ParentName>.

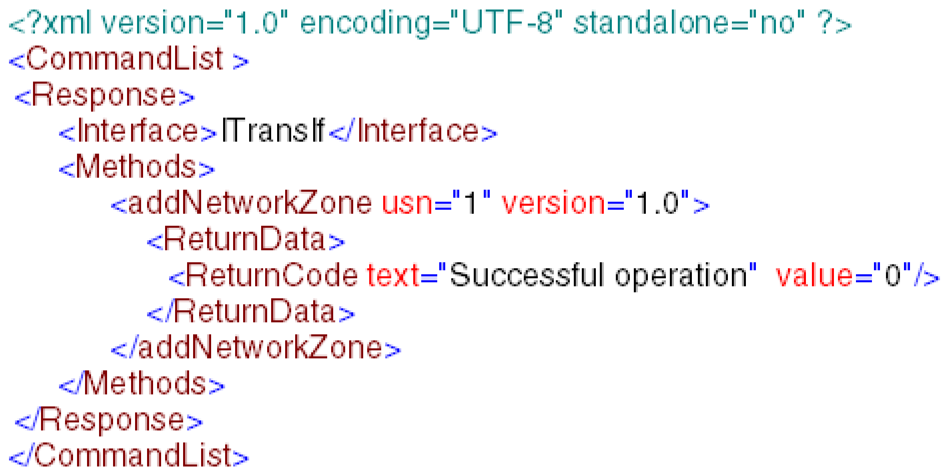
Three types of NetworkZones are supported: NAT, LBL and NAT/LBL composite. The following examples give the XML commands for adding each type of NetworkZone.

An example of an **addNetworkZone** request that adds a root LBL NZ with the <Parent> attribute not present:



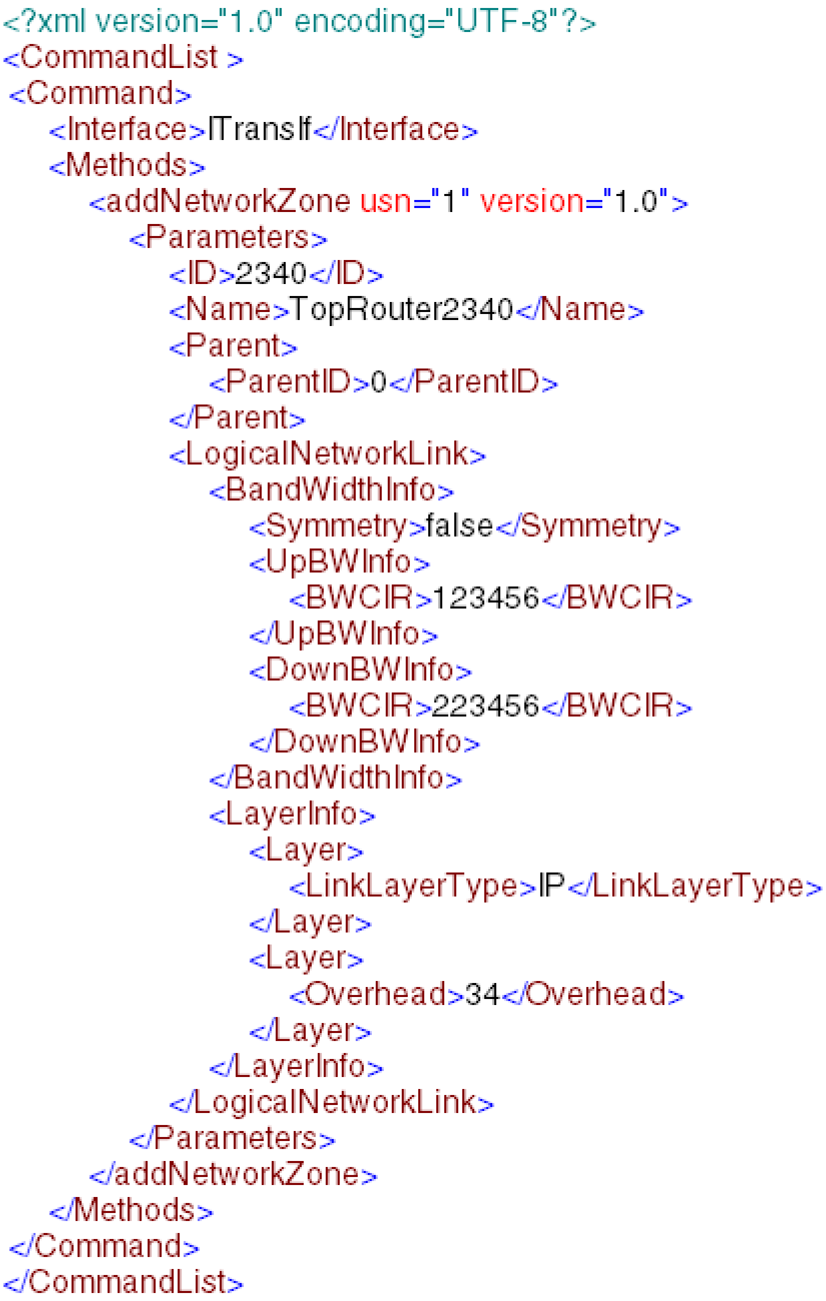
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addNetworkZone usn="1" version="1.0">
          <Parameters>
             <ID>1230</ID>
             <Name>TopRouter1230</Name>
             <LogicalNetworkLink>
                <BandWidthInfo>
                   <Symmetry>true</Symmetry>
                   <UpBWInfo>
                      <BWCIR>123456</BWCIR>
                   </UpBWInfo>
                </BandWidthInfo>
                <LayerInfo>
                   <Layer>
                      <LinkLayerType>IP</LinkLayerType>
                   </Layer>
                   <Layer>
                      <LinkLayerType>Sonet</LinkLayerType>
                   </Layer>
                </LayerInfo>
             </LogicalNetworkLink>
          </Parameters>
       </addNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addNetworkZone** success response:



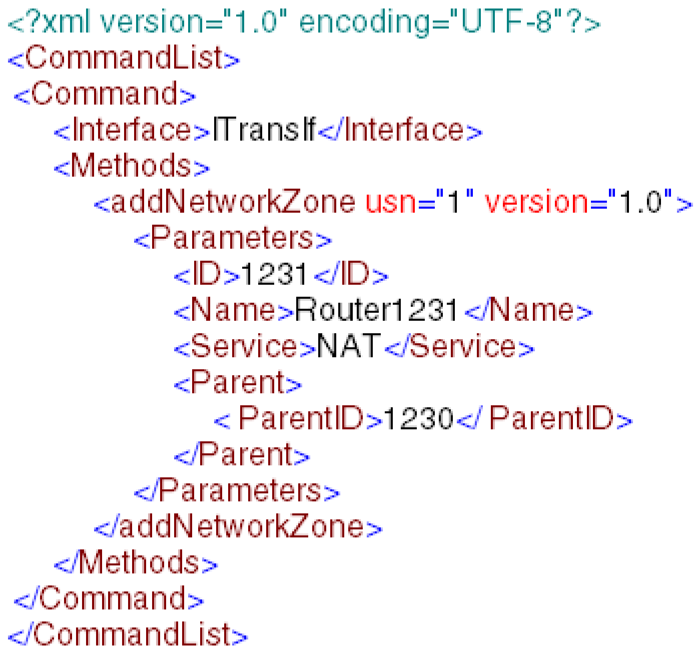
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <addNetworkZone usn="1" version="1.0">
             <ReturnData>
               <ReturnCode text="Successful operation"  value="0"/>
             </ReturnData>
          </addNetworkZone>
     </Methods>
 </Response>
</CommandList>
```

An example of an **addNetworkZone** request that adds a root LBL NZ with the <ParentID> being set to zero:



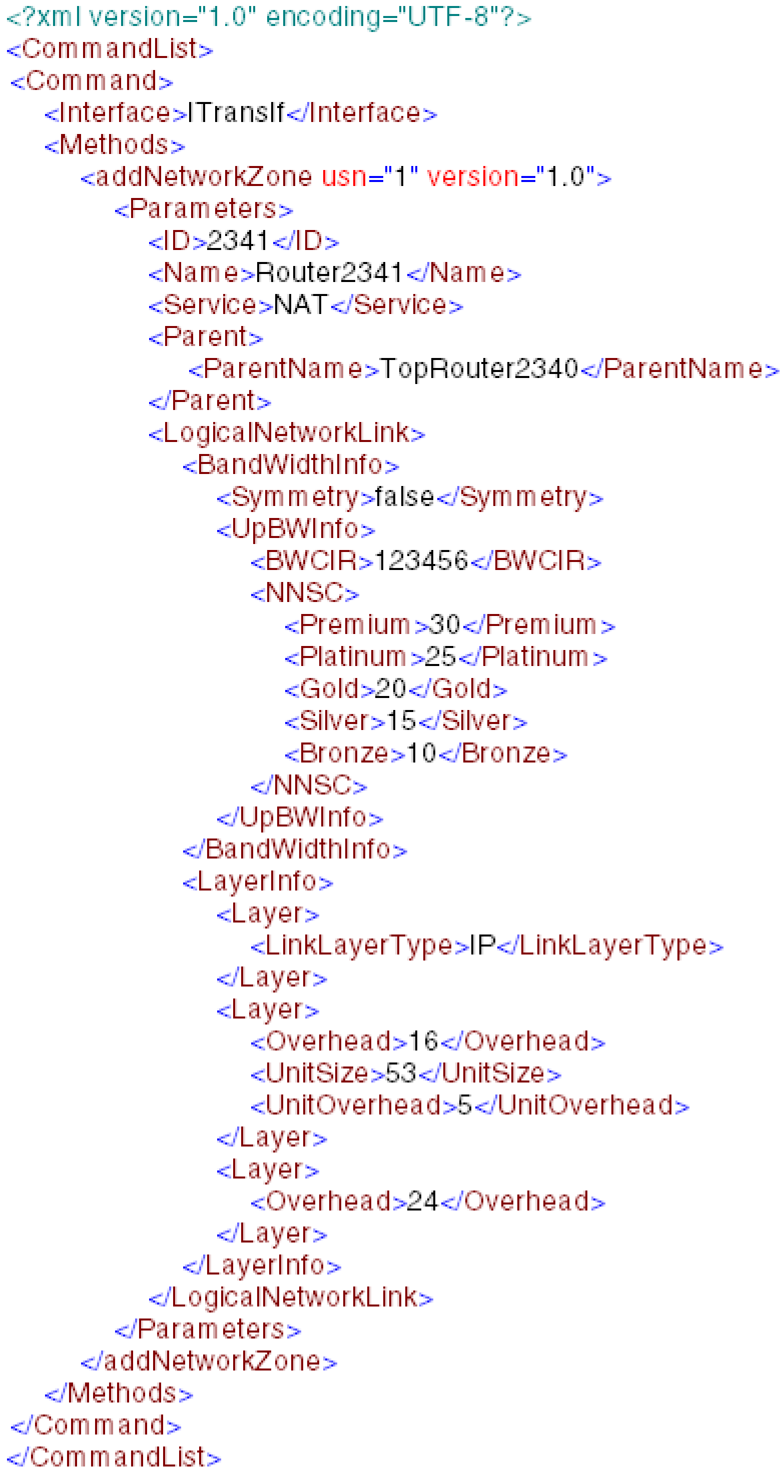
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList >
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addNetworkZone usn="1" version="1.0">
          <Parameters>
             <ID>2340</ID>
             <Name>TopRouter2340</Name>
             <Parent>
                <ParentID>0</ParentID>
             </Parent>
             <LogicalNetworkLink>
                <BandWidthInfo>
                   <Symmetry>false</Symmetry>
                   <UpBWInfo>
                      <BWCIR>123456</BWCIR>
                   </UpBWInfo>
                   <DownBWInfo>
                      <BWCIR>223456</BWCIR>
                   </DownBWInfo>
                </BandWidthInfo>
                <LayerInfo>
                   <Layer>
                      <LinkLayerType>IP</LinkLayerType>
                   </Layer>
                   <Layer>
                      <Overhead>34</Overhead>
                   </Layer>
                </LayerInfo>
             </LogicalNetworkLink>
          </Parameters>
       </addNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addNetworkZone** request that adds a non- root NAT NZ by specifying the <ParentID>:



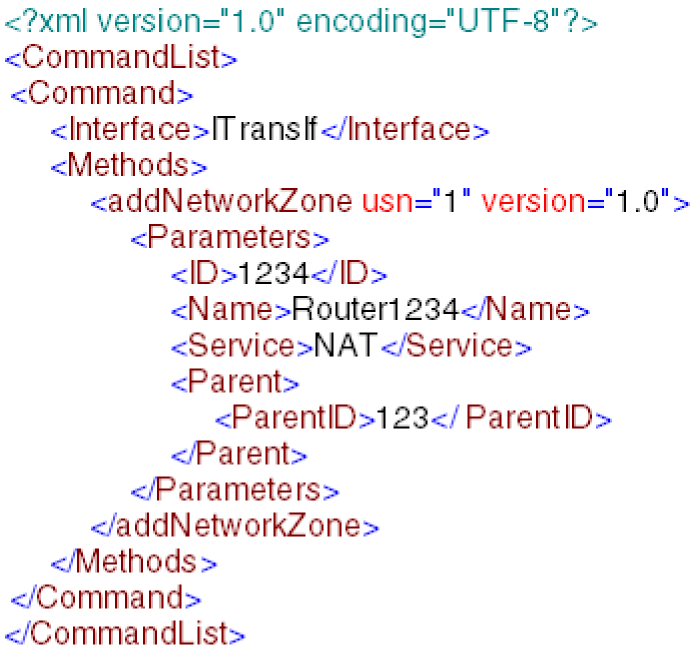
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <addNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1231</ID>
                 <Name>Router1231</Name>
                 <Service>NAT</Service>
                 <Parent>
                     < ParentID>1230</ ParentID>
                 </Parent>
             </Parameters>
         </addNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of an **addNetworkZone** request that adds a non- root NAT/LBL composite NZ by specifying the <ParentName>:



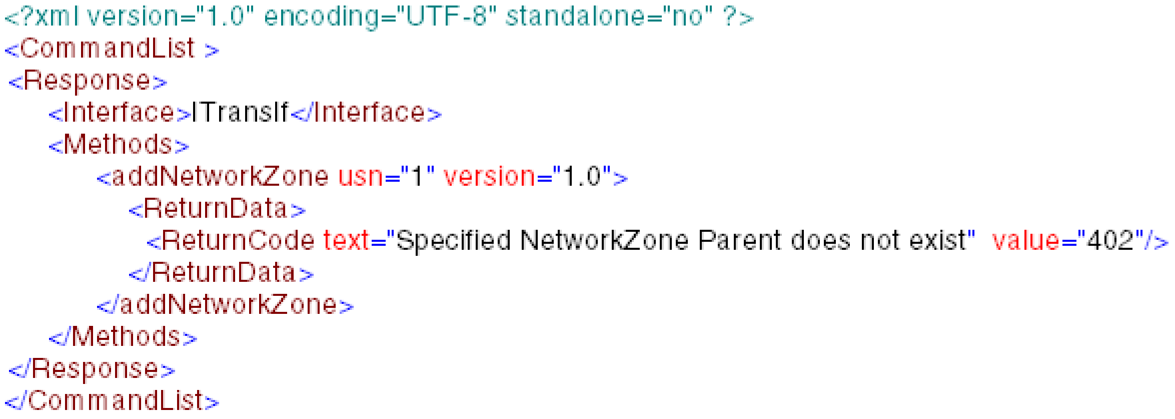
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
        <addNetworkZone usn="1" version="1.0">
            <Parameters>
                <ID>2341</ID>
                <Name>Router2341</Name>
                <Service>NAT</Service>
                <Parent>
                     <ParentName>TopRouter2340</ParentName>
                </Parent>
                <LogicalNetworkLink>
                    <BandWidthInfo>
                        <Symmetry>false</Symmetry>
                        <UpBWInfo>
                            <BWCIR>123456</BWCIR>
                            <NNSC>
                                <Premium>30</Premium>
                                <Platinum>25</Platinum>
                                <Gold>20</Gold>
                                <Silver>15</Silver>
                                <Bronze>10</Bronze>
                            </NNSC>
                        </UpBWInfo>
                    </BandWidthInfo>
                    <LayerInfo>
                        <Layer>
                            <LinkLayerType>IP</LinkLayerType>
                        </Layer>
                        <Layer>
                            <Overhead>16</Overhead>
                            <UnitSize>53</UnitSize>
                            <UnitOverhead>5</UnitOverhead>
                        </Layer>
                        <Layer>
                            <Overhead>24</Overhead>
                        </Layer>
                    </LayerInfo>
                </LogicalNetworkLink>
            </Parameters>
        </addNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addNetworkZone** request that causes a failure response - a nonexistent NetworkZone ID is used as a <ParentID>:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addNetworkZone usn="1" version="1.0">
          <Parameters>
             <ID>1234</ID>
             <Name>Router1234</Name>
             <Service>NAT</Service>
             <Parent>
                <ParentID>123</ ParentID>
             </Parent>
          </Parameters>
       </addNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addNetworkZone** failure response:



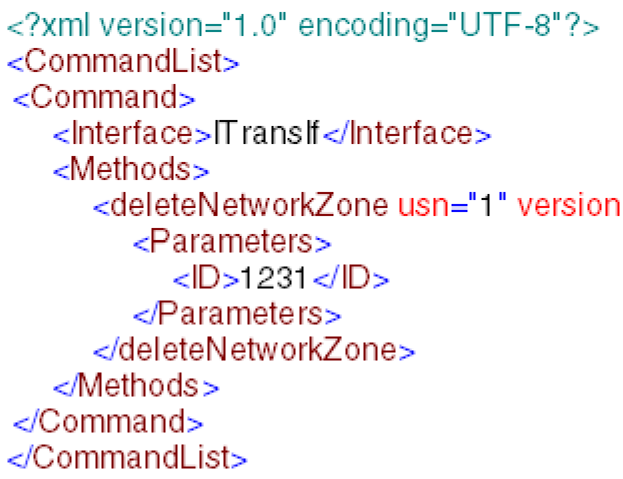
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <addNetworkZone usn="1" version="1.0">
          <ReturnData>
            <ReturnCode text="Specified NetworkZone Parent does not exist"  value="402"/>
          </ReturnData>
       </addNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

deleteNetworkZone

You can delete a NetworkZone without any child nodes by specifying the network zone ID or Name.

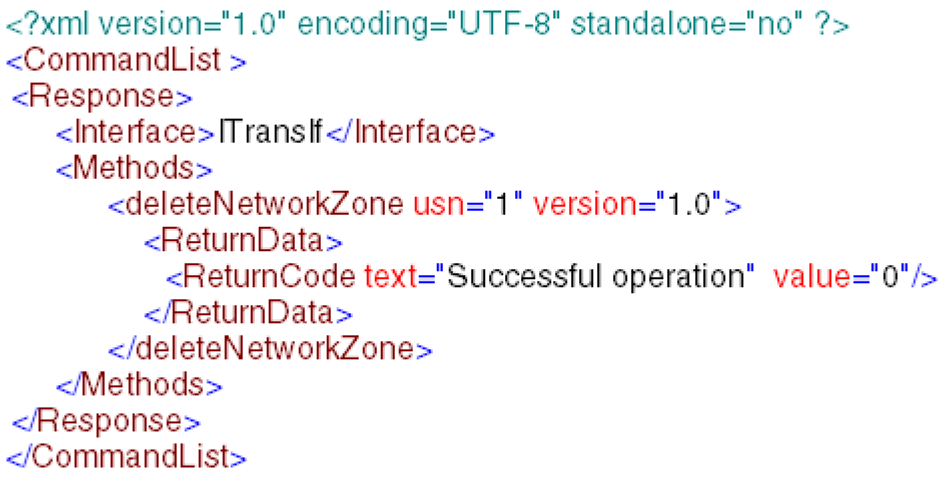
The Topology Manager will return an error message in XML when you try to delete a NetworkZone with child nodes.

An example of a **deleteNetworkZone** request that deletes a NetworkZone by specifying the ID:



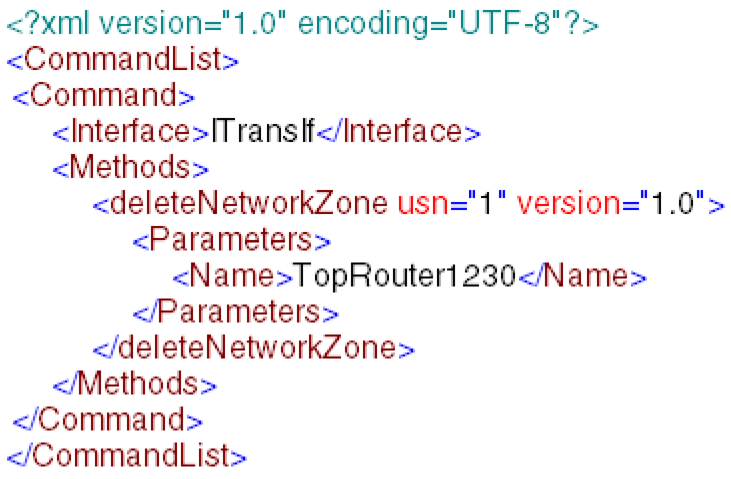
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <deleteNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1231</ID>
             </Parameters>
         </deleteNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of an **deleteNetworkZone** success response:



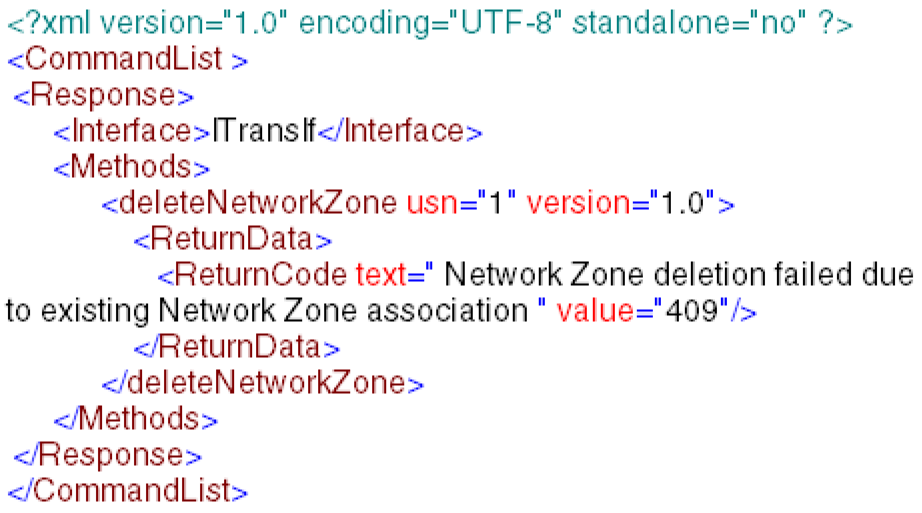
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
         <deleteNetworkZone usn="1" version="1.0">
             <ReturnData>
               <ReturnCode text="Successful operation"  value="0"/>
             </ReturnData>
         </deleteNetworkZone>
     </Methods>
 </Response>
</CommandList>
```

An example of a **deleteNetworkZone** request that deletes a NetworkZone by specifying the Name:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <deleteNetworkZone usn="1" version="1.0">
          <Parameters>
             <Name>TopRouter1230</Name>
          </Parameters>
       </deleteNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of a **deleteNetworkZone** failure response:



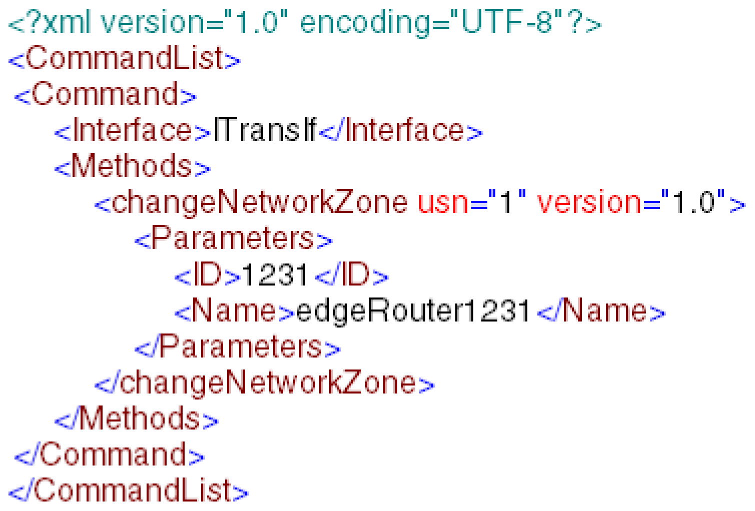
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <deleteNetworkZone usn="1" version="1.0">
          <ReturnData>
            <ReturnCode text=" Network Zone deletion failed due
to existing Network Zone association " value="409"/>
          </ReturnData>
       </deleteNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

changeNetworkZone

You cannot change the type of a NetworkZone. For example, you cannot change a NAT NetworkZone to an LBL NetworkZone or a NAT/LBL composite NetworkZone.

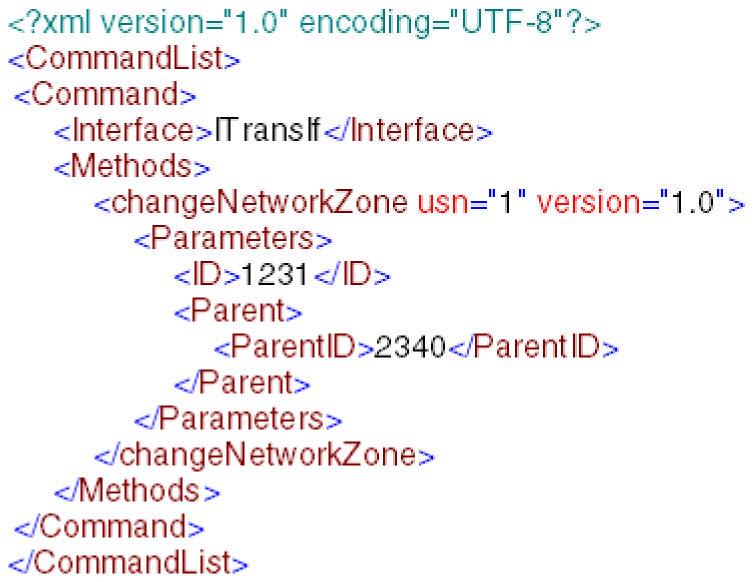
If the NetworkZone ID and Name are both provided in a **changeNetworkZone** request, the name of the NetworkZone identified by the ID will be changed to the value specified by <Name>.

An example of a **changeNetworkZone** request that changes the name of a NetworkZone:



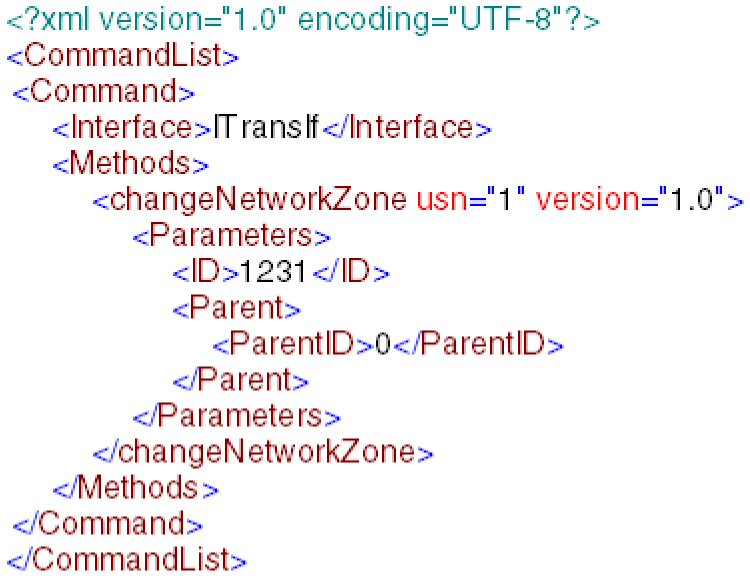
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1231</ID>
                 <Name>edgeRouter1231</Name>
             </Parameters>
         </changeNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** request that changes the parent of a NetworkZone:



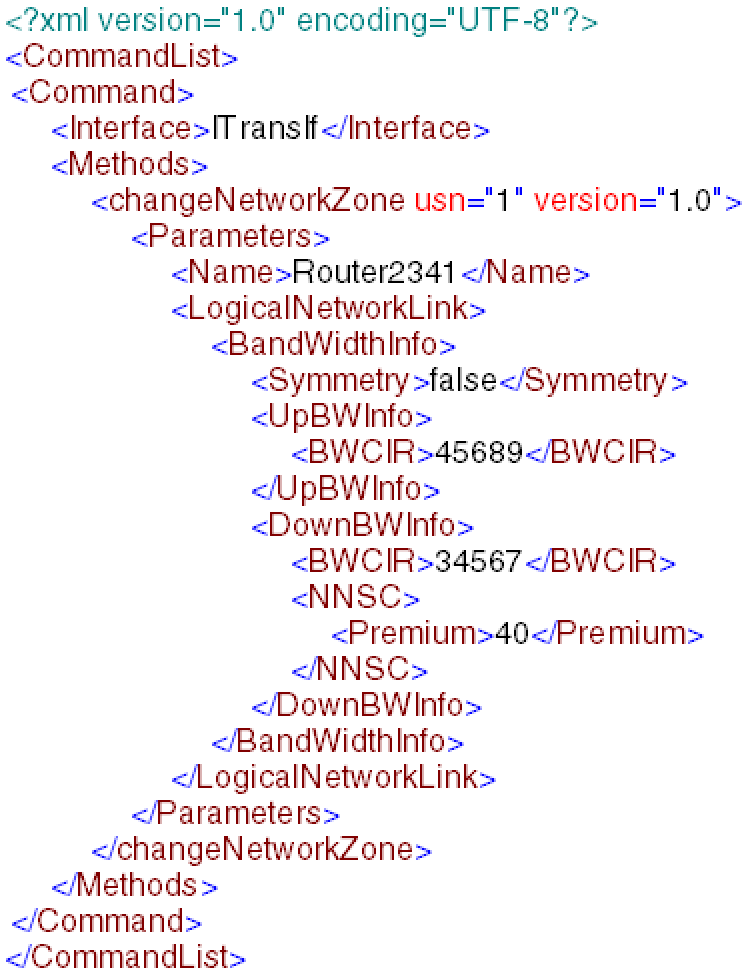
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1231</ID>
                 <Parent>
                     <ParentID>2340</ParentID>
                 </Parent>
             </Parameters>
         </changeNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** request that changes a non-root NetworkZone to a root one:



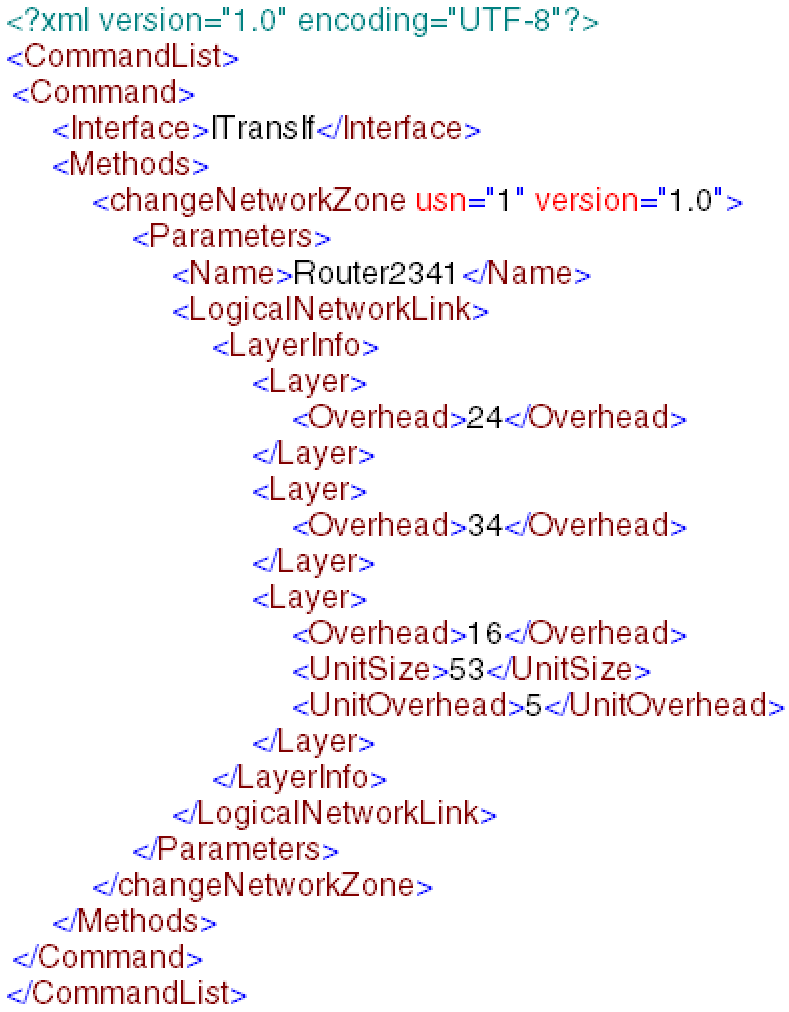
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1231</ID>
                 <Parent>
                     <ParentID>0</ParentID>
                 </Parent>
             </Parameters>
         </changeNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** request that changes the bandwidth of a NetworkZone:



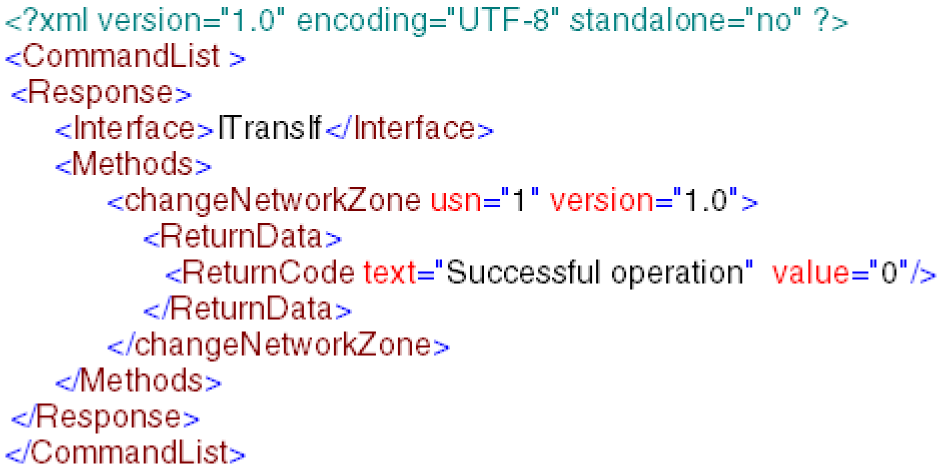
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeNetworkZone usn="1" version="1.0">
          <Parameters>
             <Name>Router2341</Name>
             <LogicalNetworkLink>
                <BandWidthInfo>
                   <Symmetry>false</Symmetry>
                   <UpBWInfo>
                      <BWCIR>45689</BWCIR>
                   </UpBWInfo>
                   <DownBWInfo>
                      <BWCIR>34567</BWCIR>
                      <NNSC>
                         <Premium>40</Premium>
                      </NNSC>
                   </DownBWInfo>
                </BandWidthInfo>
             </LogicalNetworkLink>
          </Parameters>
       </changeNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** request that changes the layer information of a NetworkZone:



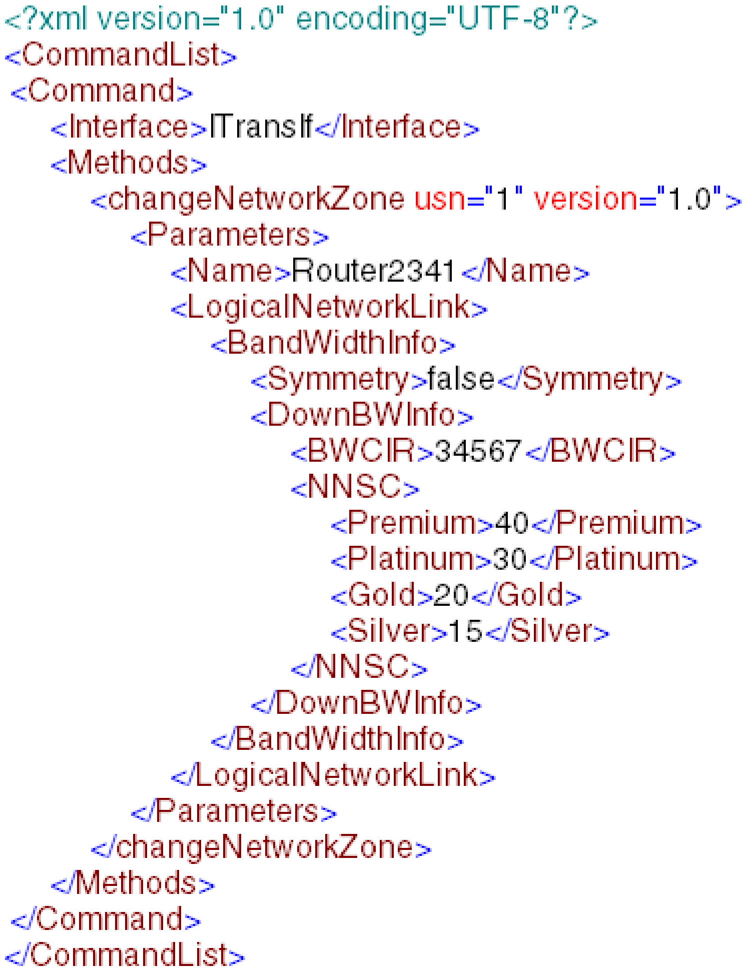
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeNetworkZone usn="1" version="1.0">
          <Parameters>
             <Name>Router2341</Name>
             <LogicalNetworkLink>
                <LayerInfo>
                   <Layer>
                      <Overhead>24</Overhead>
                   </Layer>
                   <Layer>
                      <Overhead>34</Overhead>
                   </Layer>
                   <Layer>
                      <Overhead>16</Overhead>
                      <UnitSize>53</UnitSize>
                      <UnitOverhead>5</UnitOverhead>
                   </Layer>
                </LayerInfo>
             </LogicalNetworkLink>
          </Parameters>
       </changeNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** success response:



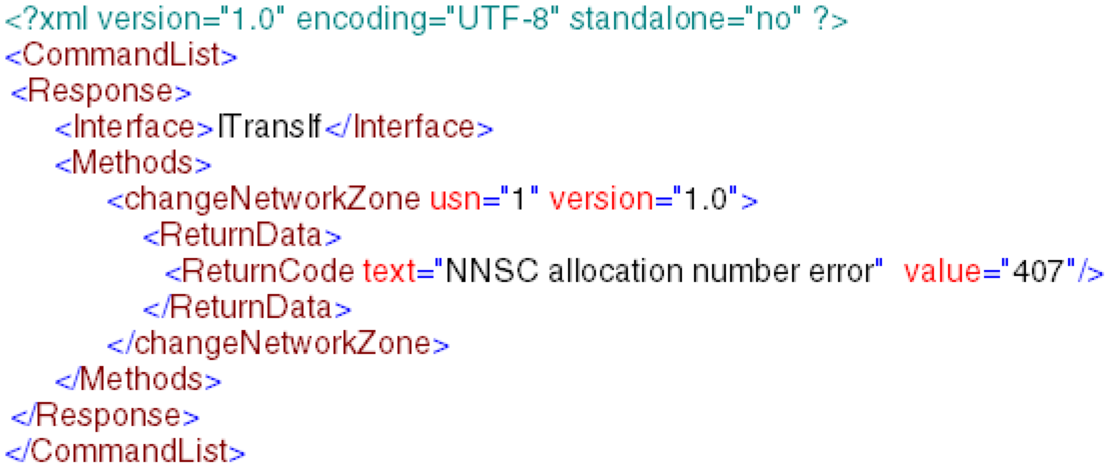
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <changeNetworkZone usn="1" version="1.0">
              <ReturnData>
                <ReturnCode text="Successful operation"  value="0"/>
              </ReturnData>
          </changeNetworkZone>
     </Methods>
 </Response>
</CommandList>
```

An example of a **changeNetworkZone** request that causes a failure response — all NNSC allocation numbers sum up to more than 100:



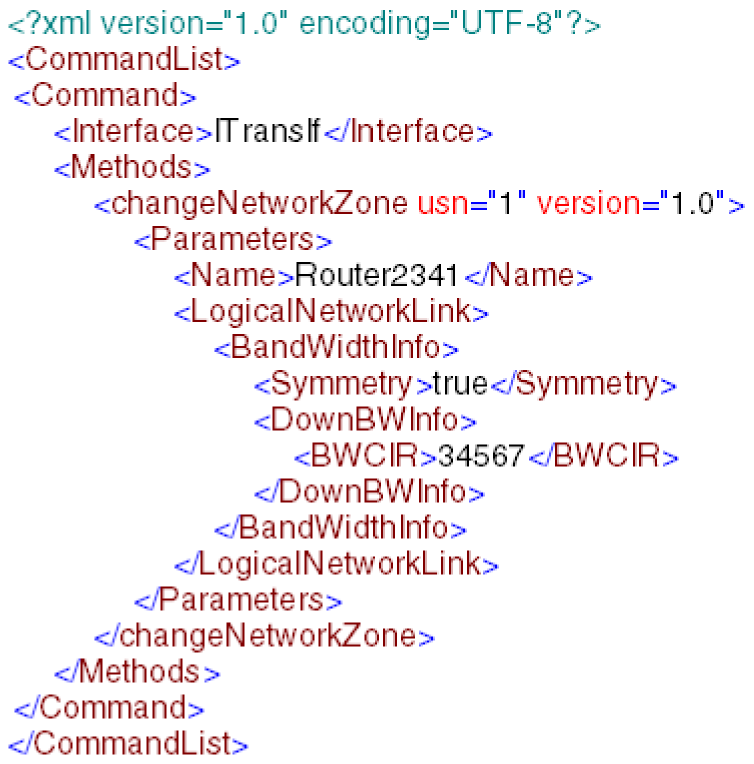
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeNetworkZone usn="1" version="1.0">
          <Parameters>
             <Name>Router2341</Name>
             <LogicalNetworkLink>
                <BandWidthInfo>
                   <Symmetry>false</Symmetry>
                   <DownBWInfo>
                      <BWCIR>34567</BWCIR>
                      <NNSC>
                         <Premium>40</Premium>
                         <Platinum>30</Platinum>
                         <Gold>20</Gold>
                         <Silver>15</Silver>
                      </NNSC>
                   </DownBWInfo>
                </BandWidthInfo>
             </LogicalNetworkLink>
          </Parameters>
       </changeNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of a **changeNetworkZone** failure response:



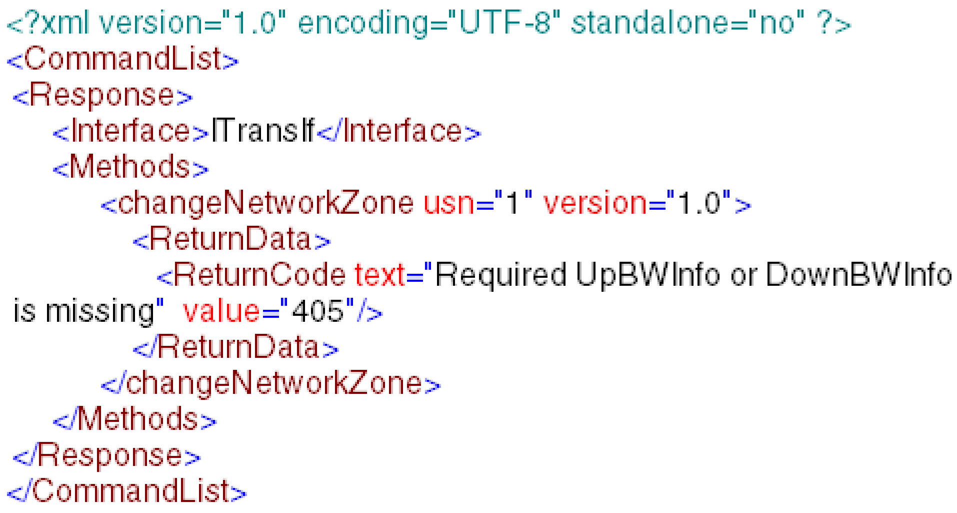
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeNetworkZone usn="1" version="1.0">
          <ReturnData>
           <ReturnCode text="NNSC allocation number error"  value="407"/>
          </ReturnData>
       </changeNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

An example of a **changeNetworkZone** request that causes a failure response — missing Up Bandwidth information with a symmetric LNL:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeNetworkZone usn="1" version="1.0">
             <Parameters>
                 <Name>Router2341</Name>
                 <LogicalNetworkLink>
                     <BandWidthInfo>
                         <Symmetry>true</Symmetry>
                         <DownBWInfo>
                             <BWCIR>34567</BWCIR>
                         </DownBWInfo>
                     </BandWidthInfo>
                 </LogicalNetworkLink>
             </Parameters>
         </changeNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example below of an **changeNetworkZone** failure response:



```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeNetworkZone usn="1" version="1.0">
            <ReturnData>
              <ReturnCode text="Required UpBWInfo or DownBWInfo
 is missing"  value="405"/>
            </ReturnData>
         </changeNetworkZone>
     </Methods>
 </Response>
</CommandList>
```

queryNetworkZone

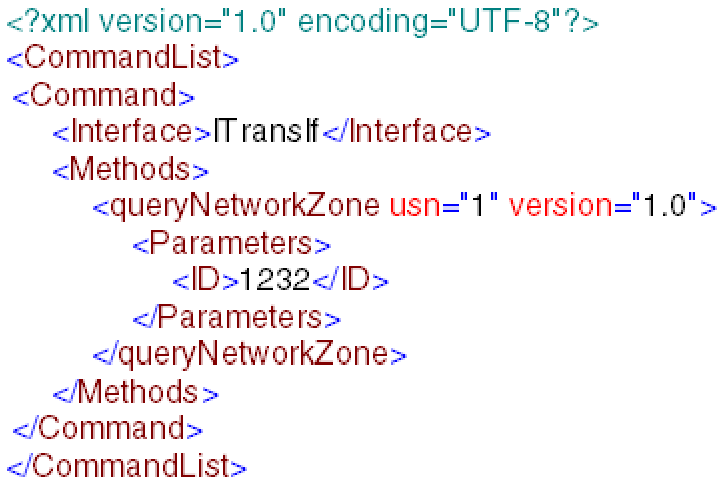
The **queryNetworkZone** command can retrieve detailed information about a NetworkZone as well as batch summary information about NetworkZones.

To retrieve detailed information about the NetworkZones, specify the ID or Name of the detailed information about NetworkZones

To retrieve detailed summary information about all NetworkZones, do not specify a parameter.

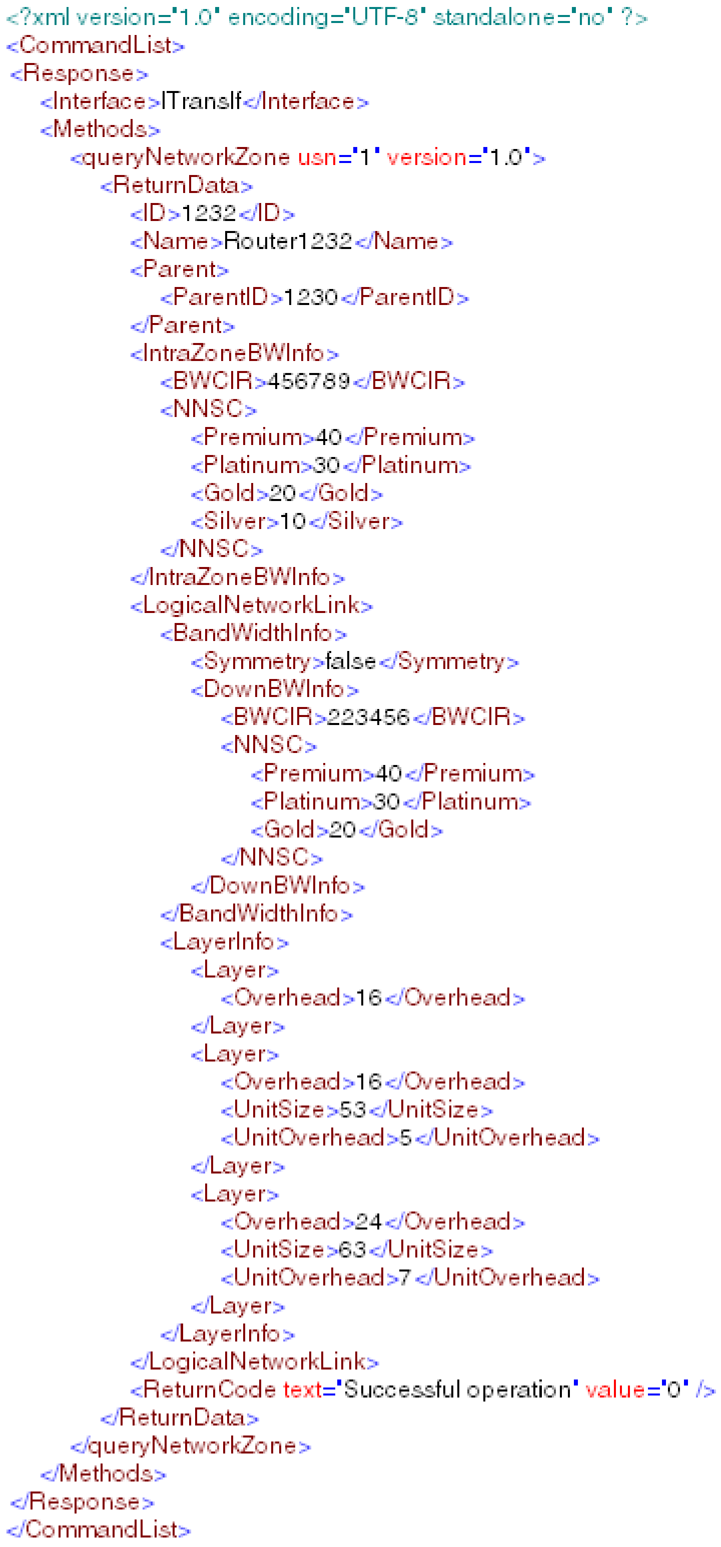
If the total number of NetworkZones exceeds 500, only the information about the first 500 NetworkZones, in ascending order by ID, can be returned at one time. You can use the IDMin and IDMax commands to retrieve information about other NetworkZones.

An example of a **queryNetworkZone** request that retrieves detailed information about a NetworkZone:



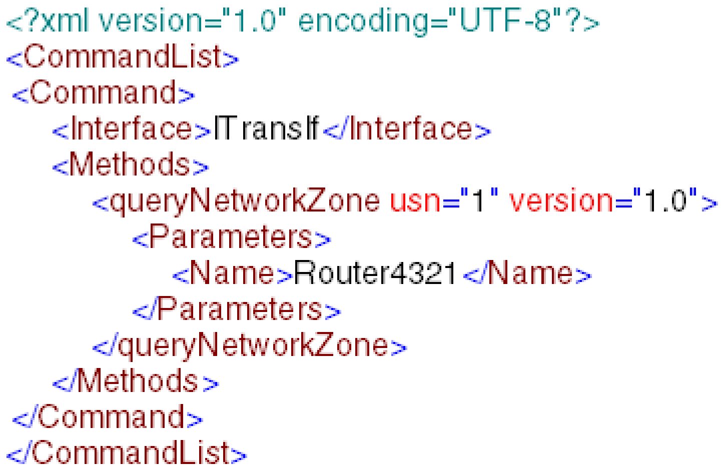
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryNetworkZone usn="1" version="1.0">
             <Parameters>
                 <ID>1232</ID>
             </Parameters>
         </queryNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **queryNetworkZone** success response:



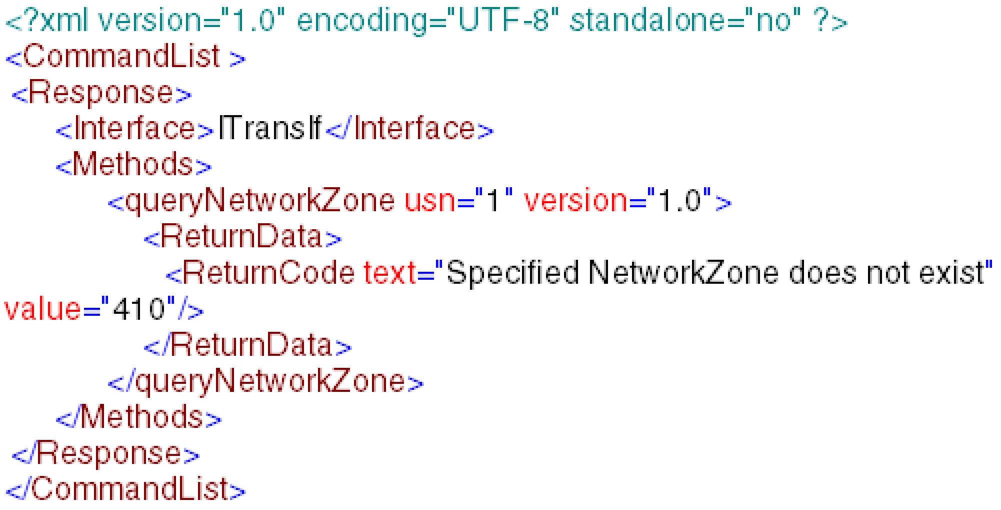
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <queryNetworkZone usn="1" version="1.0">
          <ReturnData>
             <ID>1232</ID>
             <Name>Router1232</Name>
             <Parent>
                <ParentID>1230</ParentID>
             </Parent>
             <IntraZoneBWInfo>
                <BWCIR>456789</BWCIR>
                <NNSC>
                   <Premium>40</Premium>
                   <Platinum>30</Platinum>
                   <Gold>20</Gold>
                   <Silver>10</Silver>
                </NNSC>
             </IntraZoneBWInfo>
             <LogicalNetworkLink>
                <BandWidthInfo>
                   <Symmetry>false</Symmetry>
                   <DownBWInfo>
                      <BWCIR>223456</BWCIR>
                      <NNSC>
                         <Premium>40</Premium>
                         <Platinum>30</Platinum>
                         <Gold>20</Gold>
                      </NNSC>
                   </DownBWInfo>
                </BandWidthInfo>
                <LayerInfo>
                   <Layer>
                      <Overhead>16</Overhead>
                   </Layer>
                   <Layer>
                      <Overhead>16</Overhead>
                      <UnitSize>53</UnitSize>
                      <UnitOverhead>5</UnitOverhead>
                   </Layer>
                   <Layer>
                      <Overhead>24</Overhead>
                      <UnitSize>63</UnitSize>
                      <UnitOverhead>7</UnitOverhead>
                   </Layer>
                </LayerInfo>
             </LogicalNetworkLink>
             <ReturnCode text="Successful operation" value="0" />
          </ReturnData>
       </queryNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

An example of a **queryNetworkZone** that causes a failure response - the specified NetworkZone does not exist:



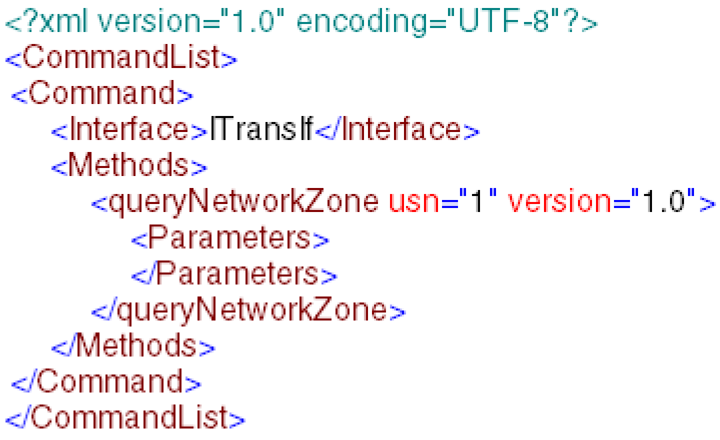
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
      <Interface>ITransIf</Interface>
      <Methods>
           <queryNetworkZone usn="1" version="1.0">
                <Parameters>
                     <Name>Router4321</Name>
                </Parameters>
           </queryNetworkZone>
      </Methods>
 </Command>
</CommandList>
```

An example of a **queryNetworkZone** failure response:



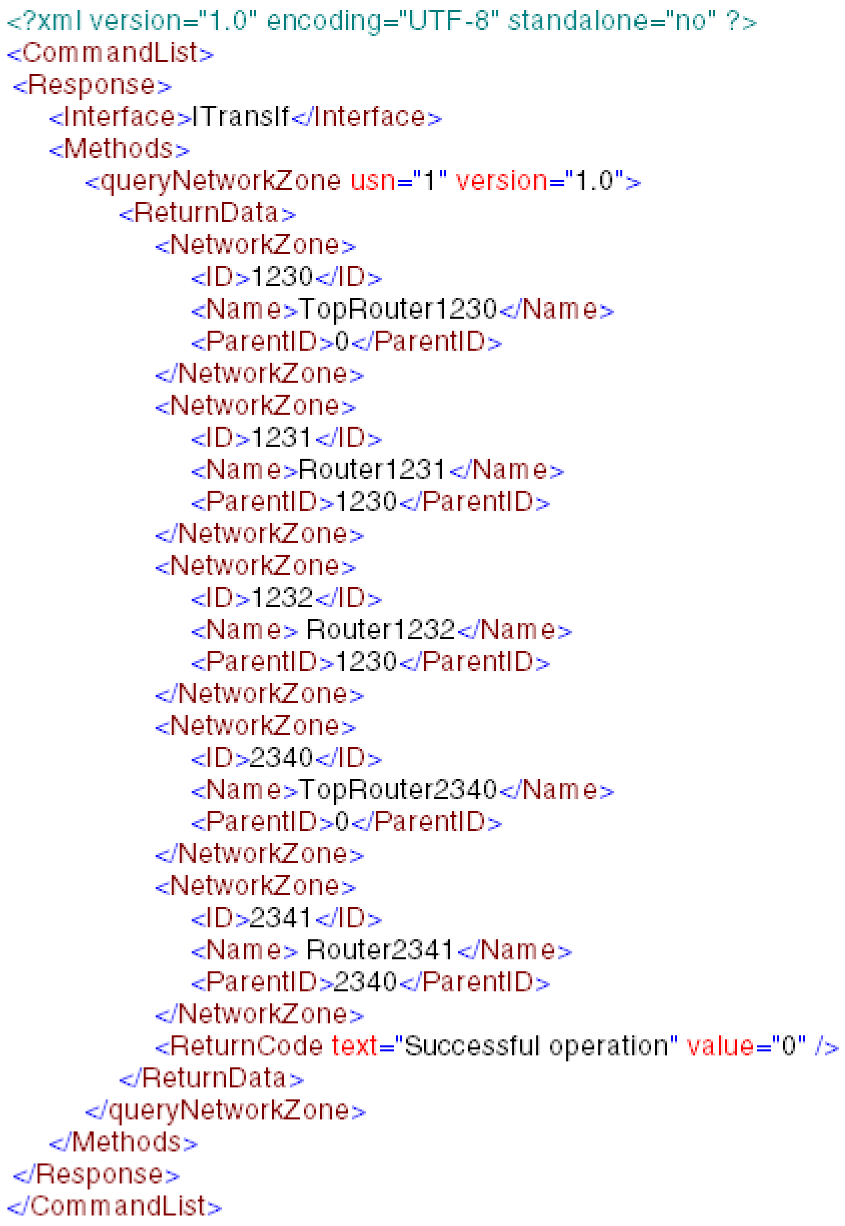
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
      <Interface>ITransIf</Interface>
      <Methods>
           <queryNetworkZone usn="1" version="1.0">
                <ReturnData>
                   <ReturnCode text="Specified NetworkZone does not exist"
value="410"/>
                </ReturnData>
           </queryNetworkZone>
      </Methods>
 </Response>
</CommandList>
```

An example of a **queryNetworkZone** request that retrieves summary information for all NetworkZones:



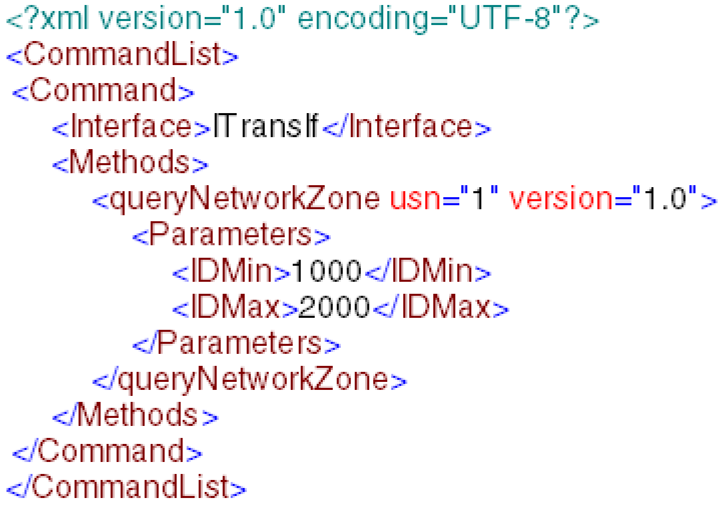
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryNetworkZone usn="1" version="1.0">
             <Parameters>
             </Parameters>
         </queryNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **queryNetworkZone** success response:



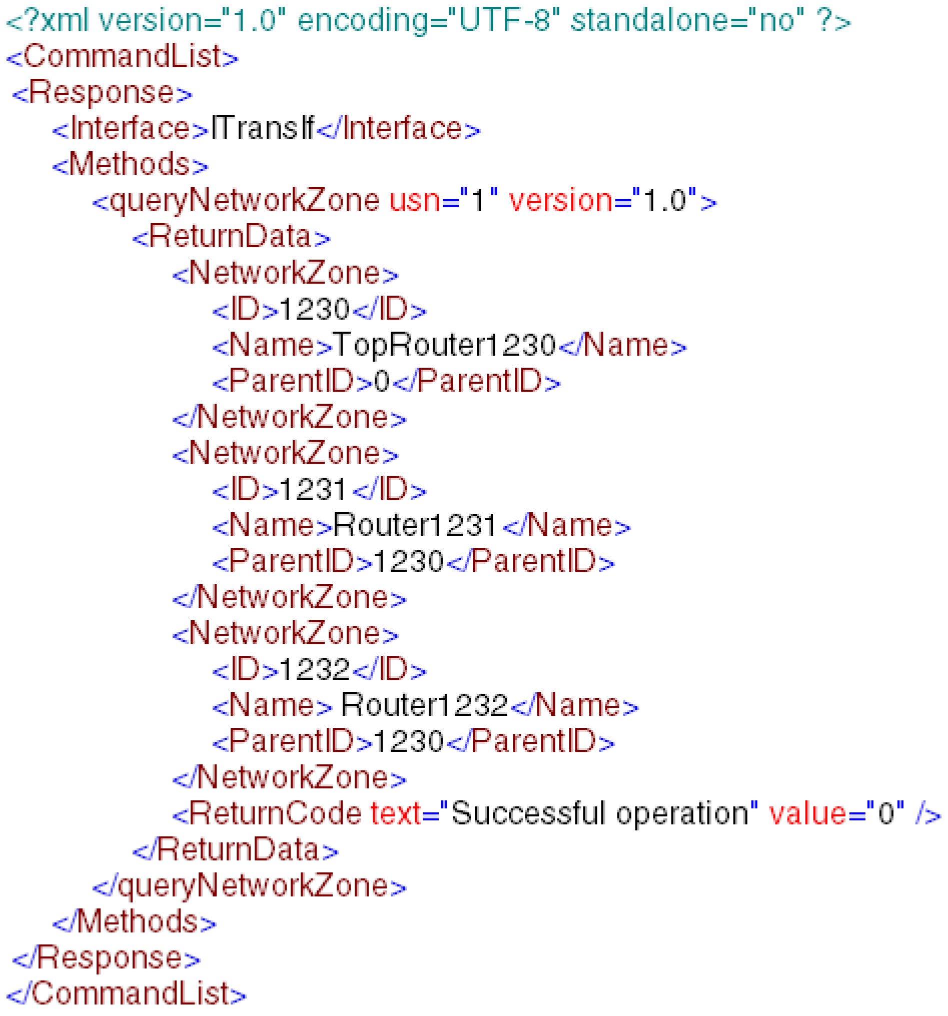
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryNetworkZone usn="1" version="1.0">
             <ReturnData>
                 <NetworkZone>
                     <ID>1230</ID>
                     <Name>TopRouter1230</Name>
                     <ParentID>0</ParentID>
                 </NetworkZone>
                 <NetworkZone>
                     <ID>1231</ID>
                     <Name>Router1231</Name>
                     <ParentID>1230</ParentID>
                 </NetworkZone>
                 <NetworkZone>
                     <ID>1232</ID>
                     <Name> Router1232</Name>
                     <ParentID>1230</ParentID>
                 </NetworkZone>
                 <NetworkZone>
                     <ID>2340</ID>
                     <Name>TopRouter2340</Name>
                     <ParentID>0</ParentID>
                 </NetworkZone>
                 <NetworkZone>
                     <ID>2341</ID>
                     <Name> Router2341</Name>
                     <ParentID>2340</ParentID>
                 </NetworkZone>
                 <ReturnCode text="Successful operation" value="0" />
             </ReturnData>
         </queryNetworkZone>
     </Methods>
 </Response>
</CommandList>
```

An example of a **queryNetworkZone** request that retrieves the NetworkZones with IDs between 1000 and 2000:



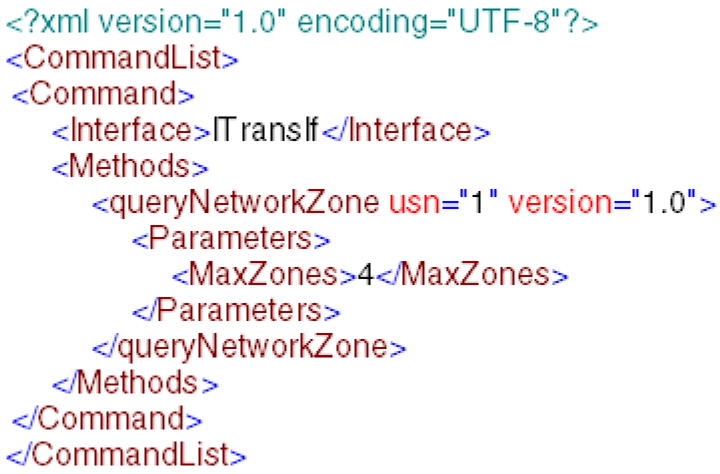
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <queryNetworkZone usn="1" version="1.0">
          <Parameters>
             <IDMin>1000</IDMin>
             <IDMax>2000</IDMax>
          </Parameters>
       </queryNetworkZone>
    </Methods>
 </Command>
</CommandList>
```

An example of a **queryNetworkZone** success response:



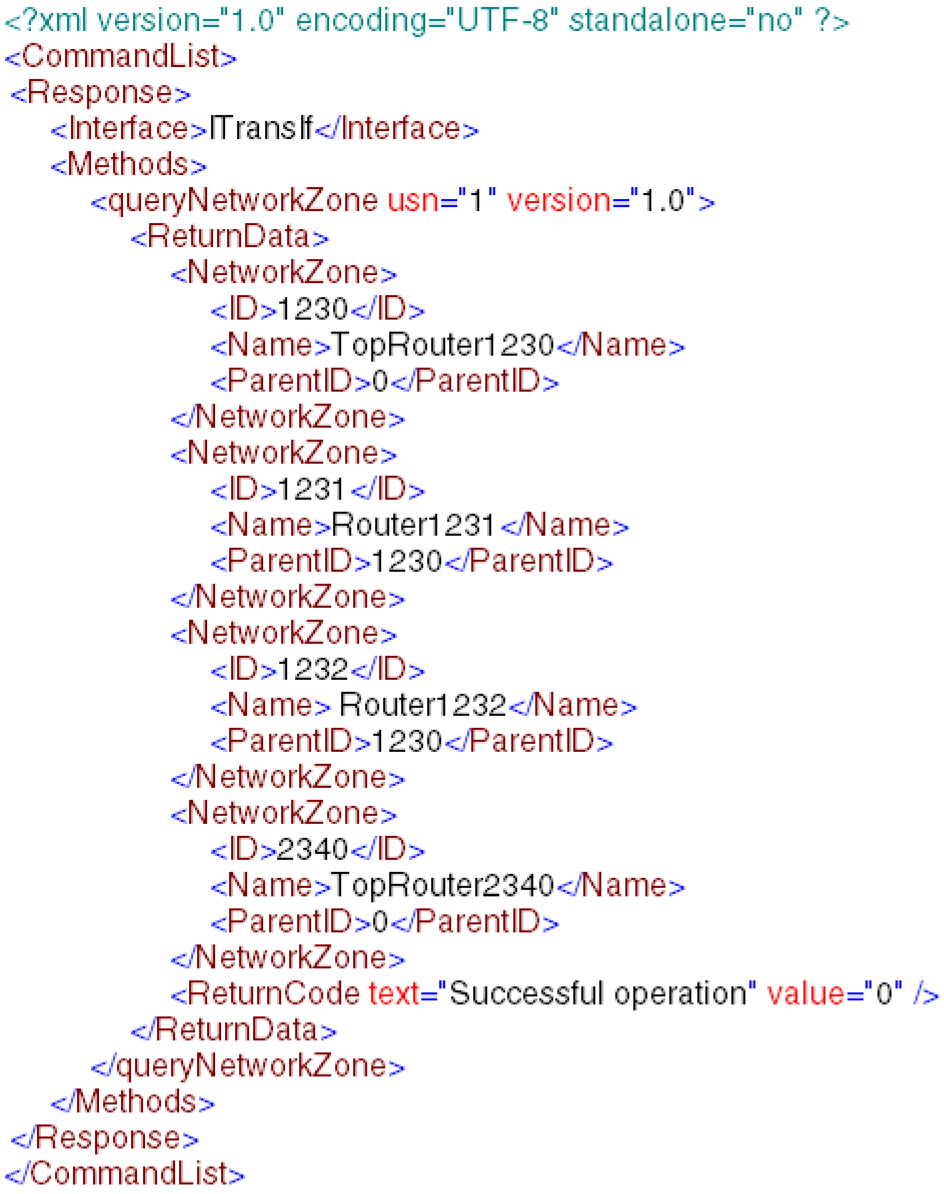
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
        <queryNetworkZone usn="1" version="1.0">
            <ReturnData>
                <NetworkZone>
                    <ID>1230</ID>
                    <Name>TopRouter1230</Name>
                    <ParentID>0</ParentID>
                </NetworkZone>
                <NetworkZone>
                    <ID>1231</ID>
                    <Name>Router1231</Name>
                    <ParentID>1230</ParentID>
                </NetworkZone>
                <NetworkZone>
                    <ID>1232</ID>
                    <Name> Router1232</Name>
                    <ParentID>1230</ParentID>
                </NetworkZone>
                <ReturnCode text="Successful operation" value="0" />
            </ReturnData>
        </queryNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

An example of a **queryNetworkZone** that retrieves a specified number of NetworkZones:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryNetworkZone usn="1" version="1.0">
             <Parameters>
                 <MaxZones>4</MaxZones>
             </Parameters>
         </queryNetworkZone>
     </Methods>
 </Command>
</CommandList>
```

An example of a **queryNetworkZone** success response:



```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <queryNetworkZone usn="1" version="1.0">
          <ReturnData>
             <NetworkZone>
                <ID>1230</ID>
                <Name>TopRouter1230</Name>
                <ParentID>0</ParentID>
             </NetworkZone>
             <NetworkZone>
                <ID>1231</ID>
                <Name>Router1231</Name>
                <ParentID>1230</ParentID>
             </NetworkZone>
             <NetworkZone>
                <ID>1232</ID>
                <Name> Router1232</Name>
                <ParentID>1230</ParentID>
             </NetworkZone>
             <NetworkZone>
                <ID>2340</ID>
                <Name>TopRouter2340</Name>
                <ParentID>0</ParentID>
             </NetworkZone>
             <ReturnCode text="Successful operation" value="0" />
          </ReturnData>
       </queryNetworkZone>
    </Methods>
 </Response>
</CommandList>
```

XML LinkLayer commands

Provisioning LinkLayerTypes

Provision a LinkLayerType according to the following rules:

- A valid Link Layer Type name follows the DNS convention and the following rules:
  - — Name can not start with a "." or "-"
  - — Name can not end with a "." or "-"
  - — Consecutive ".." are not supported.
- The Link Layer Type name is case insensitive.
- The maximum number of LinkLayerTypes supported is 500.
- A valid <Overhead> value is in the range 0 to 1000000.
- A valid <UnitSize> value is in the range 1 to 1000000.
- A valid <UnitOverhead> value is in the range 0 to 1000000.
- The <UnitSize> value has to be larger than the <UnitOverhead> value.

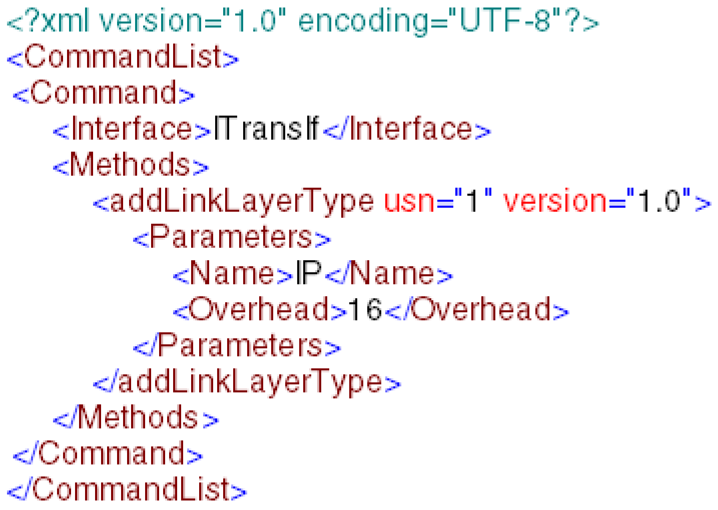
AddLinkLayerType

Two types of LinkLayerTypes are supported: variable PDU and fixed PDU.

To add a variable PDU LinkLayerType, only the <Overhead> attribute needs to be specified.

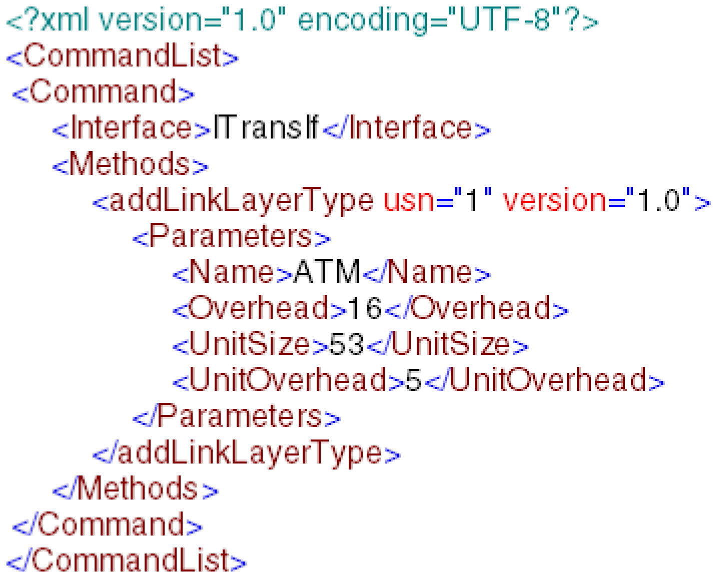
To add a fixed PDU LinkLayerType, the <Overhead>, <UnitSize> and <UnitOverhead> attributes need to be specified.

An example of an **addLinkLayerType** request that adds a variable PDU LinkLayerType:



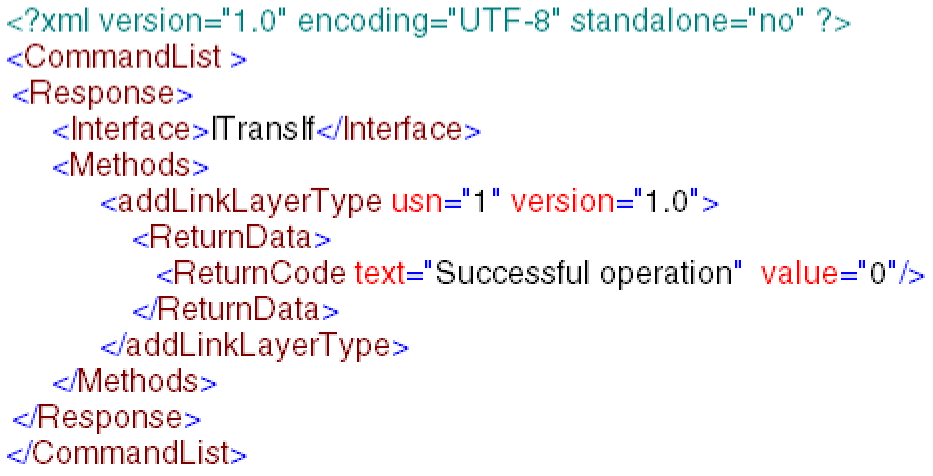
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addLinkLayerType usn="1" version="1.0">
          <Parameters>
             <Name>IP</Name>
             <Overhead>16</Overhead>
          </Parameters>
       </addLinkLayerType>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addLinkLayerType** request that adds a fixed PDU LinkLayerType:



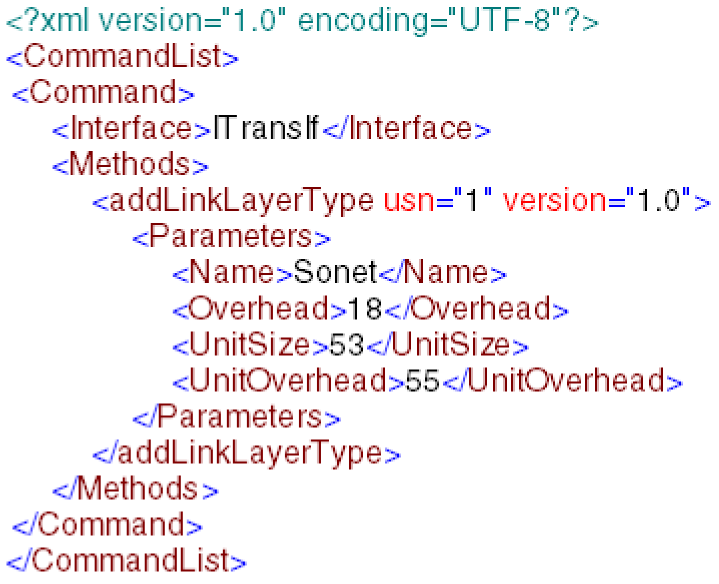
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addLinkLayerType usn="1" version="1.0">
          <Parameters>
             <Name>ATM</Name>
             <Overhead>16</Overhead>
             <UnitSize>53</UnitSize>
             <UnitOverhead>5</UnitOverhead>
          </Parameters>
       </addLinkLayerType>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addLinkLayerType** success response:



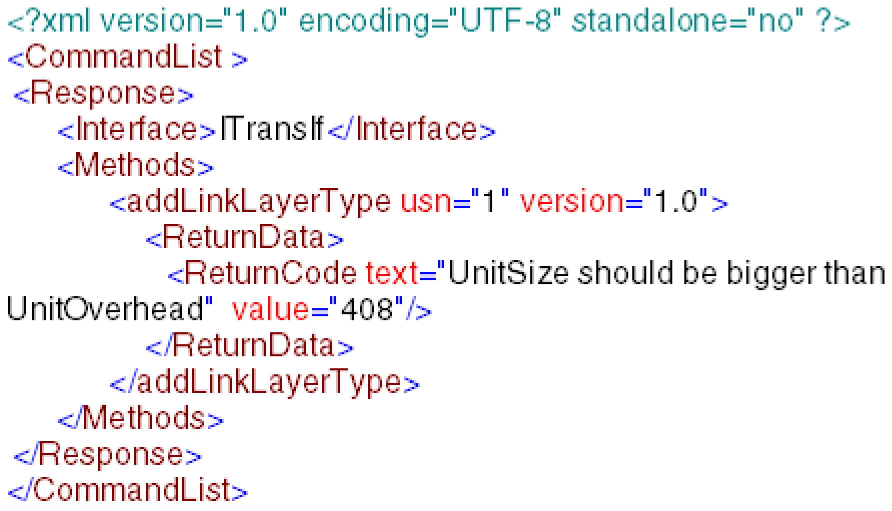
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
        <addLinkLayerType usn="1" version="1.0">
           <ReturnData>
             <ReturnCode text="Successful operation"  value="0"/>
           </ReturnData>
        </addLinkLayerType>
    </Methods>
 </Response>
</CommandList>
```

An example of an **addLinkLayerType** request that causes a failure response - the UnitSize is less than the UnitOverhead:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <addLinkLayerType usn="1" version="1.0">
          <Parameters>
             <Name>Sonet</Name>
             <Overhead>18</Overhead>
             <UnitSize>53</UnitSize>
             <UnitOverhead>55</UnitOverhead>
          </Parameters>
       </addLinkLayerType>
    </Methods>
 </Command>
</CommandList>
```

An example of an **addLinkLayerType** failure response:



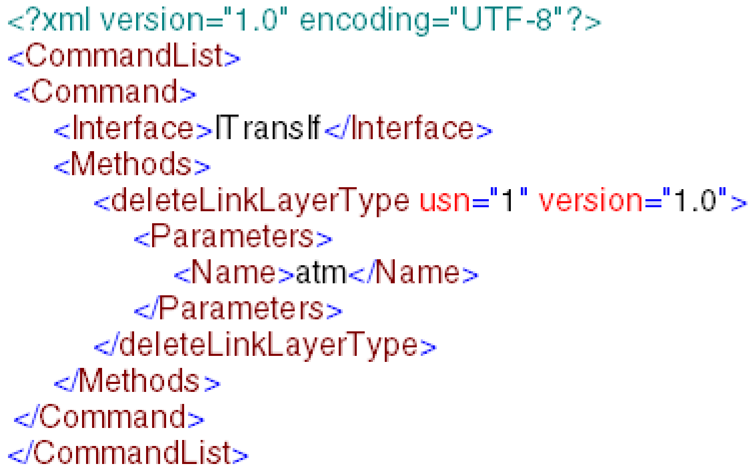
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <addLinkLayerType usn="1" version="1.0">
              <ReturnData>
                <ReturnCode text="UnitSize should be bigger than
UnitOverhead"  value="408"/>
              </ReturnData>
          </addLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

deleteLinkLayerType

You can delete a LinkLayerType that is not in use by any NetworkZones.

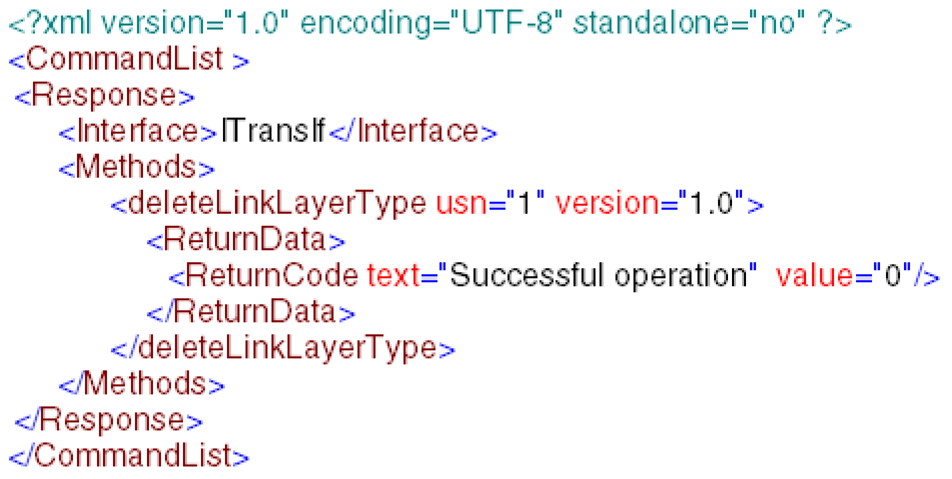
You cannot delete a LinkLayerType that is in use by some NetworkZones. The Topology Manager will return an XML error message in XML when you try to delete a LinkLayerType that is in use by some NetworkZones.

An example of a **deleteLinkLayerType** request:



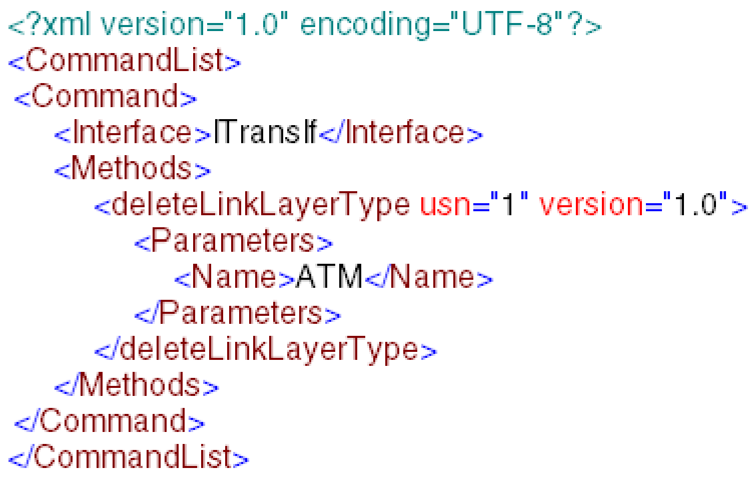
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <deleteLinkLayerType usn="1" version="1.0">
             <Parameters>
                 <Name>atm</Name>
             </Parameters>
         </deleteLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **deleteLinkLayerType** success response:



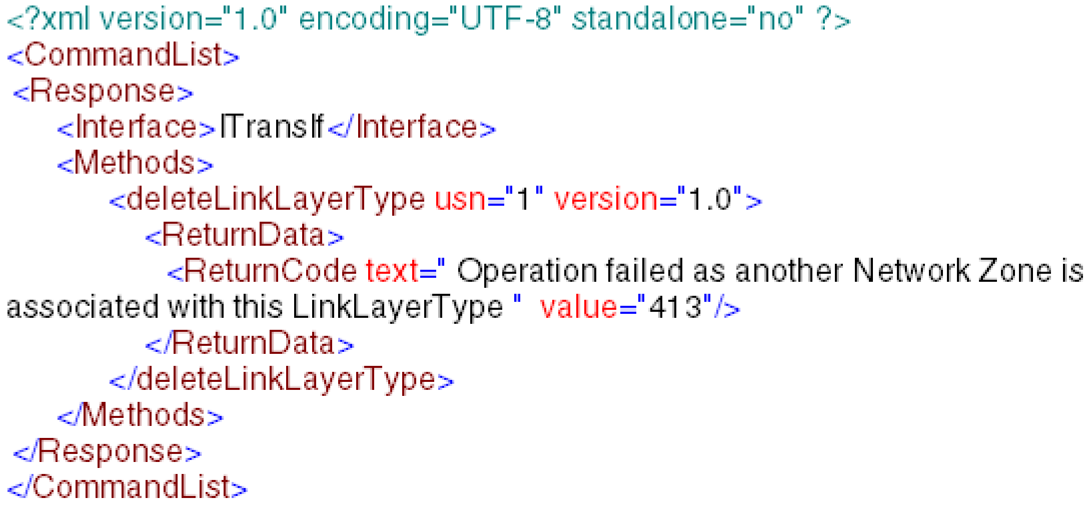
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
         <deleteLinkLayerType usn="1" version="1.0">
            <ReturnData>
              <ReturnCode text="Successful operation"  value="0"/>
            </ReturnData>
         </deleteLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

An example of a **deleteLinkLayerType** that causes a failure response - the LinkLayerType to be deleted is in use by some NetworkZones:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <deleteLinkLayerType usn="1" version="1.0">
            <Parameters>
               <Name>ATM</Name>
            </Parameters>
         </deleteLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **deleteLinkLayerType** failure response:



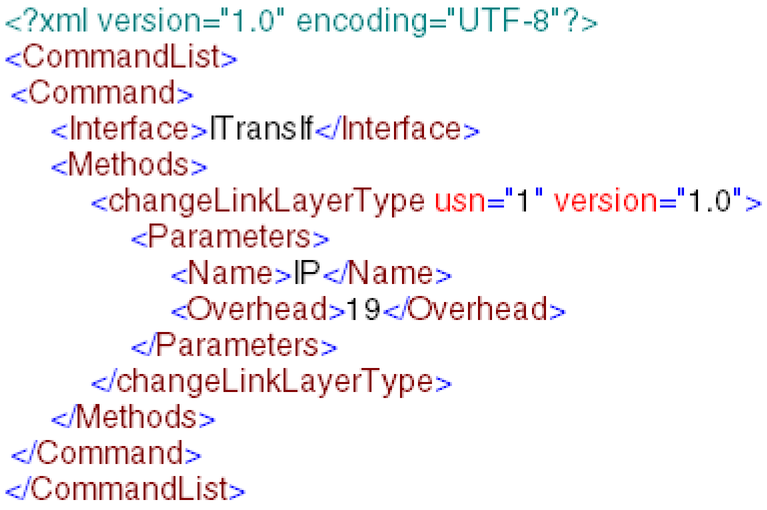
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <deleteLinkLayerType usn="1" version="1.0">
             <ReturnData>
               <ReturnCode text=" Operation failed as another Network Zone is
associated with this LinkLayerType "  value="413"/>
             </ReturnData>
          </deleteLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

changeLinkLayerType

You can change a LinkLayerType that is not in use by any NetworkZones.

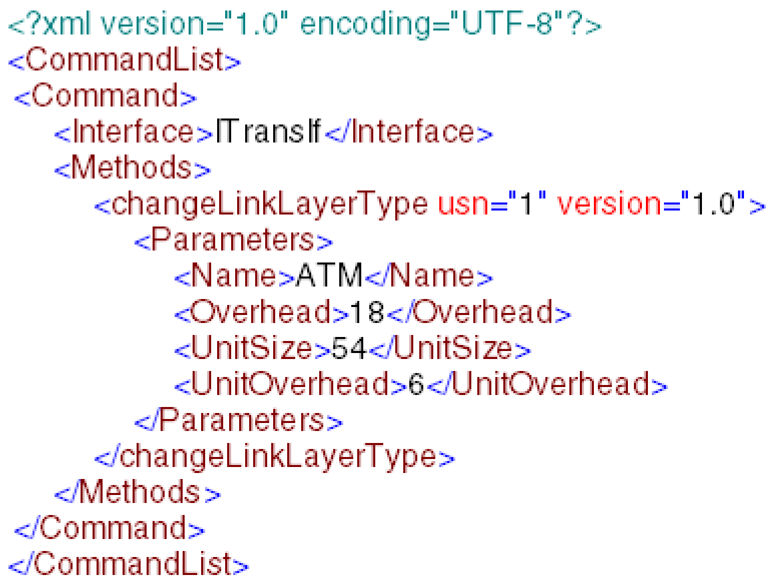
You cannot change a LinkLayerType that is in use by some NetworkZones. The Topology Manager will return an XML error message in XML when you try to change a LinkLayerType that is in use by some NetworkZones.

An example of a **changeLinkLayerType** request that changes a variable PDU LinkLayerType:



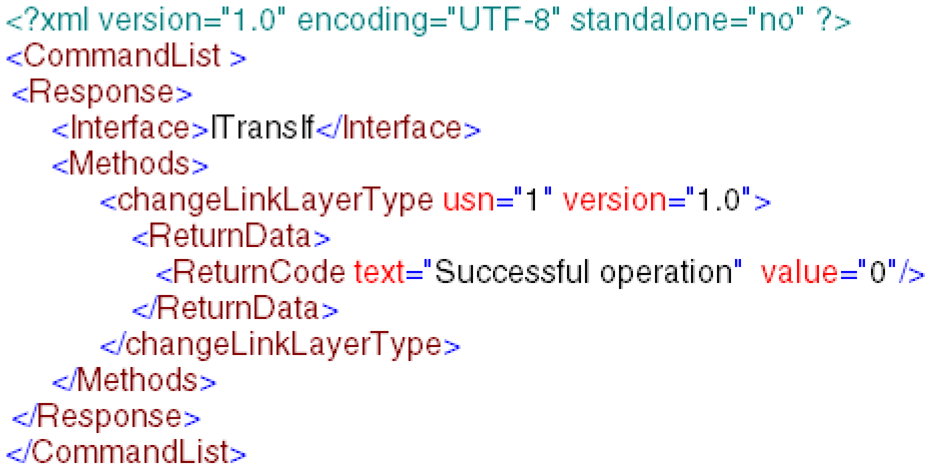
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeLinkLayerType usn="1" version="1.0">
             <Parameters>
                 <Name>IP</Name>
                 <Overhead>19</Overhead>
             </Parameters>
         </changeLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **changeLinkLayerType** request that changes a fixed PDU LinkLayerType:



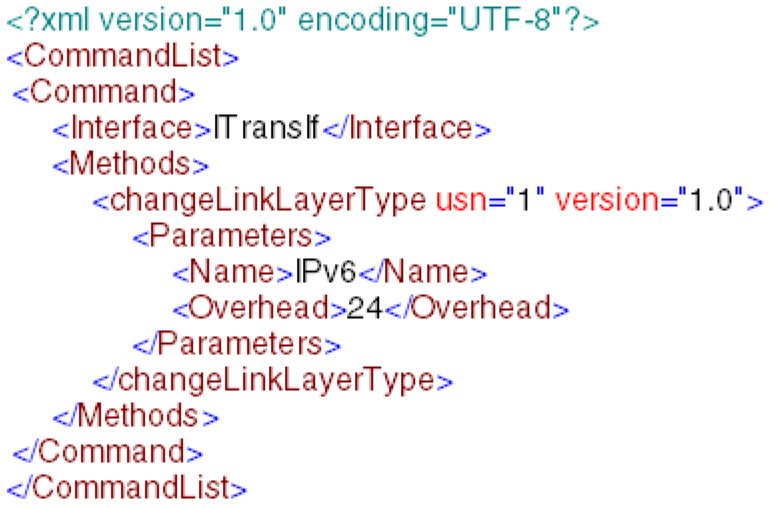
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeLinkLayerType usn="1" version="1.0">
          <Parameters>
             <Name>ATM</Name>
             <Overhead>18</Overhead>
             <UnitSize>54</UnitSize>
             <UnitOverhead>6</UnitOverhead>
          </Parameters>
       </changeLinkLayerType>
    </Methods>
 </Command>
</CommandList>
```

An example of a **changeLinkLayerType** success response:



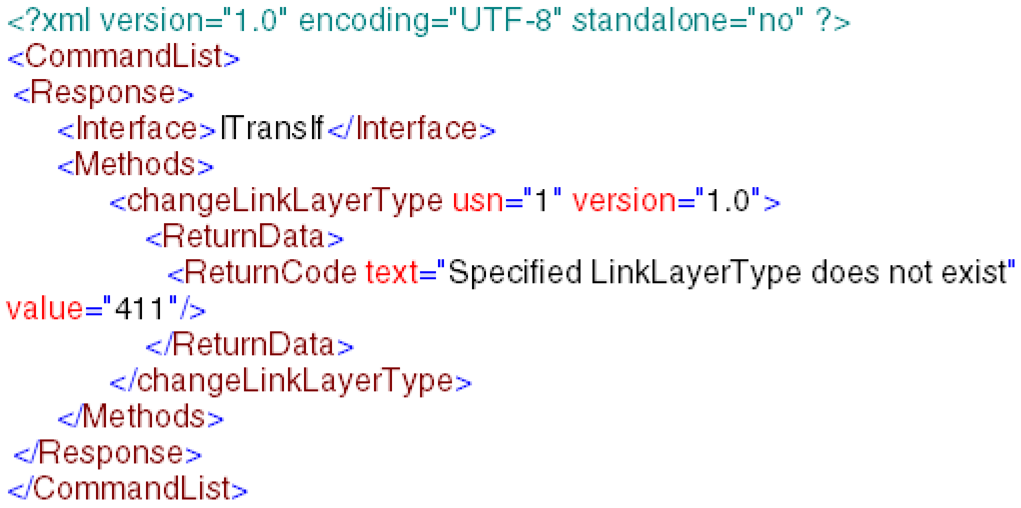
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
       <changeLinkLayerType usn="1" version="1.0">
         <ReturnData>
           <ReturnCode text="Successful operation"  value="0"/>
         </ReturnData>
       </changeLinkLayerType>
    </Methods>
 </Response>
</CommandList>
```

An example of a **changeLinkLayerType** that causes a failure response - the LinkLayerType to be changed does not exist:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <changeLinkLayerType usn="1" version="1.0">
             <Parameters>
                 <Name>IPv6</Name>
                 <Overhead>24</Overhead>
             </Parameters>
         </changeLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **changeLinkLayerType** failure response:



```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <changeLinkLayerType usn="1" version="1.0">
              <ReturnData>
                <ReturnCode text="Specified LinkLayerType does not exist"
value="411"/>
              </ReturnData>
          </changeLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

queryLinkLayerType

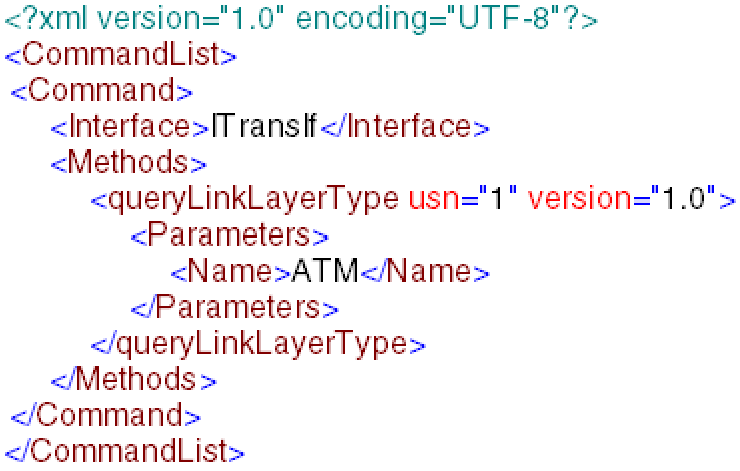
The **queryLinkLayerType** command can retrieve detailed information about a LinkLayerType and a batch of LinkLayerType names.

You can retrieve detailed information about a LinkLayerType by specifying the <Name>.

You can retrieve names of LinkLayerTypes if no parameter is specified.

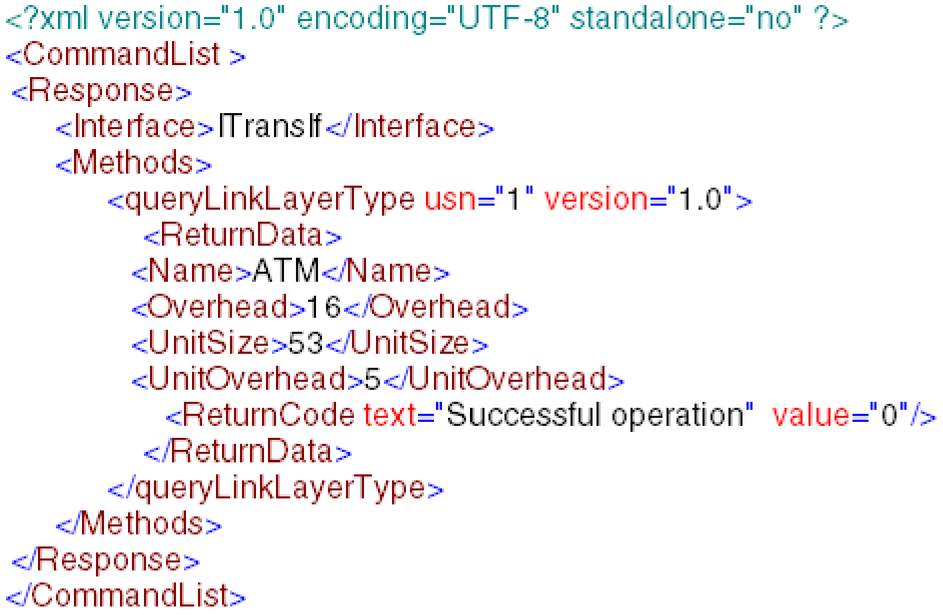
You can specify the number of LinkLayerTypes returned at a time by using the <MaxTypes> attribute.

An example of a **queryLinkLayerType** request that retrieves the detailed information of a LinkLayerType:



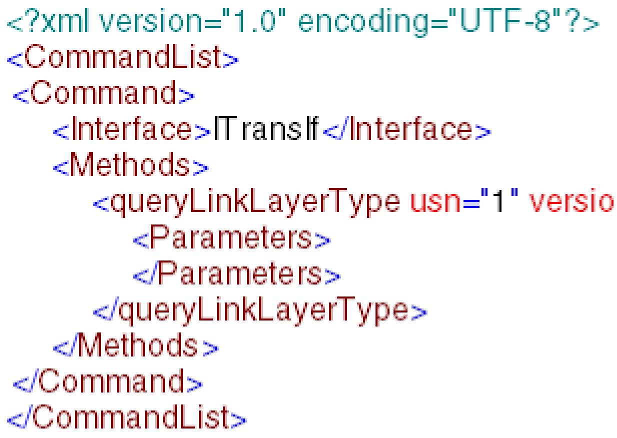
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryLinkLayerType usn="1" version="1.0">
             <Parameters>
                 <Name>ATM</Name>
             </Parameters>
         </queryLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **queryLinkLayerType** success response:



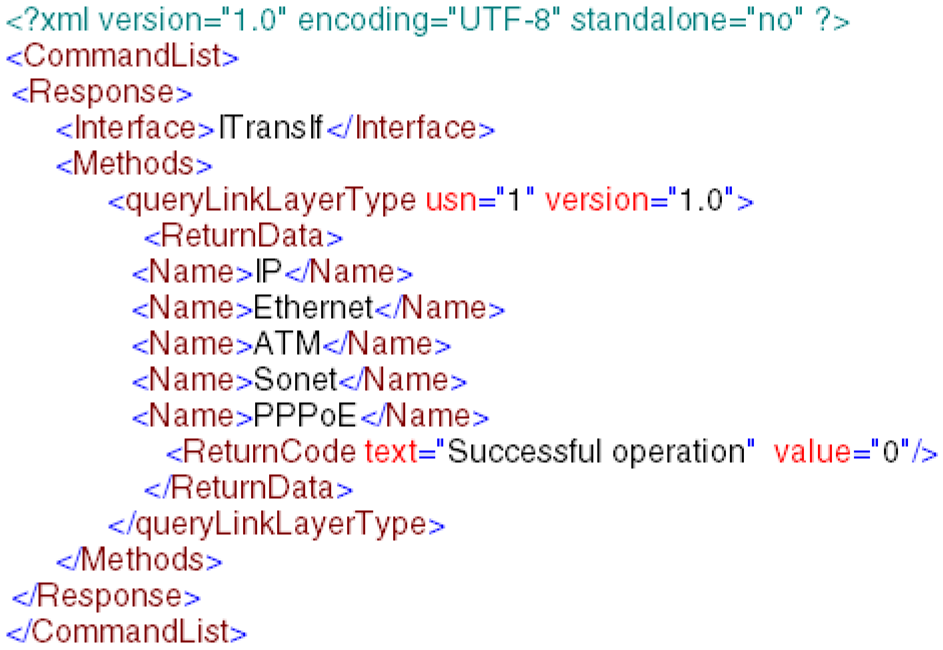
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList >
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <queryLinkLayerType usn="1" version="1.0">
              <ReturnData>
             <Name>ATM</Name>
             <Overhead>16</Overhead>
             <UnitSize>53</UnitSize>
             <UnitOverhead>5</UnitOverhead>
                 <ReturnCode text="Successful operation"  value="0"/>
              </ReturnData>
          </queryLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

An example of a **queryLinkLayerType** request that retrieves all the names of the LinkLayerTypes:



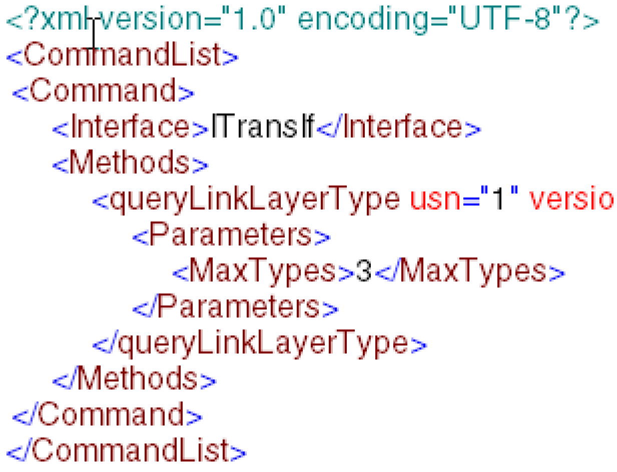
```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
    <Interface>ITransIf</Interface>
    <Methods>
       <queryLinkLayerType usn="1" version="1.0">
          <Parameters>
          </Parameters>
       </queryLinkLayerType>
    </Methods>
 </Command>
</CommandList>
```

An example of a **queryLinkLayerType** success response:



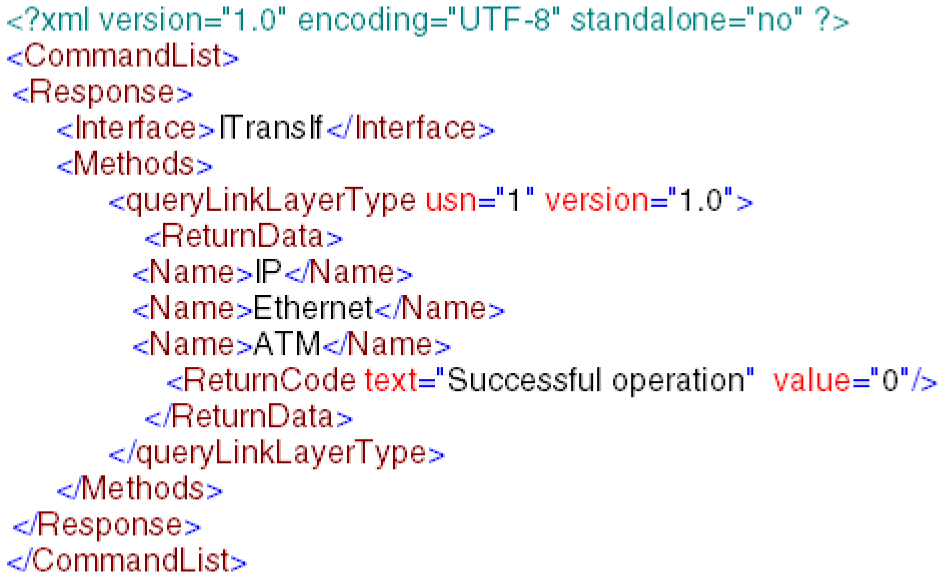
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
    <Interface>ITransIf</Interface>
    <Methods>
        <queryLinkLayerType usn="1" version="1.0">
           <ReturnData>
          <Name>IP</Name>
          <Name>Ethernet</Name>
          <Name>ATM</Name>
          <Name>Sonet</Name>
          <Name>PPPoE</Name>
             <ReturnCode text="Successful operation"  value="0"/>
           </ReturnData>
        </queryLinkLayerType>
    </Methods>
 </Response>
</CommandList>
```

An example of a **queryLinkLayerType** request that retrieves a specified number of names of LinkLayerTypes:



```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
 <Command>
     <Interface>ITransIf</Interface>
     <Methods>
         <queryLinkLayerType usn="1" version="1.0">
             <Parameters>
                 <MaxTypes>3</MaxTypes>
             </Parameters>
         </queryLinkLayerType>
     </Methods>
 </Command>
</CommandList>
```

An example of a **queryLinkLayerType** success response:



```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CommandList>
 <Response>
     <Interface>ITransIf</Interface>
     <Methods>
          <queryLinkLayerType usn="1" version="1.0">
              <ReturnData>
             <Name>IP</Name>
             <Name>Ethernet</Name>
             <Name>ATM</Name>
                 <ReturnCode text="Successful operation"  value="0"/>
              </ReturnData>
          </queryLinkLayerType>
     </Methods>
 </Response>
</CommandList>
```

Create a filesystem

Purpose of this procedure

This procedure is used to add a new filesystem to the Policy Controller hard drives. This procedure must be performed on both of the Policy Controller units in the node.

Limitations and restrictions

The following limitations apply to creating new filesystems:

- Perform this procedure at the direction of Nortel Networks support personnel.
- The minimum size for a new filesystem is 27 (MB).
- Due to overhead that the operating system requires, the size of the new filesystem is slightly larger than the value entered.
- New filesystem names must be unique from existing filesystem names currently in the system.

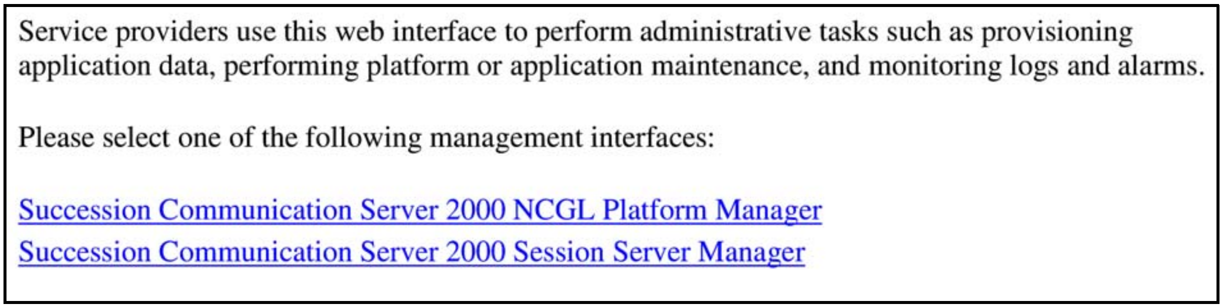
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



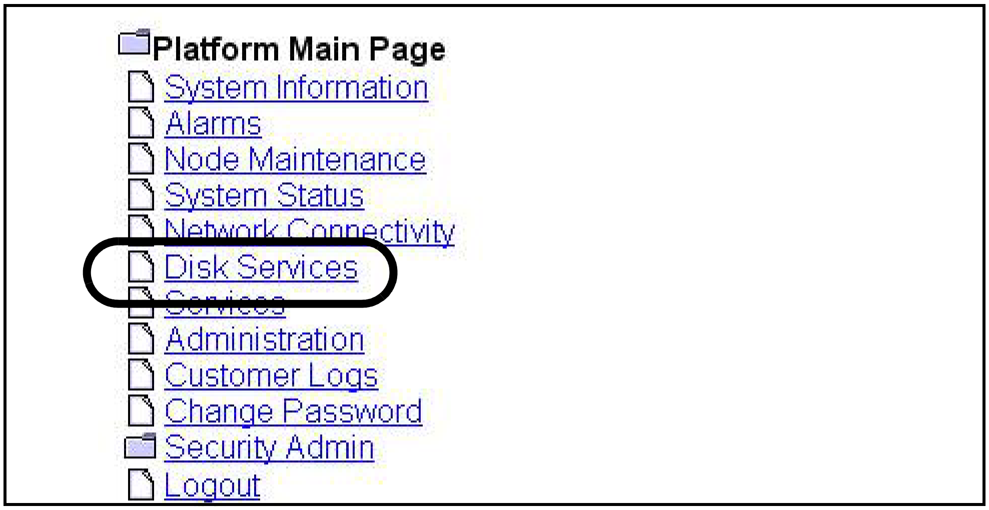
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

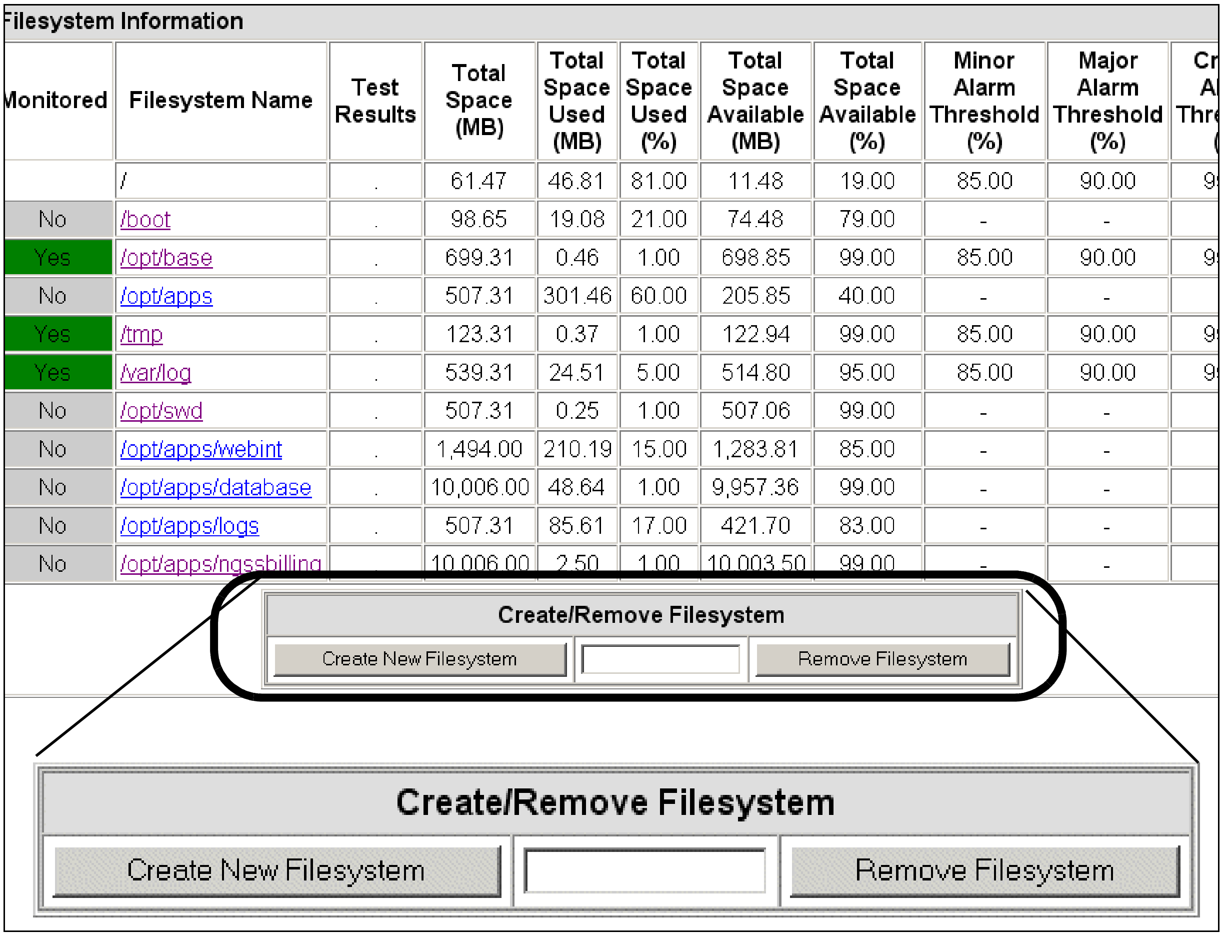
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

The Disk Services page is displayed.



3 Scroll to the *Create/Remove Filesystem* section.



Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Cr Al Thre (
	/	.	61.47	46.81	81.00	11.48	19.00	85.00	90.00	9
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	9
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00	-	-	
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00	85.00	90.00	9
Yes	/var/log	.	539.31	24.51	5.00	514.80	95.00	85.00	90.00	9
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00	-	-	
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00	-	-	
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00	-	-	
No	/opt/apps/ngssbilling		10,006.00	2.50	1.00	10,003.50	99.00	-	-	

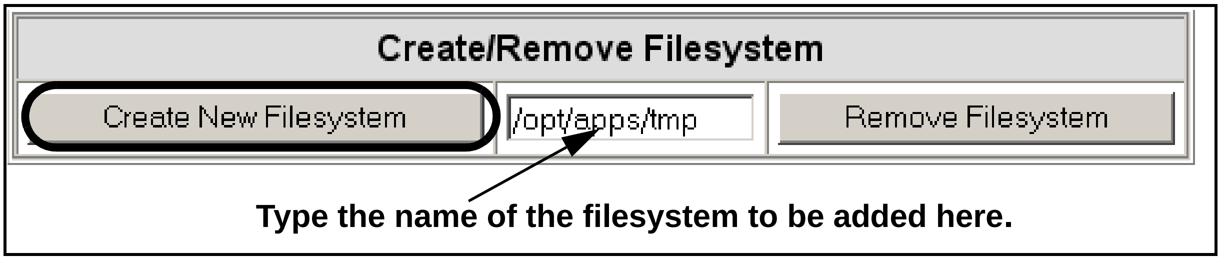
4 Type a name for the new filesystem in the blank field and click the **Create New Filesystem** button to open the Set Size window.

Note 1: The name entered for the new filesystem must be fully qualified from the root level (/) and must begin with a forward slash (/) character.

Note 2: Use only the following characters when naming the filesystem:

- 0-9
- a-z
- A-Z
- / + .- (slash, plus sign, period and dash; use of the underscore character "_" and $ are not supported)

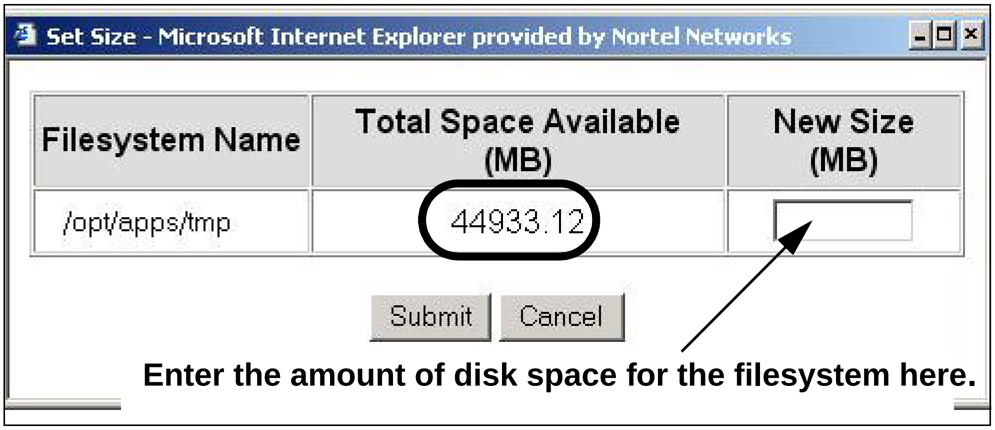
Note 3: New filesystem names must be unique from existing filesystem names currently in the system.



Type the name of the filesystem to be added here.

5 Enter the size of the filesystem to create in the New Size field then click the **Submit** button.

Note: The numeric value must be at least 27 (MB) and no more than the total space (MB) available. If you enter a value that is not in an acceptable range for the system, an error message is generated and you are prompted to enter a minimum value.

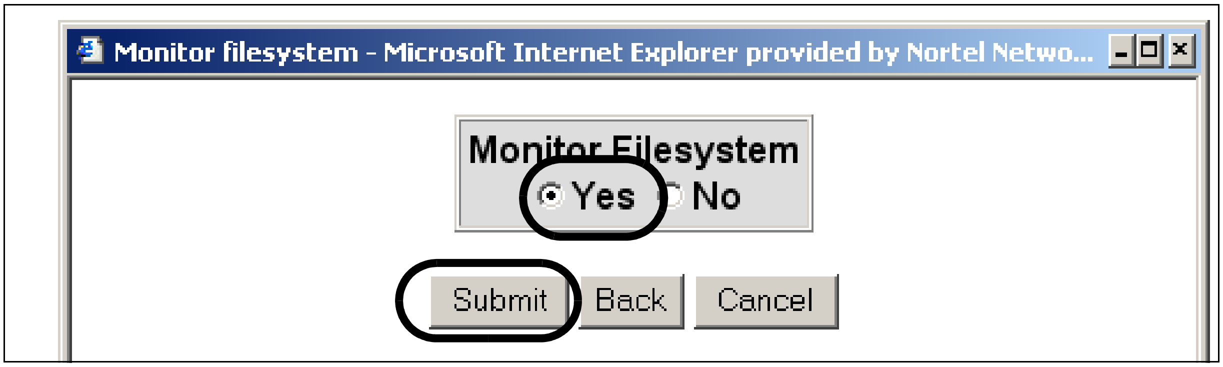

Set Size - Microsoft Internet Explorer provided by Nortel Networks
Submit
Cancel

Filesystem Name	Total Space Available (MB)	New Size (MB)
/opt/apps/tmp	44933.12	

Enter the amount of disk space for the filesystem here.

6 To enable disk space monitoring for this filesystem, click the **Yes** radio button and click **Submit**.

ATTENTION
Nortel Networks recommends monitoring for all filesystems.

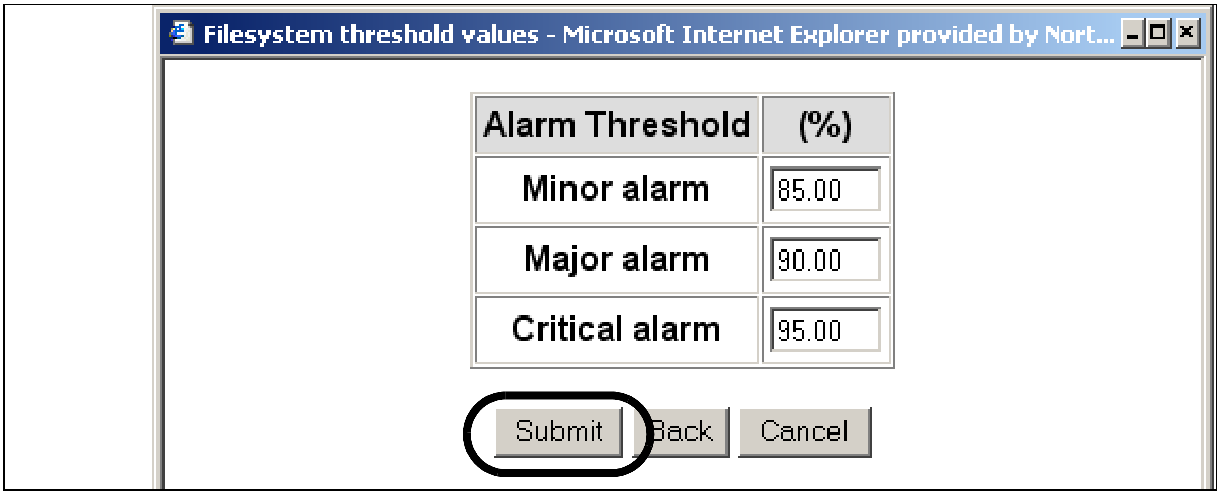

Monitor filesystem - Microsoft Internet Explorer provided by Nortel Netwo...
Monitor Filesystem
● Yes ○ No
Submit
Back
Cancel

7

ATTENTION
Ensure that you enter the highest threshold value for the critical alarm and the lowest value or the minor alarm.

It is not recommended to set the alarm thresholds lower than their default settings, unless recommended by Nortel support personnel. Doing so may produce additional alarm and log activity.

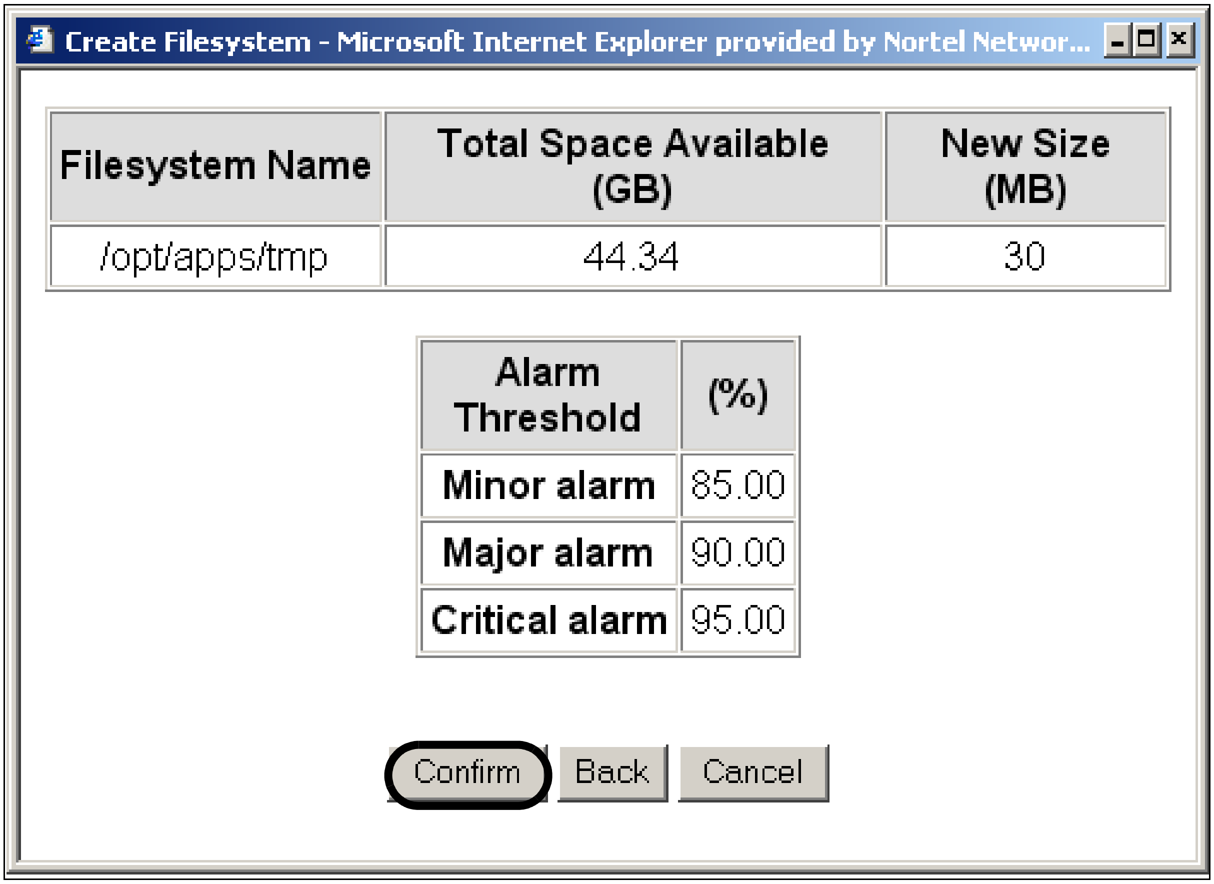
If desired, change the alarm threshold values, then click **Submit**.



Filesystem threshold values - Microsoft Internet Explorer provided by Nort...

Alarm Threshold	(%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00

8 Review the provisioning data for the new filesystem and click **Confirm** to create the new filesystem, or click **Back** to make changes.

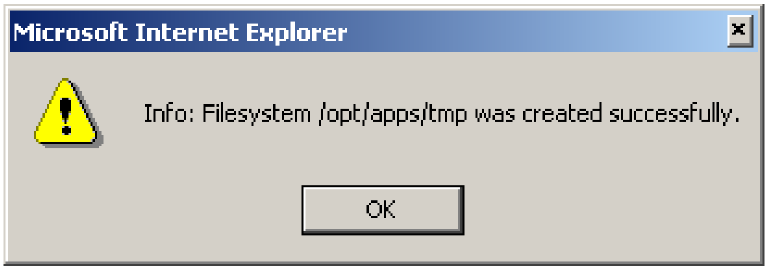


Create Filesystem - Microsoft Internet Explorer provided by Nortel Networ...

Filesystem Name	Total Space Available (GB)	New Size (MB)
/opt/apps/tmp	44.34	30

Alarm Threshold	(%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00

9 When the system indicates that the filesystem was successfully created, click **OK**.

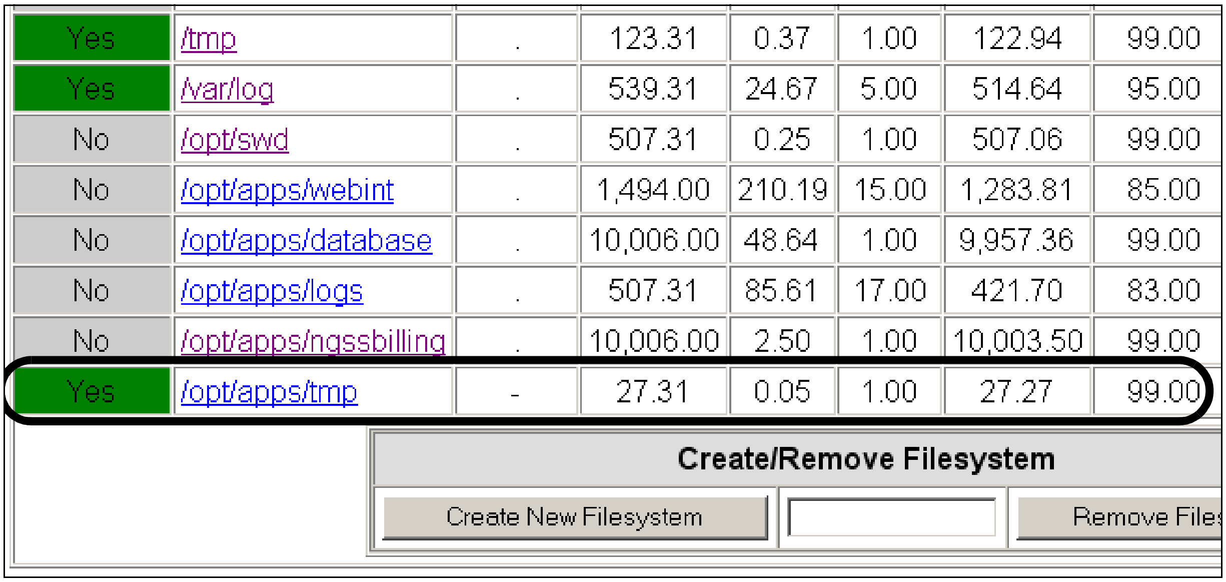


Microsoft Internet Explorer

Info: Filesystem /opt/apps/tmp was created successfully.

You are returned to the Filesystem Information view.

10 Confirm that the new file system shows up in the *Filesystem Information* view. If you need to make changes to the filesystem, refer to the appropriate procedure in this NTP for instructions.



Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00
Yes	/opt/apps/tmp	-	27.31	0.05	1.00	27.27	99.00

11 Repeat this procedure for the other (mate) Policy Controller unit, using the same values and settings as you did for the first unit.

12 This procedure is complete.

Start filesystem monitoring

Purpose of this procedure

ATTENTION
Nortel Networks recommends monitoring all filesystems.

Use this procedure to start (enable) monitoring of disk and filesystem usage. Monitoring usage means that the NCGL operating system raises a critical, major, or minor alarm when thresholds are crossed. This procedure must be performed on both of the Policy Controller units in the node.

Limitations and restrictions

There are no limitations for performing this procedure

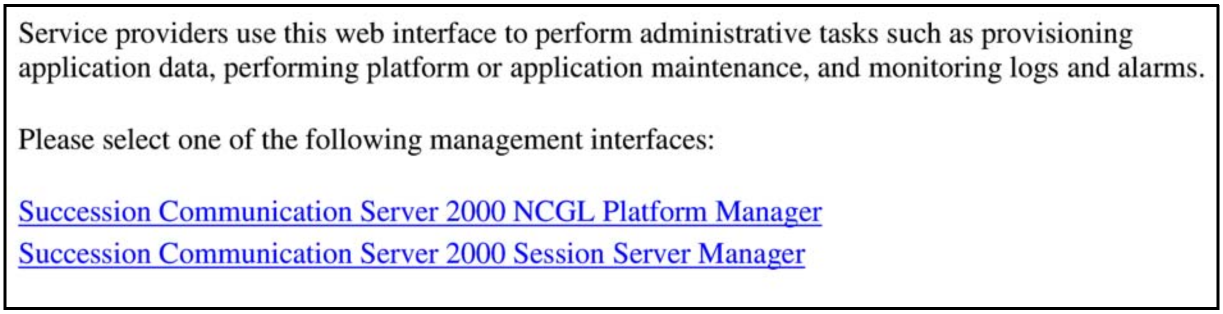
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

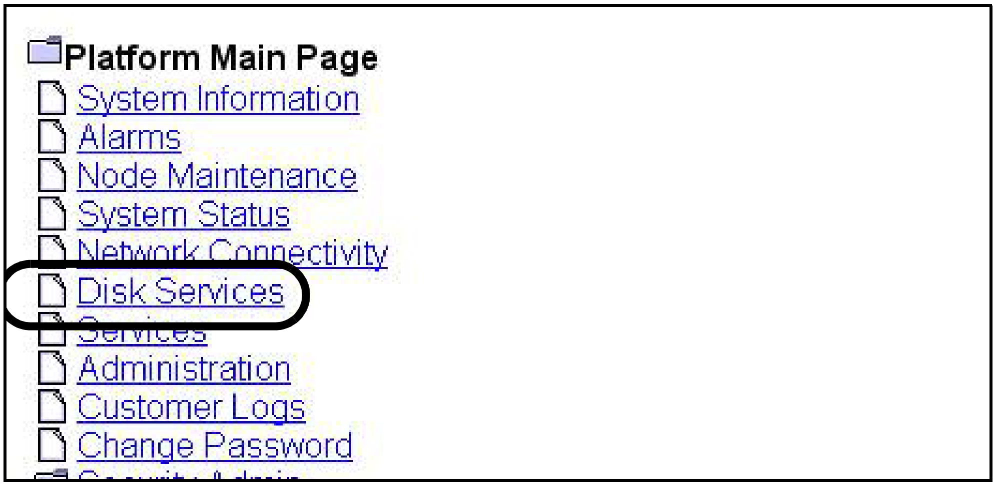


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

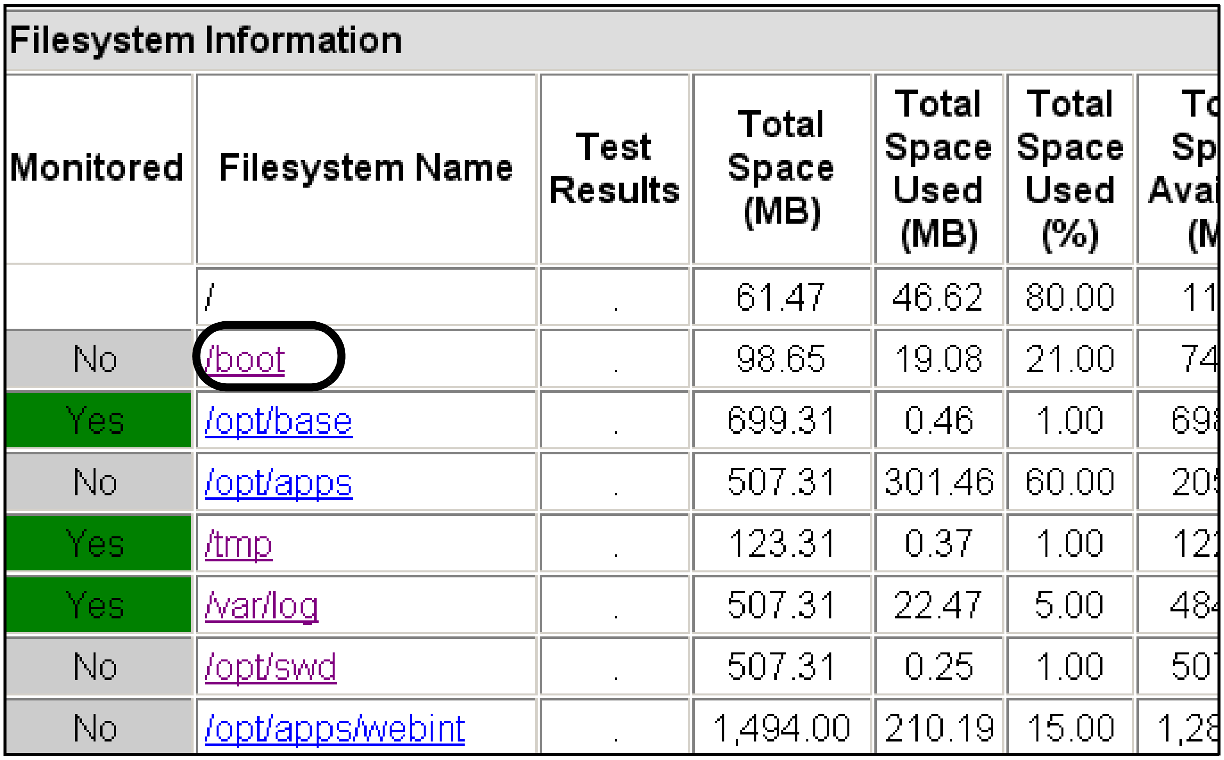
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.



The Disk Services page is displayed.

3 Filesystems that are not monitored are indicated with a ‘No’ in the *Monitored* column of the *Filesystem Information* panel. To begin monitoring a filesystem, click the filesystem link for which you want to enable monitoring.



Filesystem Information

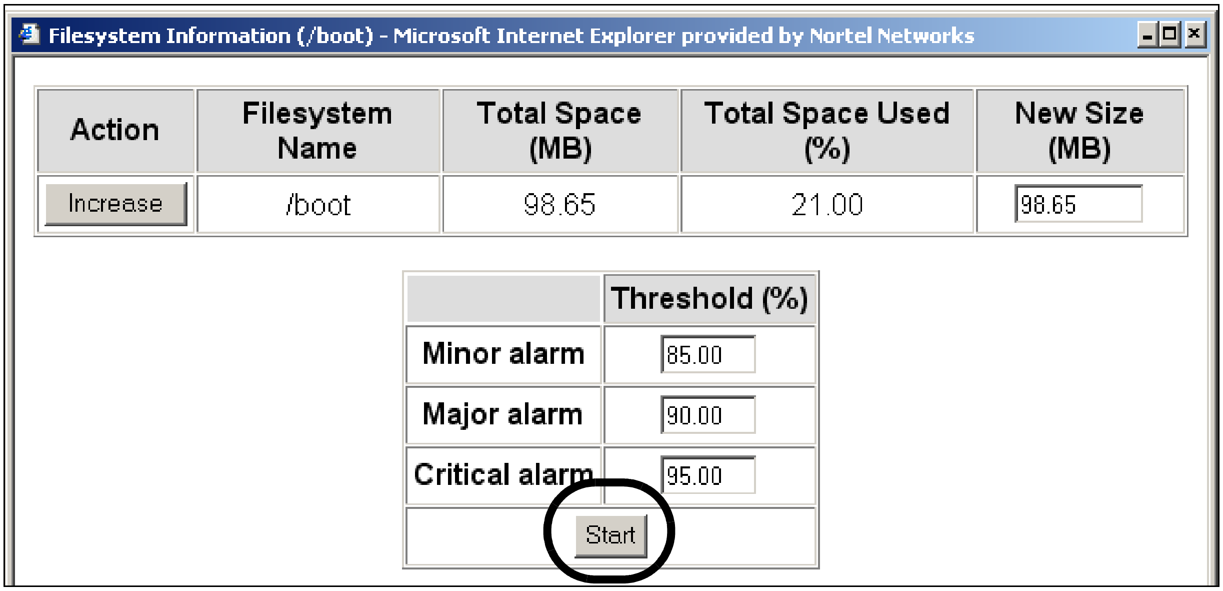
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,28

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 If you want to start filesystem monitoring using the existing settings, click the **Start** button.

or

If you would like to make adjustments to the alarm threshold levels, continue with step 5.


Filesystem Information (/boot) - Microsoft Internet Explorer provided by Nortel Networks

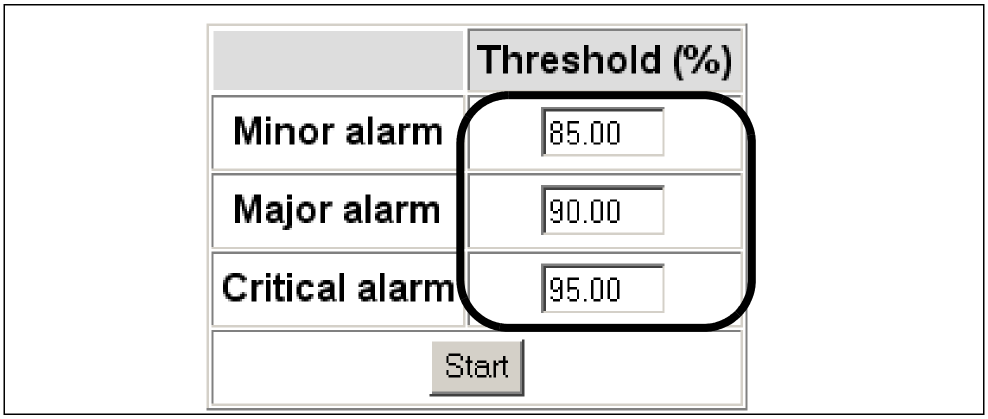
Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/boot	98.65	21.00	98.65

	Threshold (%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00
Start	

5

ATTENTION
Ensure that you enter the highest threshold value for the critical alarm and the lowest value or the minor alarm.

Adjust the monitoring thresholds for the filesystem by entering a new threshold value for one or more of the alarm severity types. When you are done then click the **Start** button.



	Threshold (%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00

6 Repeat this procedure for the same filesystem on the second (mate) Policy Controller unit.

7 This procedure is complete.

Modify filesystem monitoring thresholds

Purpose of this procedure

Use this procedure to modify the thresholds for monitoring disk and filesystem usage. Policy Controller has the ability to raise critical, major, or minor alarms when specified disk resource usage thresholds are crossed. This procedure must be performed on both of the Policy Controller units in the node.

> **ATTENTION**
> Nortel Networks recommends monitoring all filesystems.

Limitations and restrictions

It is not recommended to set the alarm thresholds lower than their default settings, unless recommended by Nortel support personnel. Doing so may produce additional alarm and log activity.

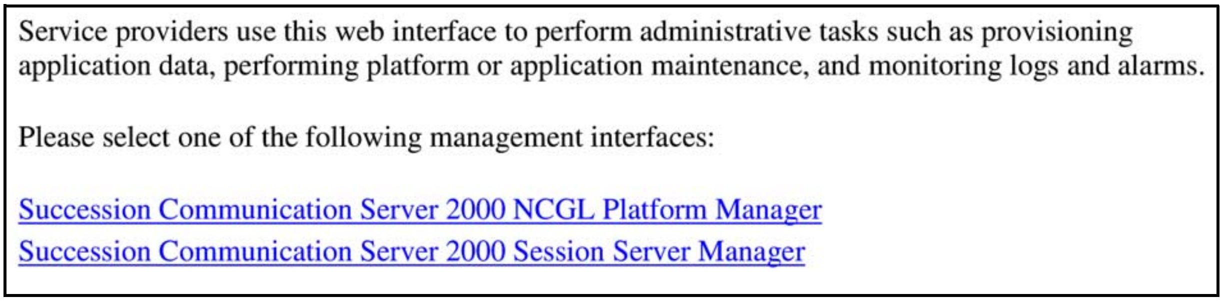
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

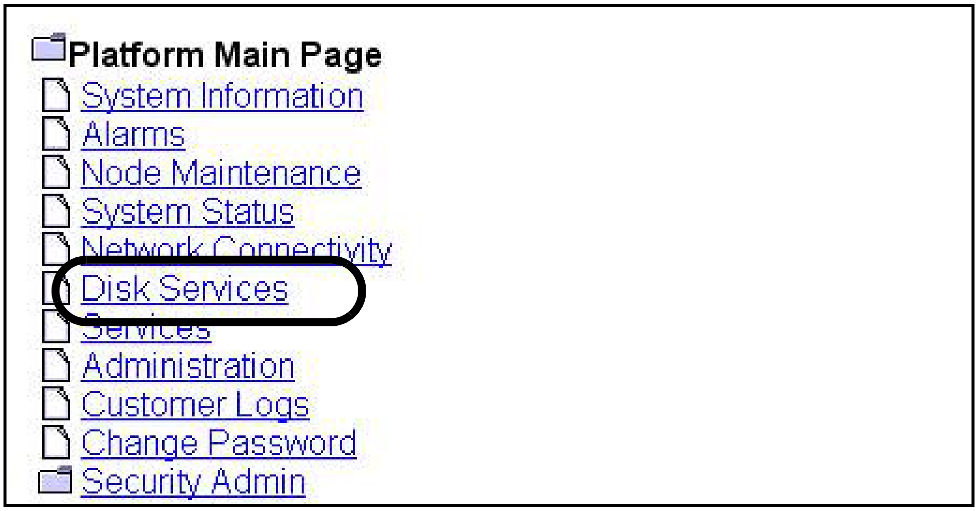


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

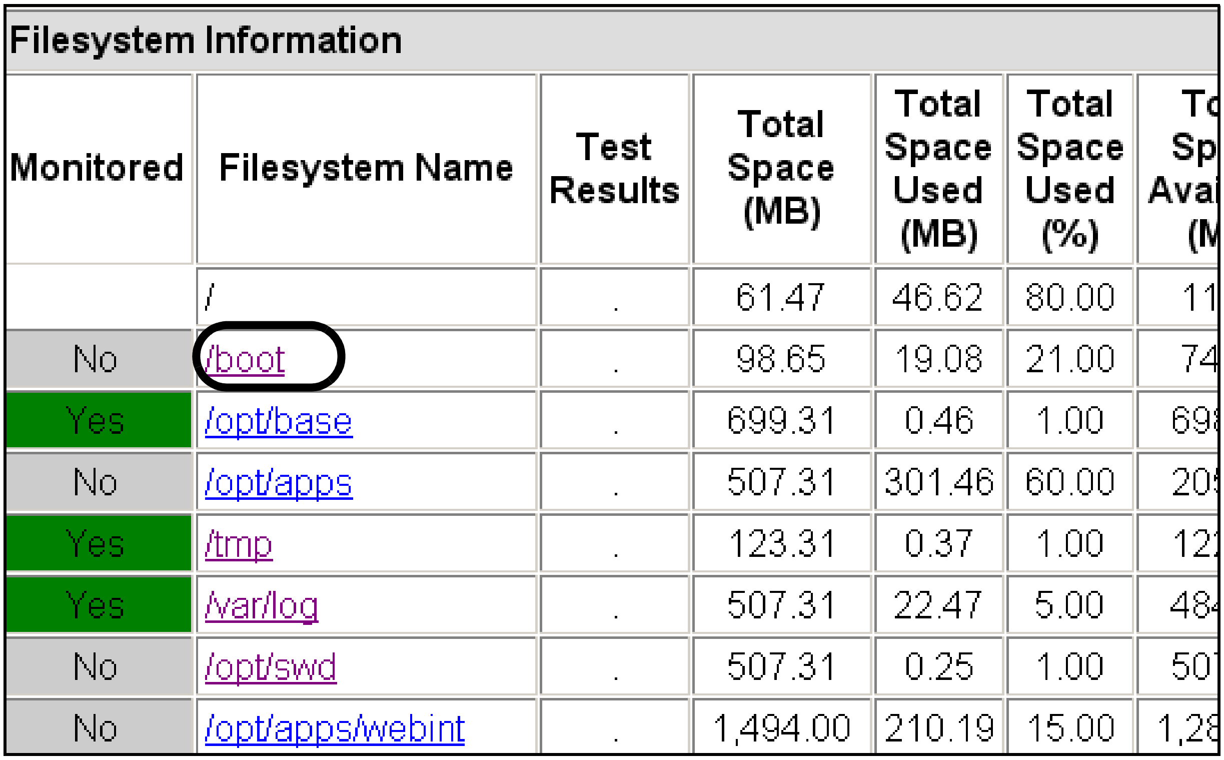
2 Click the **Disk Services** link.



Platform Main Page
- System Information
- Alarms
- Node Maintenance
- System Status
- Network Connectivity
- Disk Services
- Services
- Administration
- Customer Logs
- Change Password
- Security Admin

The Disk Services page is displayed.

3 Filesystems that are monitored are indicated with a ‘Yes’ in the *Monitored* column of the *Filesystem Information* panel. To modify settings for a monitored filesystem, click the filesystem link for the filesystem you want to modify monitored settings for.



Filesystem Information

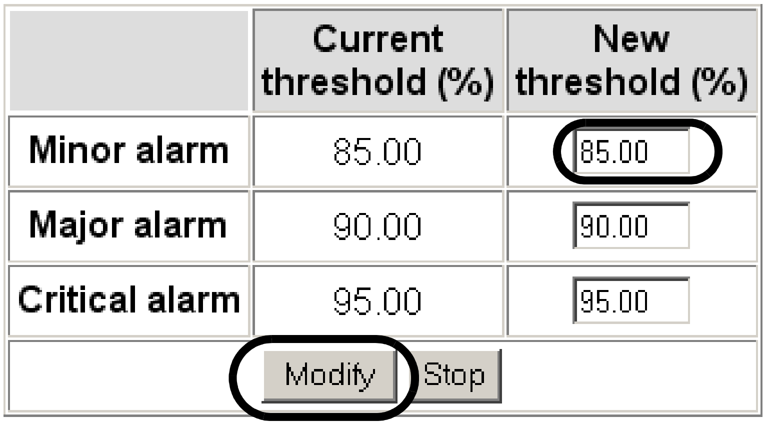
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,28

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 Enter a new threshold value for the filesystem monitor, for each of the alarm severity types, then click the **Modify** button.

ATTENTION

Ensure that you enter the highest threshold value for the critical alarm and the lowest value for the minor alarm.



	Current threshold (%)	New threshold (%)
Minor alarm	85.00	85.00
Major alarm	90.00	90.00
Critical alarm	95.00	95.00

5 Repeat this procedure for the same filesystem on the second (mate) Policy Controller unit.

6 This procedure is complete.

Increase a filesystem size

Purpose of this procedure

This procedure is used to increase the size (in MB) of an existing filesystem on the Policy Controller hard drives. This procedure must be performed on both of the Policy Controller units in the node.

Limitations and restrictions

Perform this procedure at the direction of Nortel Networks support personnel.

Due to overhead that the operating system requires, the new size of the filesystem is slightly larger than the value entered.

You cannot reduce the size of a filesystem. You must first remove the filesystem completely using procedure Remove a filesystem on page 171, then recreate the filesystem, using a smaller amount of disk space, using procedure Create a filesystem on page 149.

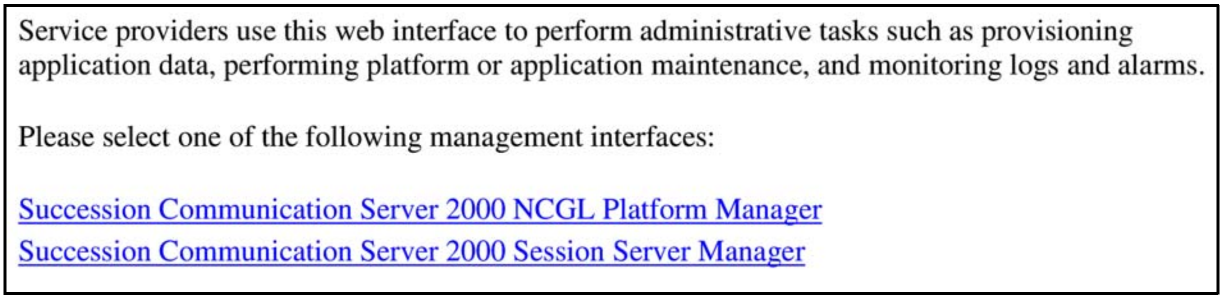
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



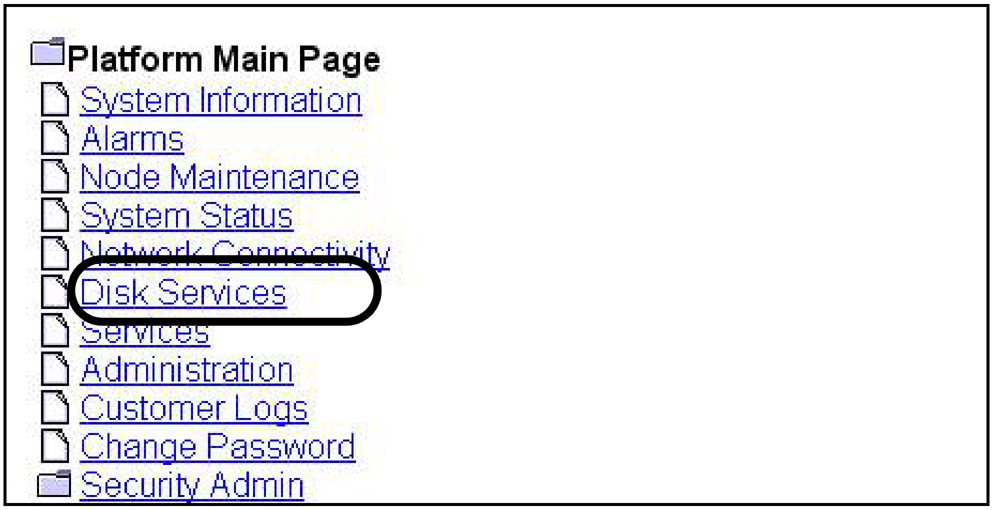
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

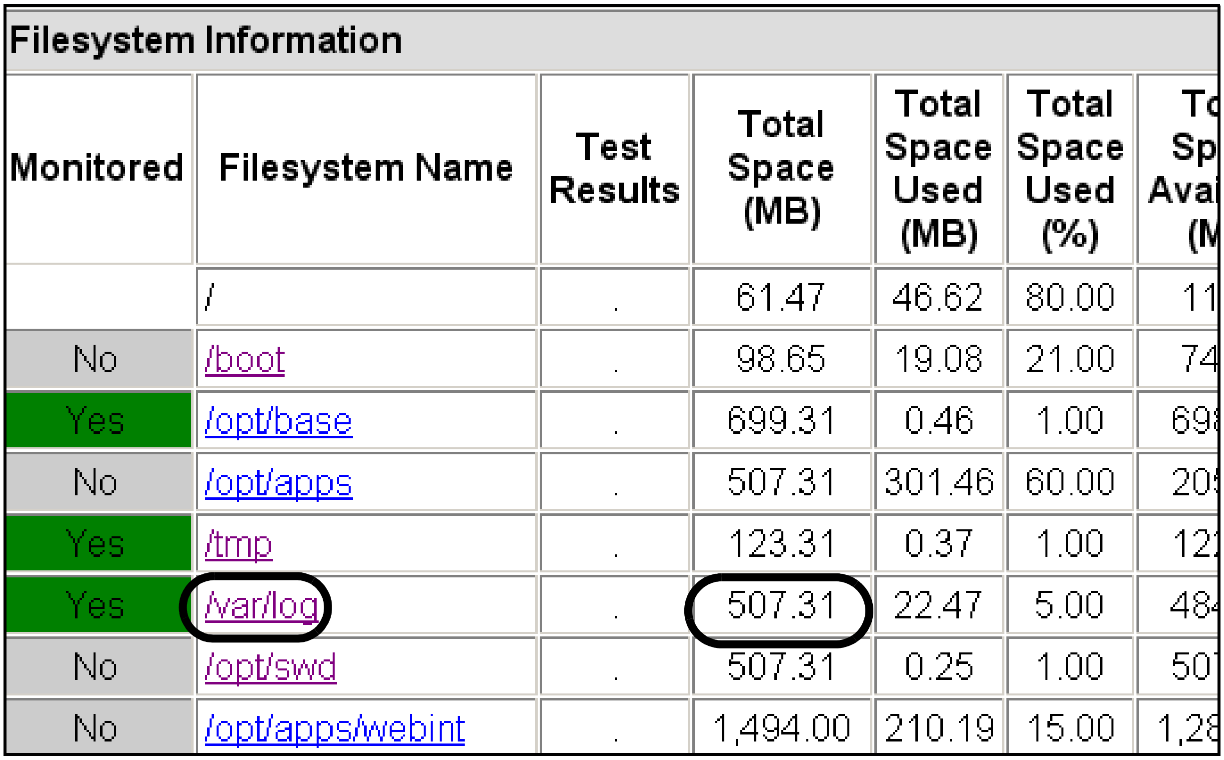
The Disk Services page is displayed.



Platform Main Page
- System Information
- Alarms
- Node Maintenance
- System Status
- Network Connectivity
- Disk Services
- Services
- Administration
- Customer Logs
- Change Password
- Security Admin

The Disk Services page is displayed.

3 Make a note of the current filesystem size, then click the filesystem link for the filesystem that you want to increase in size.



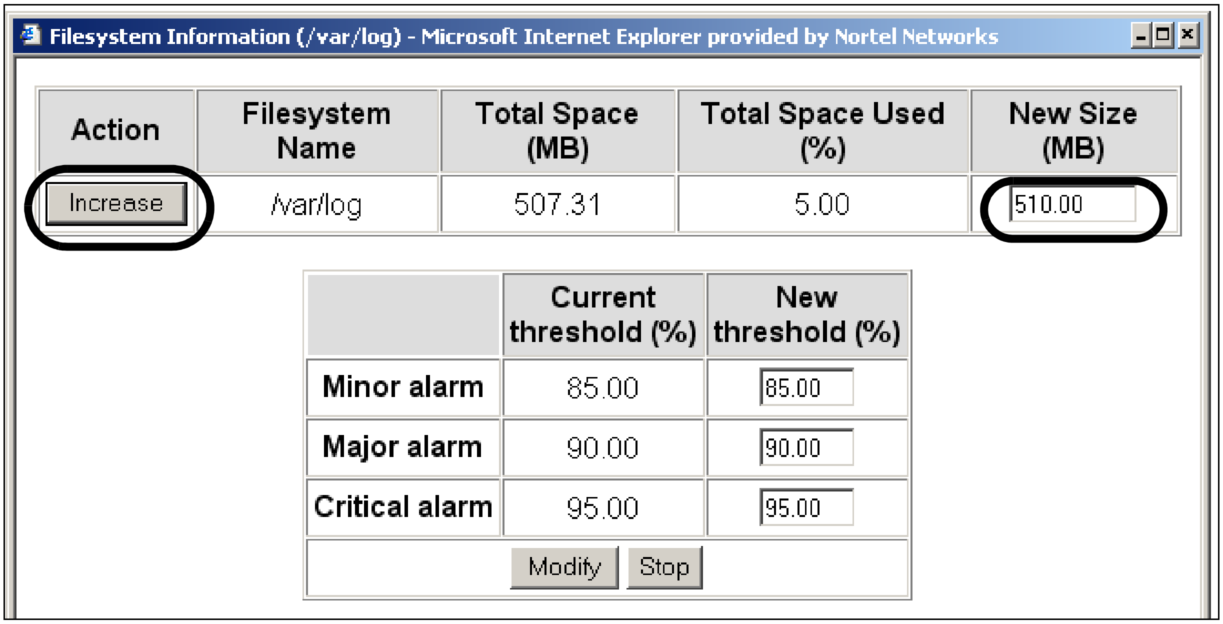
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,28

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 Enter a new value for the filesystem size in the **New Size** field then click the **Increase** button.

Note: Enter a value that is larger than the value shown in the Total Space (MB) field.

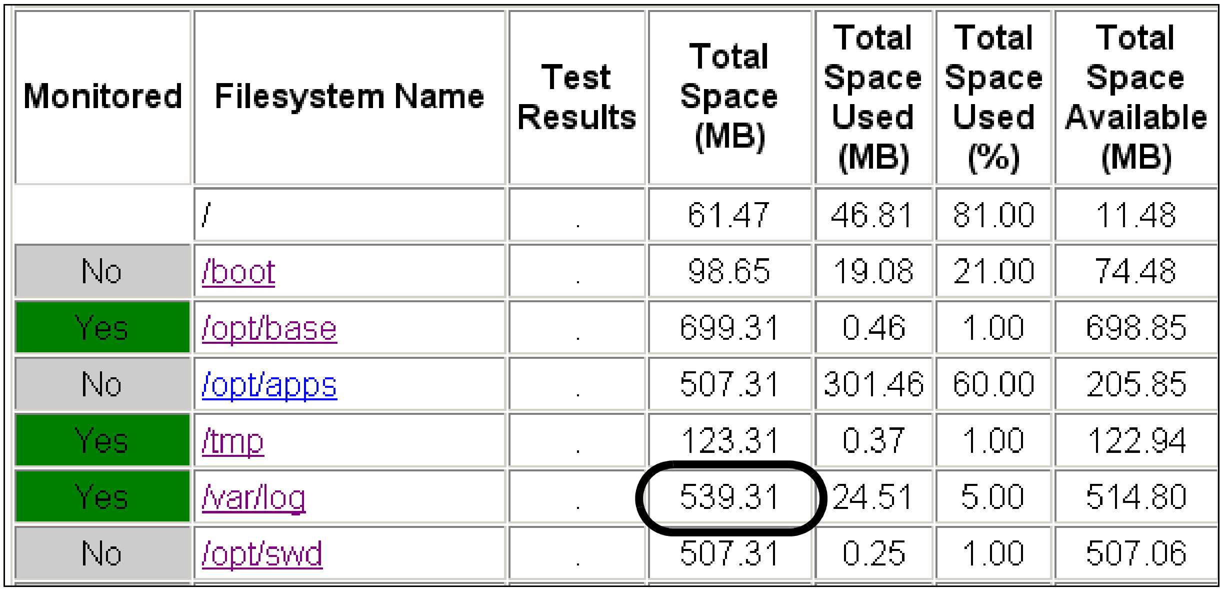

Filesystem Information (/var/log) - Microsoft Internet Explorer provided by Nortel Networks
Increase
Modify
Stop

Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/var/log	507.31	5.00	510.00

	Current threshold (%)	New threshold (%)
Minor alarm	85.00	85.00
Major alarm	90.00	90.00
Critical alarm	95.00	95.00
	Modify Stop	

5 Verify that the increase is indicated in the Total Space (MB) column of the *Filesystem Information* panel.

Note: Due to overhead that the operating system requires, the new size of the filesystem is slightly larger than the value entered.



Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)
	/	.	61.47	46.81	81.00	11.48
No	/boot	.	98.65	19.08	21.00	74.48
Yes	/opt/base	.	699.31	0.46	1.00	698.85
No	/opt/apps	.	507.31	301.46	60.00	205.85
Yes	/tmp	.	123.31	0.37	1.00	122.94
Yes	/var/log	.	539.31	24.51	5.00	514.80
No	/opt/swd	.	507.31	0.25	1.00	507.06

6 Repeat this procedure on the second (mate) Policy Controller unit.

7 This procedure is complete.

Stop filesystem monitoring

Purpose of this procedure

Use this procedure to stop (disable) monitoring of disk and filesystem usage. This procedure must be performed on both Policy Controller units in the node.

Limitations and restrictions

ATTENTION
Nortel Networks recommends monitoring all filesystems. Use this procedure only when necessary.

Do not leave monitoring disabled any longer than necessary.

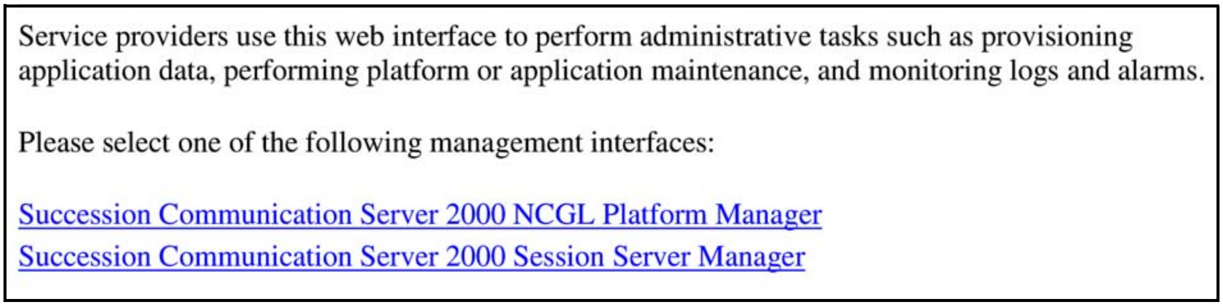
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

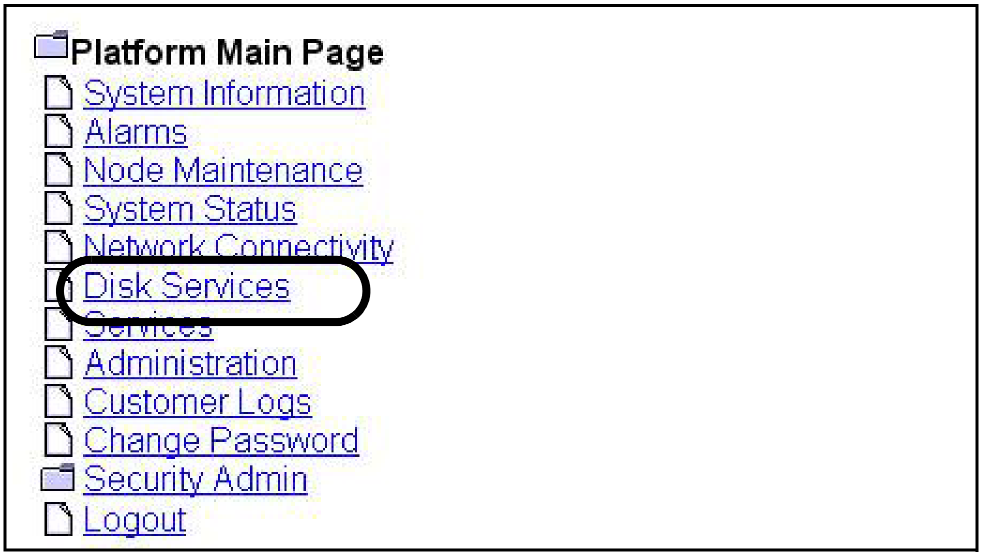


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

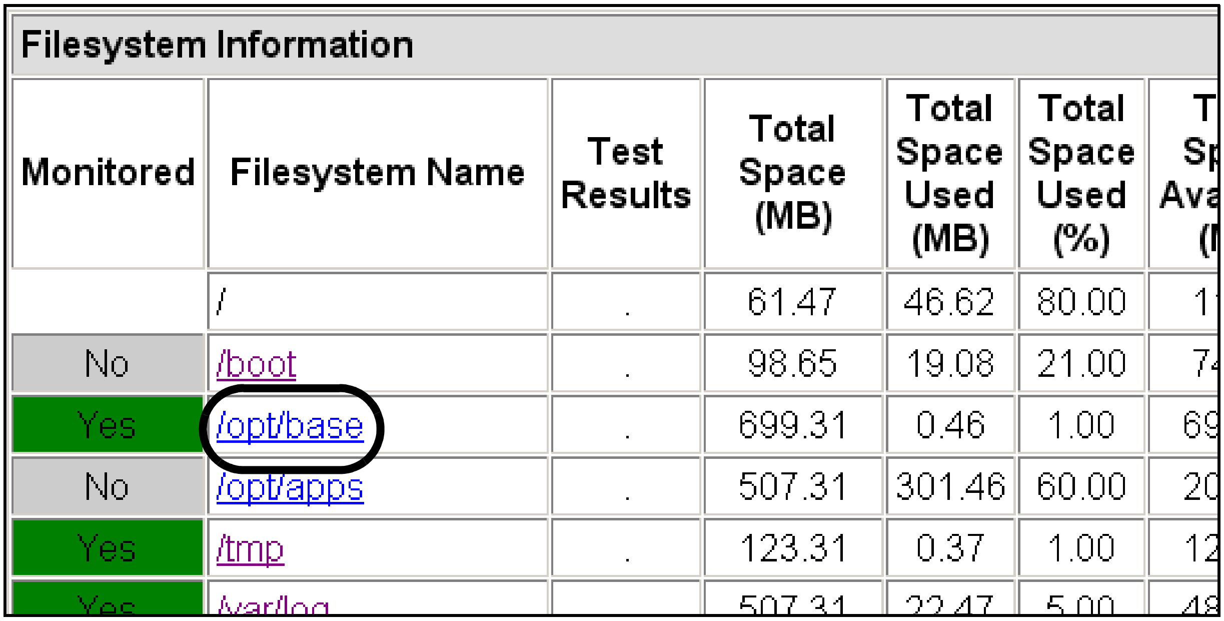
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.



The Disk Services page is displayed.

3 Click the filesystem link for the filesystem you want to stop monitoring.



Filesystem Information

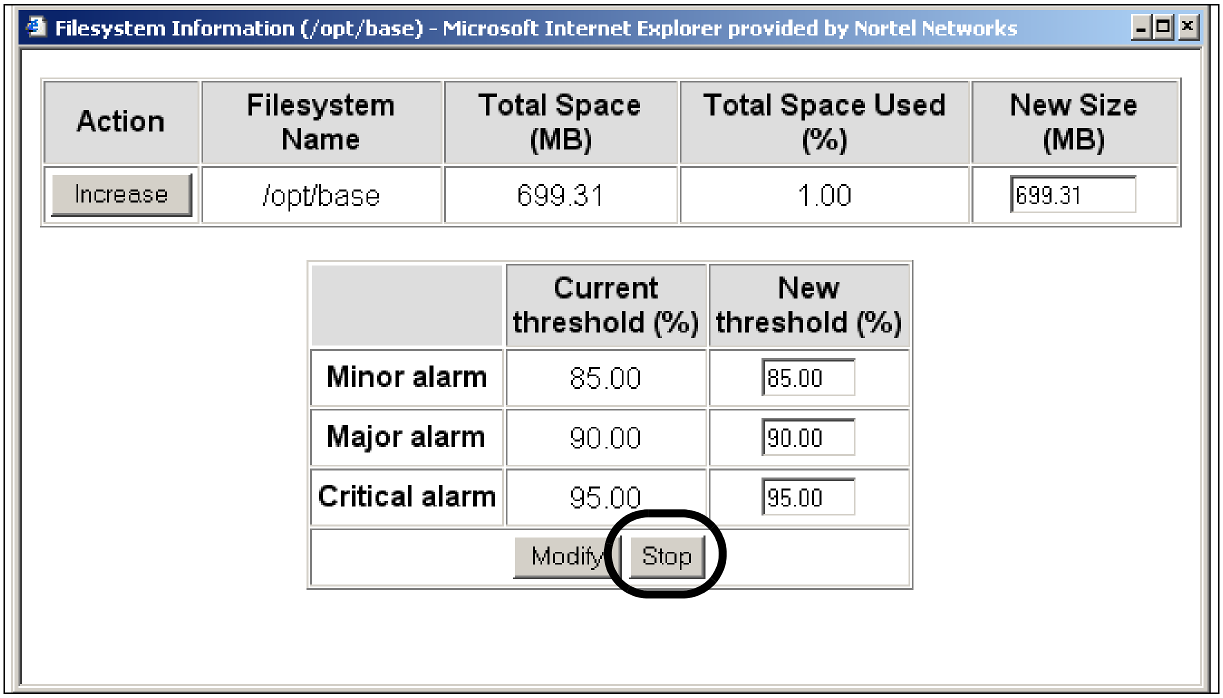
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	T Sp Ava (I
	/	.	61.47	46.62	80.00	1
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4

ATTENTION
Nortel Networks recommends monitoring all filesystems. Do not leave monitoring disabled any longer than necessary.

To stop filesystem monitoring, click the **Stop** button.



Filesystem Information (/opt/base) - Microsoft Internet Explorer provided by Nortel Networks

Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/opt/base	699.31	1.00	699.31

	Current threshold (%)	New threshold (%)
Minor alarm	85.00	85.00
Major alarm	90.00	90.00
Critical alarm	95.00	95.00

5 Repeat this procedure for the same filesystem on the second (mate) Policy Controller unit.

6 This procedure is complete.

Remove a filesystem

Purpose of this procedure

This procedure is used to remove an entire filesystem from the Policy Controller hard drives. This procedure must be performed on both of the Policy Controller units in the node.

Limitations and restrictions

Deleting the following filesystems is not allowed.

- / (root)
- /boot
- all filesystems prefixed by /opt

CAUTION

Removing filesystems permanently destroys all data on that filesystem. Since such data cannot be recovered, ensure that you have made a backup of any important data.

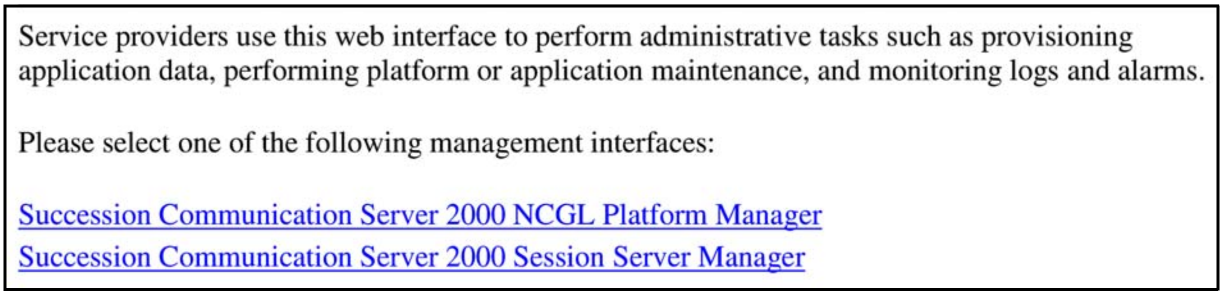
Prerequisites

For information about backing up filesystems, refer to procedures Configure database backups for the Policy Controller and Perform a data backup of the Policy Controller found in NTP *Policy Controller Security and Administration*, NN10434-611.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



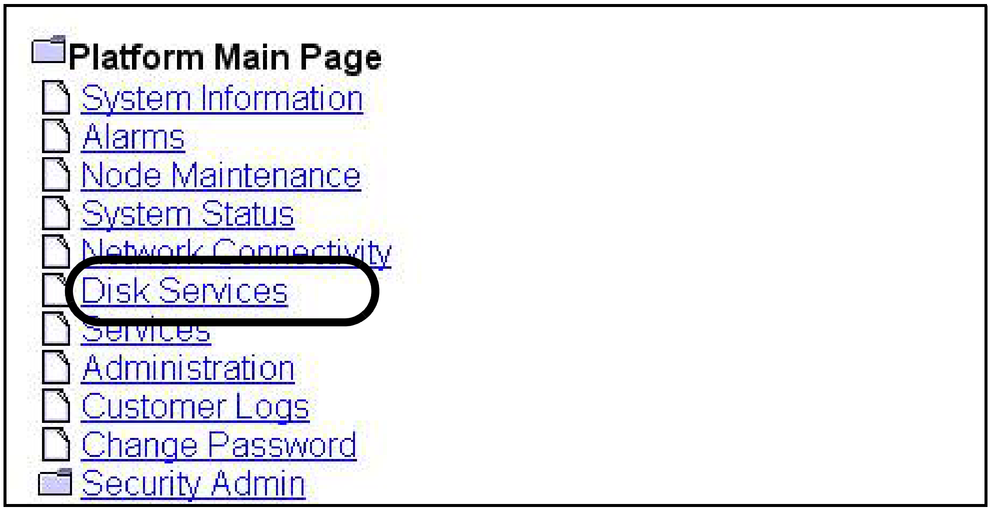
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

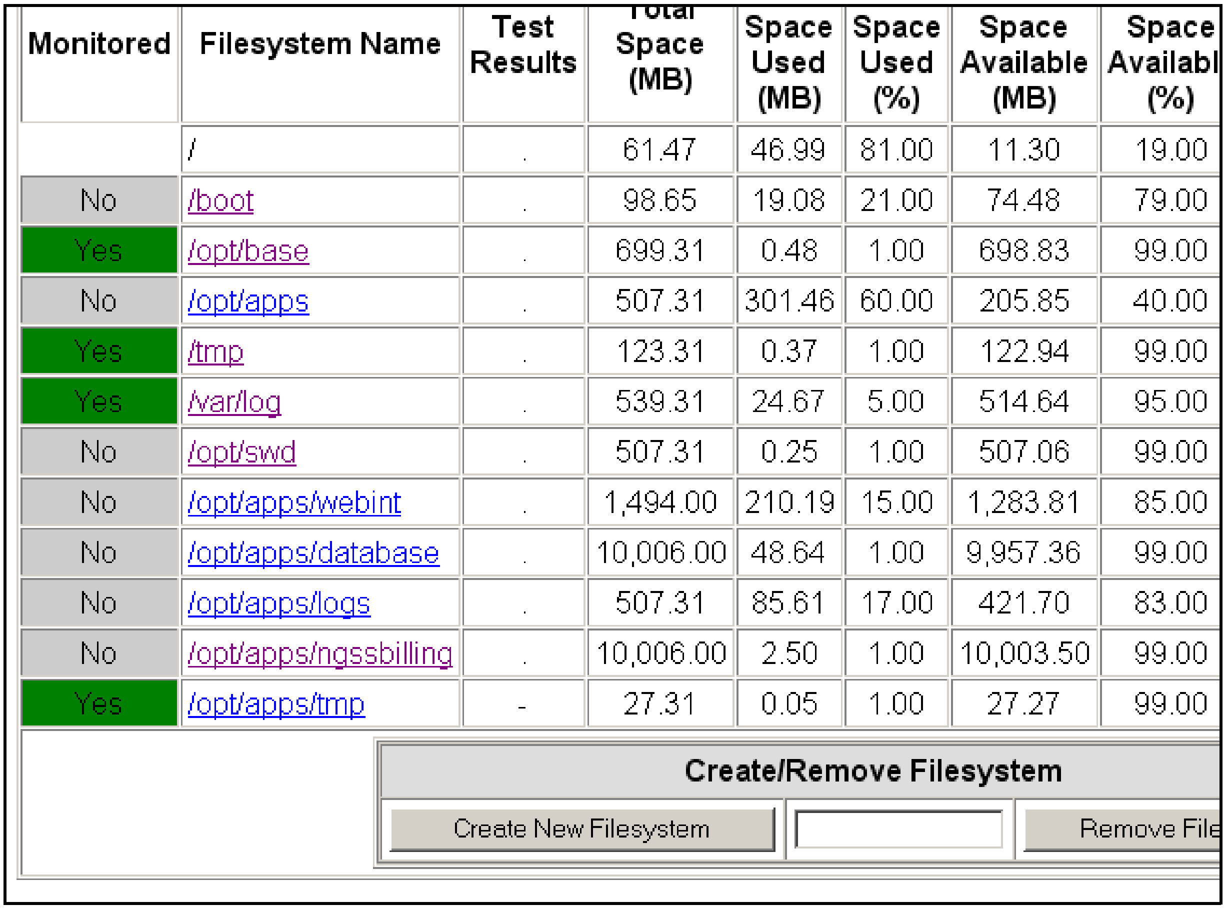
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

The Disk Services page is displayed.



3 Locate the name of the filesystem that you want to remove in the *Filesystems Information* view.

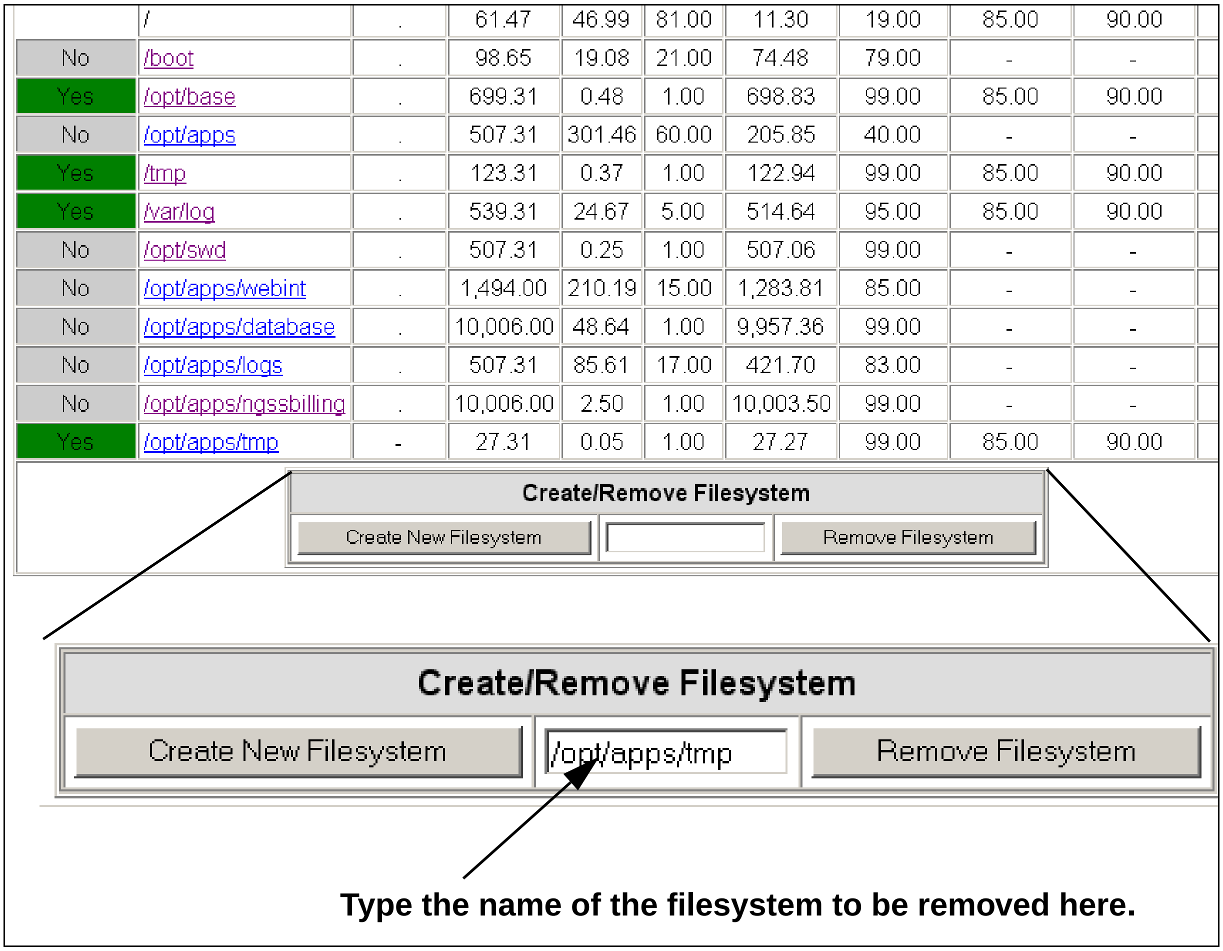


Monitored	Filesystem Name	Test Results	Total Space (MB)	Space Used (MB)	Space Used (%)	Space Available (MB)	Space Availabl (%)
	/	.	61.47	46.99	81.00	11.30	19.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00
Yes	/opt/base	.	699.31	0.48	1.00	698.83	99.00
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00
Yes	/opt/apps/tmp	-	27.31	0.05	1.00	27.27	99.00

4

ATTENTION
Deletion of the / (root) and /boot filesystems is not allowed.

Type the name of the filesystem in the blank field of the *Create/Remove Filesystem* panel, then click the **Remove Filesystem** button

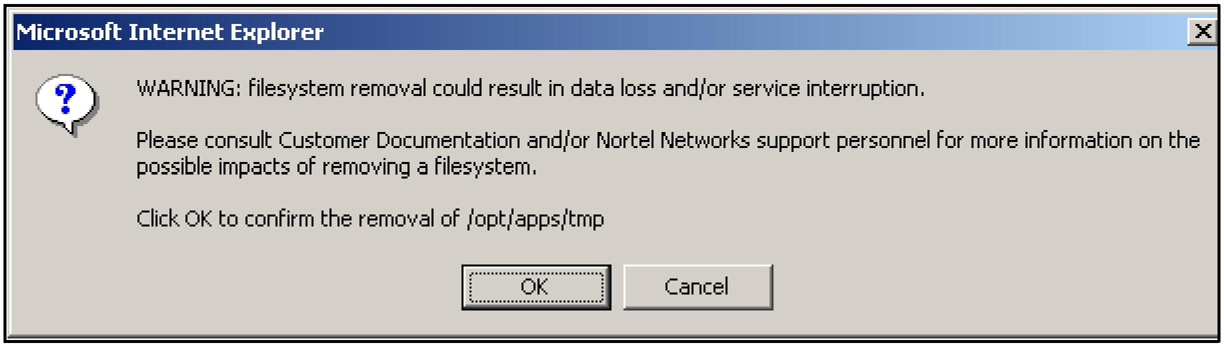


	/	.	61.47	46.99	81.00	11.30	19.00	85.00	90.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-
Yes	/opt/base	.	699.31	0.48	1.00	698.83	99.00	85.00	90.00
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00	-	-
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00	85.00	90.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00	85.00	90.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00	-	-
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00	-	-
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-
Yes	/opt/apps/tmp	-	27.31	0.05	1.00	27.27	99.00	85.00	90.00

/opt/apps/tmp

Type the name of the filesystem to be removed here.

5 Confirm that you want to remove the filesystem by clicking **OK**.

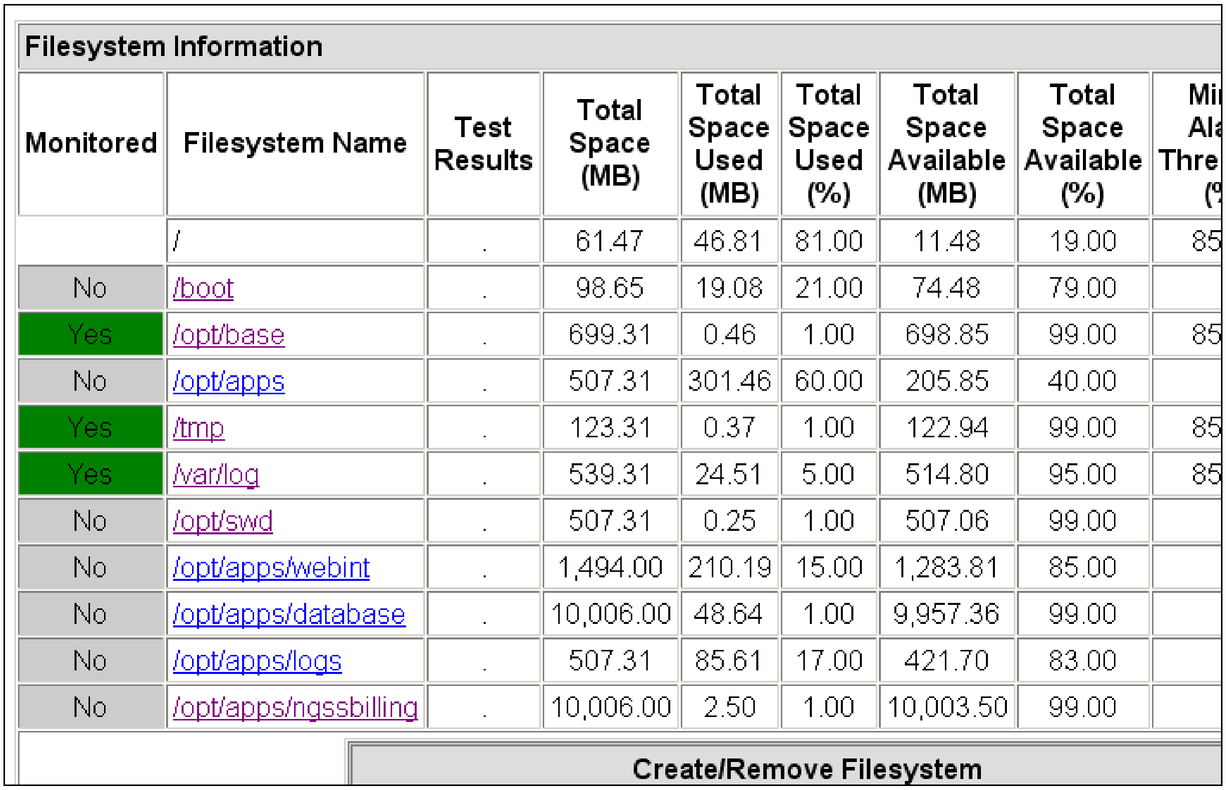


WARNING: filesystem removal could result in data loss and/or service interruption.

Please consult Customer Documentation and/or Nortel Networks support personnel for more information on the possible impacts of removing a filesystem.

Click OK to confirm the removal of /opt/apps/tmp

6 Confirm that the file system has been deleted from the *Filesystem Information* view.



Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Mi Ala Thre (%
	/	.	61.47	46.81	81.00	11.48	19.00	85
No	/boot	.	98.65	19.08	21.00	74.48	79.00	
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00	
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00	85
Yes	/var/log	.	539.31	24.51	5.00	514.80	95.00	85
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00	
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00	
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00	
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	

7 Repeat this procedure for the other (mate) Policy Controller unit, using the same values and settings as you did for the first unit.

8 This procedure is complete.

View web proxy settings in SSPFS for Policy Controller

Purpose of this procedure

Use the following activity to view the configuration of existing Policy Controller node web proxy services on the SSPFS server (part of the CS 2000 Management Tools server). Use this procedure as a standalone task or as part of a higher level activity such as a major upgrade activity.

Limitations and restrictions

If the web proxy entry for a particular Policy Controller node requires changing, you must configure a new proxy entry with the modified values, then remove the obsolete proxy entry. To add a new Policy Controller node to the proxy service configuration, refer to procedure Add a Policy Controller node to the SSPFS server web proxy, found in NTP *Policy Controller Configuration Management*, NN10432-511.

Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Policy Controller Manager GUI)

If necessary, refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

Action

At the Policy Controller CLI or Integrated EMS client

1 Verify that a security certificate has been installed on the CS 2000 Management Tools Server SSPFS platform. For assistance use procedure Installing an HTTPS certificate on a Sun server found in the NTP *Carrier Voice over IP Network Upgrade Overview*, NN10440-450.

2 Log onto the CS 2000 Management Tools server. If necessary, refer to procedure Configuring the Apache Web Server for HTTPS proxy, found in NTP *ATM/IP Solution-level Configuration Management*, NN10409-500.

3 Change to the root user by typing

```
su - root
```

and pressing the Enter key.

4 Enter the root password and press Enter.

5 Start the command line interface application by typing

```
cli
```

and pressing the Enter key.

The system responds:

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Access the Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Configuration

 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 .
 .
 18 - snmp_poller (SNMP Poller Configuration)
 X - exit
select -
```

7 Access the Apache Proxy Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Apache Proxy Configuration
 1 - add_proxy_conf (Add an IP to the Apache
Proxy Module configuration)
 2 - del_proxy_conf (Delete an IP from the
Apache Proxy Module configuration)
 3 - list_proxy_conf (List the Apache Proxy
Module configuration)

 X - exit

select -
```

8 List the current Apache Proxy Configuration entries by typing

3

and pressing the Enter key.

The system responds:

```
=== Executing “list_proxy_conf”
```

```
#Begin Proxy Config
<IfModule mod_proxy.c>
  ProxyRequests On
  # Add Proxy Entries Here
  ProxyPass /47.174.74.184/ https://47.174.74.184:443/
  ProxyPassReverse /47.174.74.184/ https://47.174.74.184:443/
  ProxyPass /47.142.209.118/ https://47.142.209.118:443/
 ProxyPassReverse /47.142.209.118/ https://47.142.209.118:443/
  ProxyPass /47.142.209.116/ https://47.142.209.116:443/
 ProxyPassReverse /47.142.209.116/ https://47.142.209.116:443/
  ProxyPass /prov/ https://47.174.74.184:8443/prov/
  ProxyPassReverse /prov/ https://47.174.74.184:8443/prov/
  AllowCONNECT 433
  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

      </IfModule>
      #End Proxy Config
      === “list_proxy_conf” completed successfully
```

9 Locate the proxy entry for the active unit GUI used by the CS 2000 Policy Controller Manager GUI. Refer to the following figure for assistance in locating this entry.

ProxyPass /10.65.99.67/ https://10.65.99.67:443/ *ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/*	Entry for physical unit 0
ProxyPass /10.65.99.70/ https://10.65.99.70:443/ *ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/*	Entry for physical Unit 1
ProxyPass /10.65.99.72/ https://10.65.99.72:443/ *ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/*	Entry for active unit
*ProxyPass /**prov**/ https://10.67.99.72:8443/**prov**/* *ProxyPassReverse /**prov**/ https://10.67.99.72:8443/**prov**/*	Entry for active unit GUI

10 If necessary, record the label for the remote hostname/tag associated with the Policy Controller active unit.

ATTENTION

If necessary, please refer to section Selecting and using tag names in SN08 and newer on page 181 for more information about using remote tag names. The tag name shown must match the tag name used by the Policy Controller application for the same Policy Controller node when you installed or upgrading it.

11 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

12 Exit the Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

13 Exit the CLI by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 If applicable, logout from the workstation.

Selecting and using tag names in SN08 and newer

Tag names for the active Policy Controller unit web proxy entries, must match the tag name entered when installing or upgrading Policy Controller application. Failure to use the same tag name will prevent access to the Policy Controller GUIs after the SSPFS web proxy services restart.

ATTENTION

If you are upgrading from SN08, or rolling back to SN08, the SSPFS web proxy server must be using the “prov” tag name.

If the remote tag name for a Policy Controller node does not match that used during installation or upgrade of the Policy Controller application, you must configure a new proxy entry using the correct remote tag name, then remove the obsolete proxy entry. To perform this activity, refer to procedure Add a Policy Controller node to the SSPFS server web proxy, found in NTP *Policy Controller Configuration Management*, NN10432-511.

Add a Policy Controller node to the SSPFS server web proxy

Purpose of this procedure

Use the following activity to add web proxy services to the SSPFS server, (part of the CS 2000 Management Tools server) for supporting a Policy Controller node or to replace an existing web proxy entry for a Policy Controller entry with updated values like a new IP address or tagname.

Limitations and restrictions

DNS services are enabled on the CS 2000 Management Tools server. However, if you get an error message asking you to enable DNS while executing this procedure, quit the procedure, then complete procedure *Configuring the Domain Name Service on a Sun server* found in the ATM/IP Solution-level Configuration Management NTP, NN10409-500.

CAUTION

Executing this activity causes the Apache web service to stop and start multiple times.

You cannot modify existing web proxy entries. If you want to change web proxy IP addresses or tagnames for an existing Policy Controller node, add new web proxy entries for the node using the new values. Deleting the old entries is not necessary.

Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

Refer to section for more information about Policy Controller IP addressing and naming schemes needed to complete this activity. The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Session Server Manager GUI)

Action

At the applicable network element interface

1 Verify that an HTTPS Certificate has been installed on the CS 2000 Management Tools Server SSPFS platform. For assistance use procedure *Installing an HTTPS certificate on a Sun server* found in the IP Solution Upgrades NTP, NN10344-450/IP or the Solution level Security and Administration NTP, NN10402-600.

2 Log onto the CS 2000 Management Tools server and complete the following sub-steps to add the Policy Controller node to the proxy. If needed, you can refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

3 Change to the root user by typing

```
su - root
```

and pressing the Enter key.

4 Enter the root password and press Enter.

5 Start the command line interface application by typing

```
cli
```

and pressing the Enter key.

The system responds:

```
   Command Line Interface
   1 - View
   2 - Configuration
   3 - Other
   X - exit

select -
```

6 Access the Configuration level by typing

```
2
```

and pressing the Enter key.

The system responds:

```
  Configuration

   1 - NTP Configuration
   2 - Apache Proxy Configuration
   3 - DCE Configuration
   .
   .
   .
   18 - snmp_poller (SNMP Poller Configuration)
   X - exit

select -
```

7 Access the Apache Proxy Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Apache Proxy Configuration
 1 - add_proxy_conf (Add an IP to the Apache
Proxy Module configuration)
 2 - del_proxy_conf (Delete an IP from the
Apache Proxy Module configuration)
 3 - list_proxy_conf (List the Apache Proxy
Module configuration)

 X - exit

select -
```

8 Complete the following sub-steps to add a Policy Controller physical **Unit 0** to the proxy.

a Add Policy Controller Unit 0 to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing “add_proxy_conf”
```

b Enter the IP address for Policy Controller Unit 0 and press the Enter key.

c Enter the same IP address for the hostname/tag associated with Policy Controller Unit 0 and press the Enter key.

d Skip entering (leave blank) the optional remote hostname/tag associated with Unit 0 by pressing the Enter key.

e Enter the port number associated with the IP address for Policy Controller Unit 0 and press the Enter key.

Note: For the port number, use “443”.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.67
    Hostname   = 10.65.99.67
    Remote Tag =
    Port Num   = 443
!!WARNING!! This will result in WEBSERVER
going down (restarting) for a short time.
Continue? [Y/N]:
```

f Confirm the values you entered for Policy Controller Unit 0 by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

9 Complete the following sub-steps for the Policy Controller physical **Unit 1** to the proxy.

a Add Policy Controller Unit 1 to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing “add_proxy_conf”
```

b Enter the IP address for Policy Controller Unit 1 and press the Enter key.

c Enter the same IP address for the hostname/tag associated with Policy Controller Unit 1 and press the Enter key.

d Skip entering (leave blank) the optional remote hostname/tag associated with Unit 1 by pressing the Enter key.

e Enter the port number associated with the IP address for Policy Controller Unit 1 and press the Enter key.

Note: For the port number, use “443”.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.70
    Hostname   = 10.65.99.70
    Remote Tag =
    Port Num   = 443
!!WARNING!! This will result in WEBSERVER
going down (restarting) for a short time.
Continue? [Y/N]:
```

f Confirm the values you entered for the Unit 1 by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

10 Complete the following sub-steps to add a Policy Controller logically **Active** unit to the proxy.

a Add a Policy Controller active unit to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing “add_proxy_conf”
```

b Enter the IP address for the Policy Controller active unit and press the Enter key.

c Enter the same IP address for the hostname/tag associated with the active unit and press the Enter key.

d Skip entering (leave blank) the optional remote hostname/tag associated with the active unit by pressing the Enter key.

e Enter the port number associated with the IP address for Policy Controller active unit and press the Enter key.

Note: For the port number, use “443”.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.72
    Hostname   = 10.65.99.72
    Remote Tag =
    Port Num   = 443
!!WARNING!! This will result in WEBSERVER
going down (restarting) for a short time.
Continue? [Y/N]:
```

f Confirm the values you entered for the active Policy Controller unit by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

11 Complete the following sub-steps to add an entry for the CS 2000 Session Server Manager GUI to the proxy.

a From the Apache Proxy Configuration level, add the CS 2000 Session Server Manager GUI to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing “add_proxy_conf”
```

b Enter the IP address for the Policy Controller active unit and press the Enter key.

> ***Note:*** The CS 2000 Session Server Manager GUI must always be loaded from the active Policy Controller unit.

c Enter the Policy Controller tagname for the hostname/tag associated with the Policy Controller active unit and press the Enter key.

> ***Note:*** The tagname entered here must be the same one entered on both Policy Controller units when the application was installed. If the correct tagname is not entered, you will be unable to access the CS 2000 Session Server Manager GUI.

d Enter the Policy Controller tagname for the remote hostname/tag associated with the Policy Controller active unit and press the Enter key.

e Enter the port number associated with the proxy IP address for active unit's CS 2000 Session Server Manager GUI and press the Enter key.

Note: For the port number, use "8443".

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.72
    Hostname   = prov
    Remote Tag = prov
    Port Num   = 8443
!!WARNING!! This will result in WEBSERVER
going down (restarting) for a short time.
Continue? [Y/N]:
```

f Confirm the values you entered for the active unit by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

12 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

13 Exit the Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 Exit the CLI by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

15 If applicable, logout from the workstation.

At a Policy Controller command line interface (CLI)

16 Use procedure, found in this NTP to configure the SNMP trap IP address and the web proxy IP address of the Integrated EMS server on the Policy Controller.

17 The procedure is complete.

Using multiple tag names for multiple Policy Controller nodes

Multiple Policy Controller nodes (made of the active and inactive units) are allowed in the same CS-LAN network. Therefore, as a rule, you must use a different tag name for each node installed in the network. Ensure that the tag name used in the web proxy entry is the correct one for that node, based on the tag name entered when the node was installed. For assistance, match the tag name to the active unit IP addresses used in the web proxy entry to ensure a correct match. Failure to follow this rule will prevent you from accessing a node’s GUIs properly.

Reconfigure the Policy Controller BIOS

Purpose of this procedure

Use the following procedure to make changes to the BIOS settings on the Policy Controller platform hardware, when you have replaced the Policy Controller chassis with a spare and the unit does not boot properly or if you want to verify that the BIOS is properly set up.

If you are changing any settings from their default, you may need to perform this procedure on both Policy Controller units. BIOS settings for both units must match.

Limitations and restrictions

Do not use this procedure to configure a new Policy Controller node installation.

ATTENTION

Do not use this procedure on an active Policy Controller unit.

Prerequisites

Verify that there are no active alarms on the active Policy Controller unit.

CAUTION

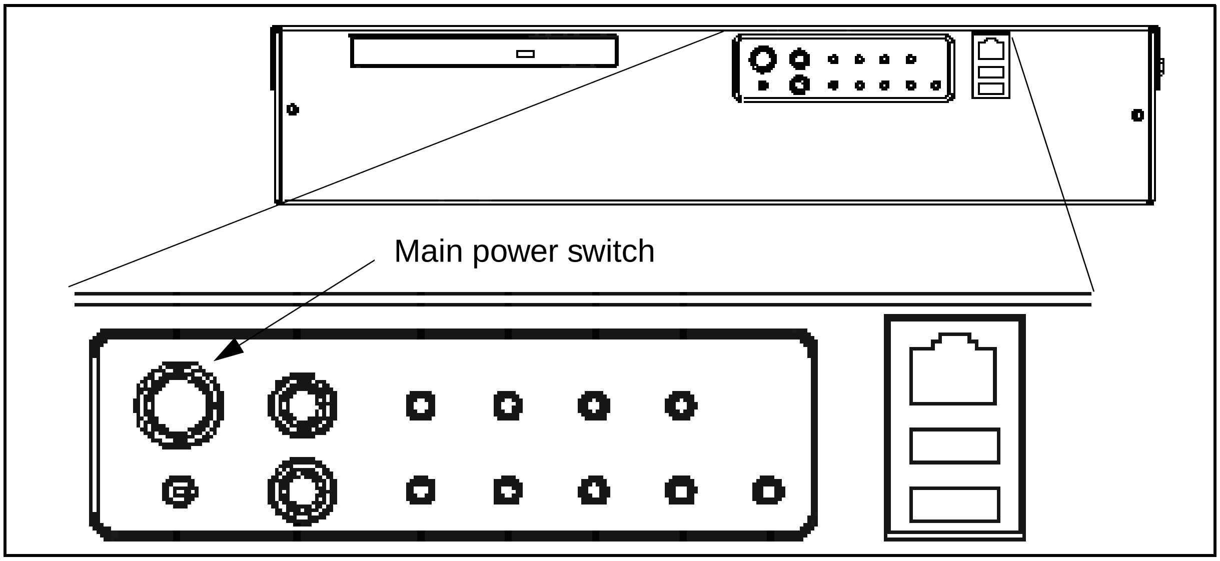
Performing this procedure on a Policy Controller node performing call processing temporarily affects fault-tolerant capability and overall system performance while the affected unit is offline.

Action

At the Policy Controller console

1 Ensure that you have a console interface connected to the rear of the Policy Controller you are reprovisioning. Your site may support other connection options.

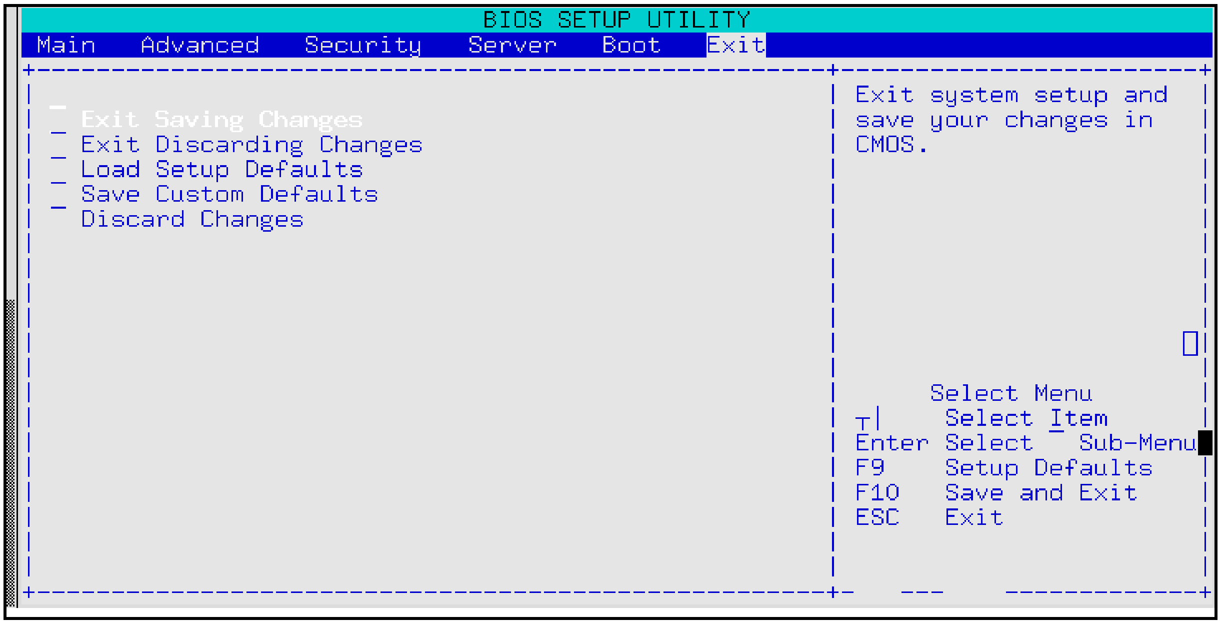
2 If necessary, power on the Policy Controller using the main power switch located on the front panel, as shown in the following figure.



The BIOS information screen appears

3 At the BIOS information screen, press the **<F2>** key to enter the BIOS setup.

The main BIOS setup screen appears.



```
                               BIOS SETUP UTILITY
 Main    Advanced    Security    Server    Boot    Exit
+-------------------------------------------------------+------------------------+
|                                                       | Exit system setup and  |
|   Exit Saving Changes                                 | save your changes in   |
|   Exit Discarding Changes                             | CMOS.                  |
|   Load Setup Defaults                                 |                        |
|   Save Custom Defaults                                |                        |
|   Discard Changes                                     |                        |
|                                                       |                        |
|                                                       |      Select Menu       |
|                                                       |       Select Item      |
|                                                       | Enter Select  Sub-Menu |
|                                                       | F9    Setup Defaults   |
|                                                       | F10   Save and Exit    |
|                                                       | ESC   Exit             |
|                                                       |                        |
+-------------------------------------------------------+------------------------+
```

4 Use the right arrow key to move to the Server menu to validate (and change if necessary) the following entries:

Asset NMI on PERR: **Disabled**

Asset NMI on SERR: **Disabled**

FRB-2 Policy: **Retry 3 times**

POST Error Pause: **Disabled**

Boot Monitoring: **5 minutes**

Boot Monitoring Policy: **Always Reset**

5 Highlight the **Console Redirection item** and press **Enter** to validate (and change if necessary) the following entries:

BIOS Redirection Port: **Serial 2 (RJ45)**

ACPI Redirection Port: **Serial 2 (RJ45)**

Baud Rate: **9600**

Flow Control: **No flow control**

Terminal Type: **VT100+**

6 Press the **ESC** key to return to the Server menu, select the **Fault Resilient Booting** menu option and press **Enter**.

7 Validate (and change if necessary) the following entries:

Late POST timeout: **Disabled**

Fault Resilient Booting: **Reset**

8 Press the **ESC** key to return to the Server menu, then press the right arrow key to move to the Boot menu.

9 Select **Boot Device Priority** and press **Enter** to validate (and change if necessary) the following settings:

1st Boot Device: **ATAPI CD-ROM**

2nd Boot Device: **Hard Drive**

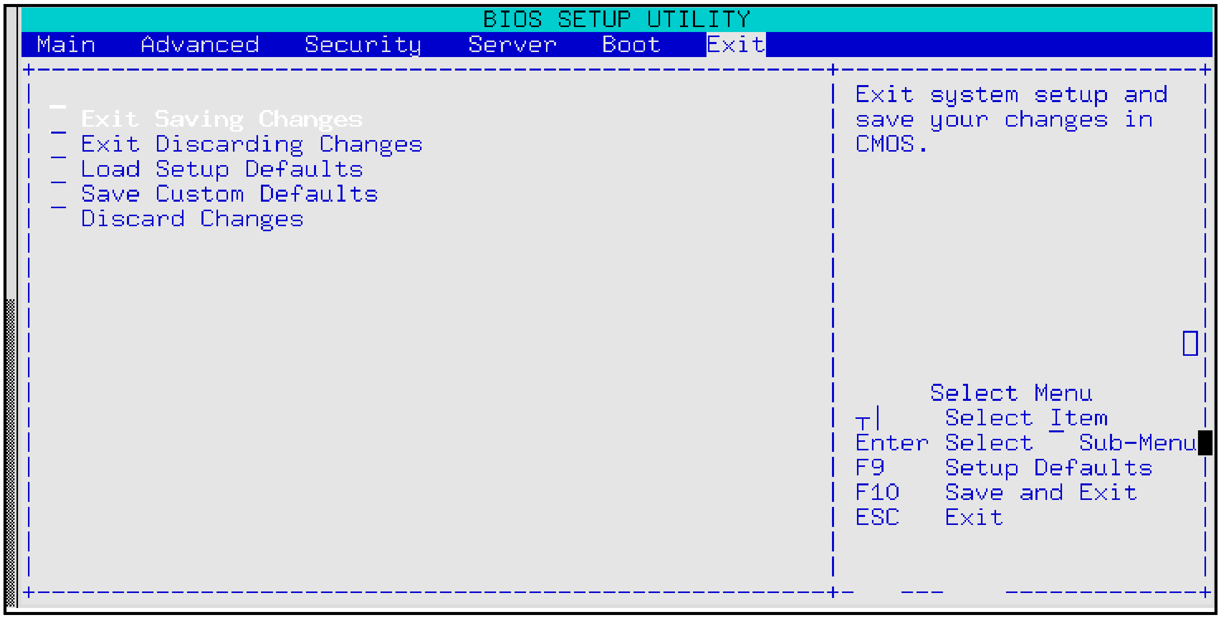
3rd/4th Boot Device: **Disabled**

10 Press the **ESC** key to return to the main menu.

11 Press the right arrow key to move to the **Exit** menu.

12 Highlight **Exit Saving Changes** and press **Enter**.

13 Type **Yes** in confirmation dialog box.



```
                              BIOS SETUP UTILITY
 Main    Advanced    Security    Server    Boot    Exit
+------------------------------------------------------+------------------------+
|                                                      | Exit system setup and  |
|  _ Exit Saving Changes                               | save your changes in   |
|  _ Exit Discarding Changes                           | CMOS.                  |
|  _ Load Setup Defaults                               |                        |
|  _ Save Custom Defaults                              |                        |
|  _ Discard Changes                                   |                        |
|                                                      |                        |
|                                                      |       Select Menu      |
|                                                      | T|     Select Item      |
|                                                      | Enter  Select  Sub-Menu|
|                                                      | F9     Setup Defaults  |
|                                                      | F10    Save and Exit   |
|                                                      | ESC    Exit            |
|                                                      |                        |
+------------------------------------------------------+------------------------+
```

The Policy Controller unit resets and begins to boot.

14 Once the unit has rebooted, use procedure to confirm that the rebooted unit has performed any necessary recoveries, returned to operational standby service and has generated no new alarms.

15 The procedure is complete.

Reprovision the Policy Controller NCGL platform software

Purpose of this procedure

Use this procedure when you need to reinstall the Policy Controller platform software from the NCGL CD/DVD software disk because of a disk drive replacement where data has been lost or because of a software upgrade failure.

Limitations and restrictions

Do not use this procedure to configure a new Policy Controller installation.

If the Policy Controller node is in operation and performing call processing activities, only perform this procedure on the standby unit.

CAUTION

This procedure destroys all data on the affected unit’s disk drives. Any critical data should be backed up.

CAUTION

Use care when executing this procedure. This procedure may cause the loss of customer data and causes all network configuration values to be reset to a default setting.

CAUTION

When using the *commish* tool to commission the NCGL platform, ensure that all values (other than hostname and IP address) entered match those on the other (mate) unit. Failure to do so may cause a service outage for SIP call traffic.

Prerequisites

Complete procedure Reconfigure the Policy Controller BIOS on page 191 to ensure that the Boot Device Priority is set so that the DVD/CDROM drive is accessed before the hard drive for booting.

Action

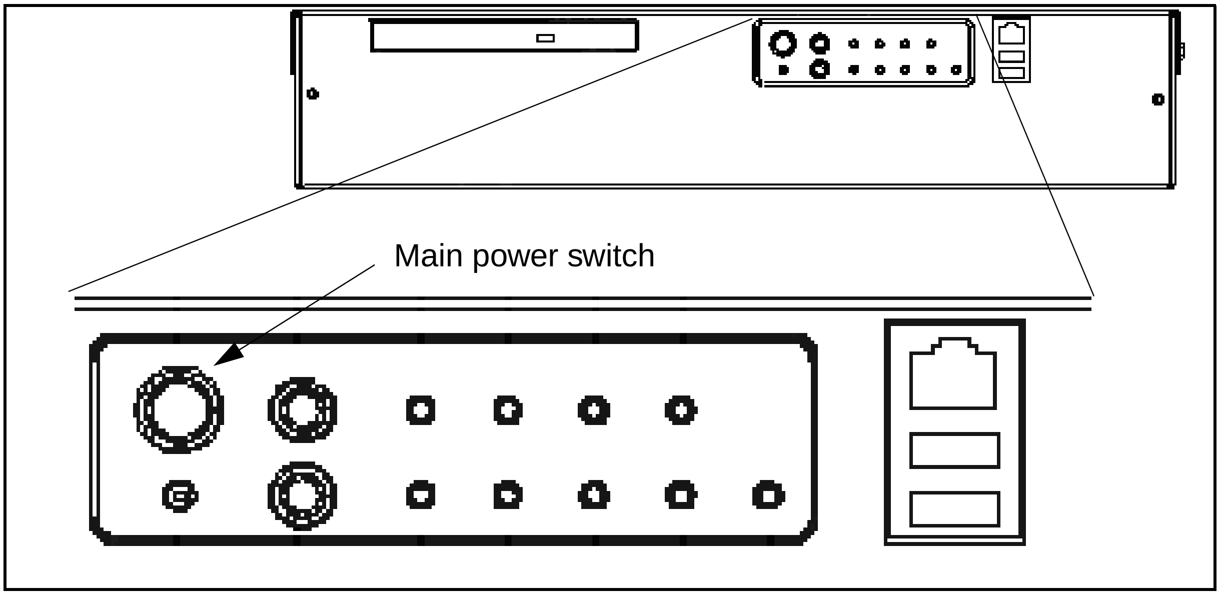
At the Policy Controller Serial Console

1 Ensure that you have a console interface connected to the rear of the Policy Controller you are reprovisioning. Your site may support other connection options. Do not use a VGA console to complete this procedure.

2 If the standby Policy Controller unit is still operating, shut it down using procedure *Halt (shutdown) a Policy Controller unit*, found in the Policy Controller Security and Administration NTP 10434-611.

> ***Note:*** This procedure does not power-off the unit.

3 If necessary, power-off the Policy Controller using the main power switch located on the front panel.



4 Power-on the Policy Controller using the main power switch located on the front panel.

The BIOS information screen appears

5 Once the BIOS information screen appears, press the **F2** key when prompted.

6 Change the boot device priority by using the right arrow key to advance to the *Boot* menu.

7 Select **Boot Device Priority** and press **Enter**.

8 Navigate down to **Hard Drive** to change the boot priority. Change the boot priority to the following settings:

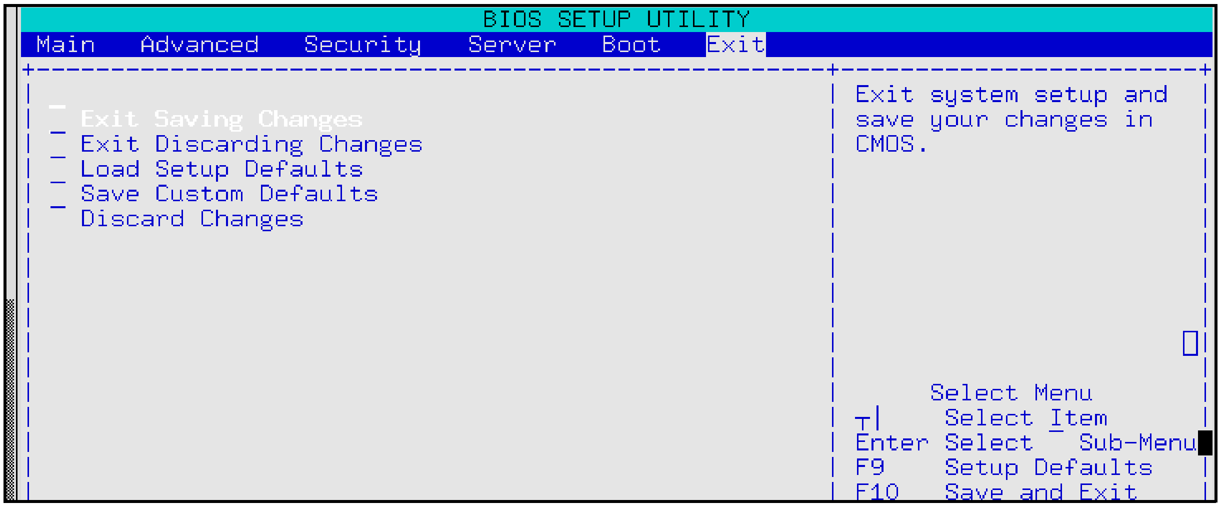
1st Boot Device: ATAPI CD-ROM (the DVD-Rom drive)

2nd Boot Device: Hard Drive

3rd/4th Boot Device: Disabled

9 Press **ESC** to return to the *Boot* menu, and then press the right arrow key to move to the *Exit* menu.

10 Highlight **Exit Saving Changes** and press **Enter**.



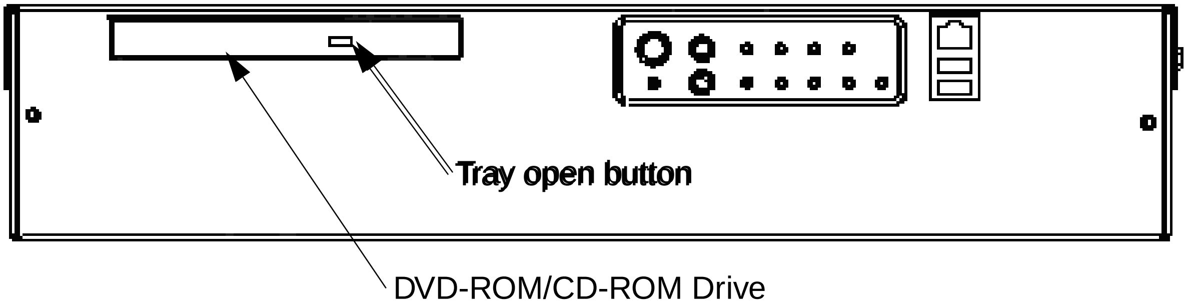
```
                          BIOS SETUP UTILITY
 Main    Advanced    Security    Server    Boot    Exit
+--------------------------------------------------------+---------------------------+
|                                                        | Exit system setup and     |
|  _ Exit Saving Changes                                 | save your changes in      |
|  _ Exit Discarding Changes                             | CMOS.                     |
|  _ Load Setup Defaults                                 |                           |
|  _ Save Custom Defaults                                |                           |
|    Discard Changes                                     |                           |
|                                                        |      Select Menu          |
|                                                        | ↑↓     Select Item        |
|                                                        | Enter  Select  Sub-Menu   |
|                                                        | F9     Setup Defaults     |
|                                                        | F10    Save and Exit      |
```

11 Type **Yes** in confirmation dialog box.

The Policy Controller resets and begins to boot.

12 Immediately press the tray open button on the DVD-ROM and insert the NCGL CD/DVD disk into the DVD-ROM drive.

Policy Controller Unit Front Panel



13 At the boot prompt, you have 5 seconds to quickly type **NUKE** and press **Enter**.

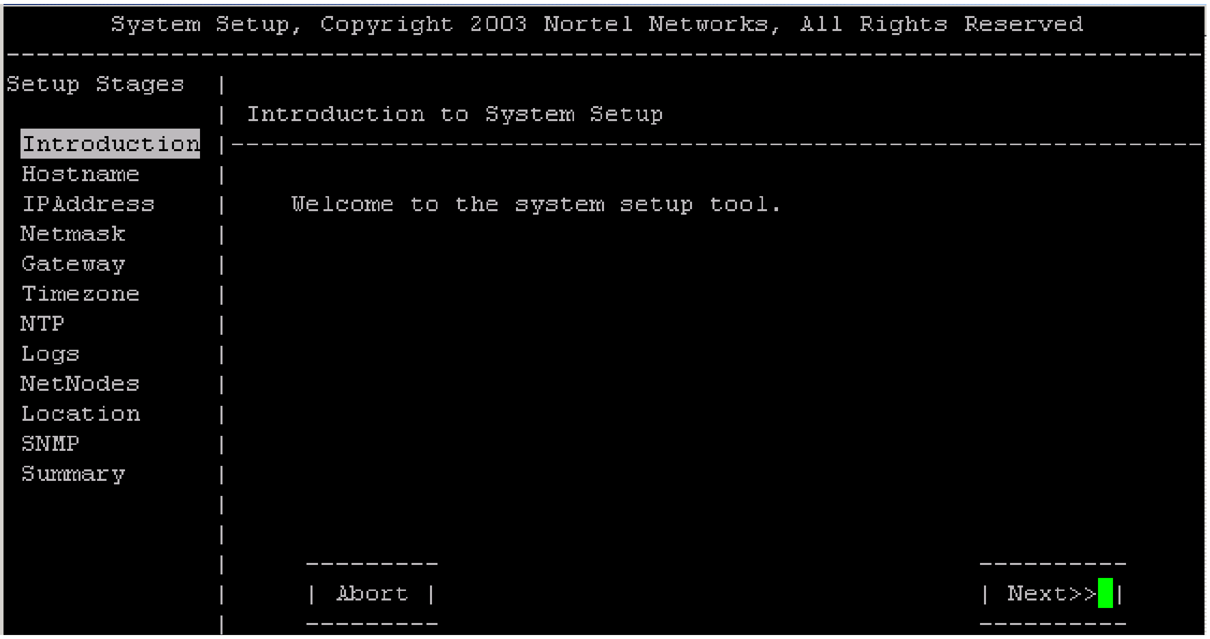
> **CAUTION**
>
> The NUKE command completely erases the drive and initiates a reboot from the CD/DVD disk.

Once the Boot prompt appears, only 5 seconds are given to type NUKE before the Server continues booting. If you miss the 5 second window, immediately power-off the unit using the power button on the front panel and return to step 4.

14 Observe that after the NUKE command has erased the disk drive, the server reboots from the CD/DVD disk.

After several seconds, the NCGL load screen appears and the boot process continues.

Once the Policy Controller completes the boot-up process, the NCGL system setup tool is displayed.

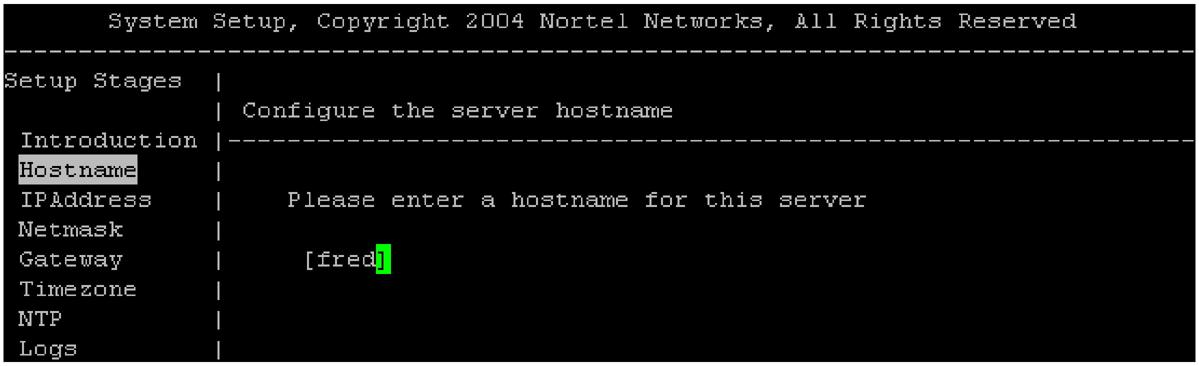


```
       System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              |  Introduction to System Setup
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |     Welcome to the system setup tool.
 Netmask      |
 Gateway      |
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
              |
              |
              |     ---------                                    ----------
              |     | Abort |                                    | Next>> |
              |     ---------                                    ----------
```

15 Position the cursor on the Next button and press **Enter**.

Note: In general, use the **Tab** key to navigate between fields on the screen and use **Enter** to select a field or entry.

The server hostname screen appears.

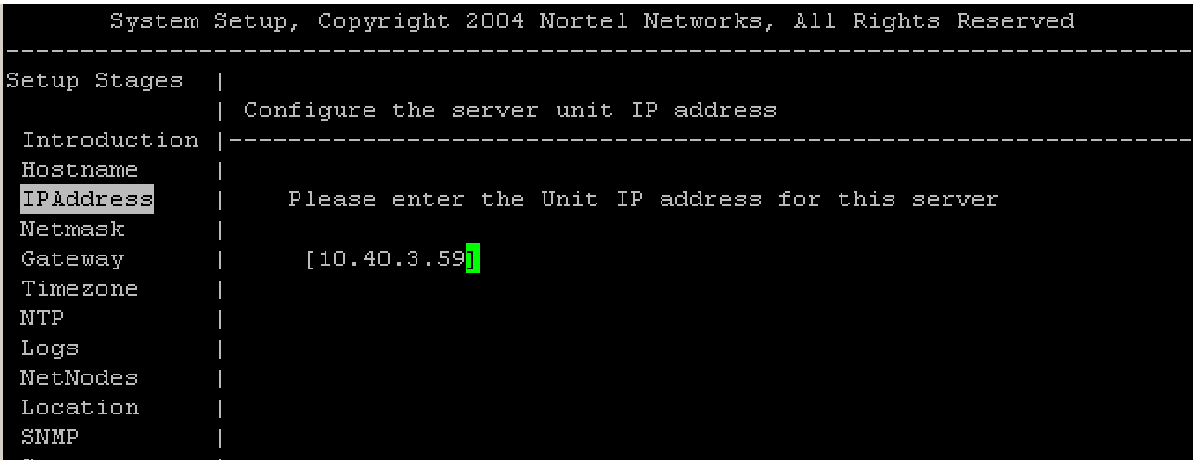


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server hostname
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a hostname for this server
 Netmask      |
 Gateway      |     [fred]
 Timezone     |
 NTP          |
 Logs         |
```

16 If applicable, enter a hostname for this Policy Controller unit using up to 60 alphanumeric characters. Hyphens, underscores are allowed. Periods are not allowed.

17 Position the cursor on the **Next** button and press **Enter**.

The IP address configuration screen appears.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server unit IP address
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter the Unit IP address for this server
 Netmask      |
 Gateway      |     [10.40.3.59]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
```

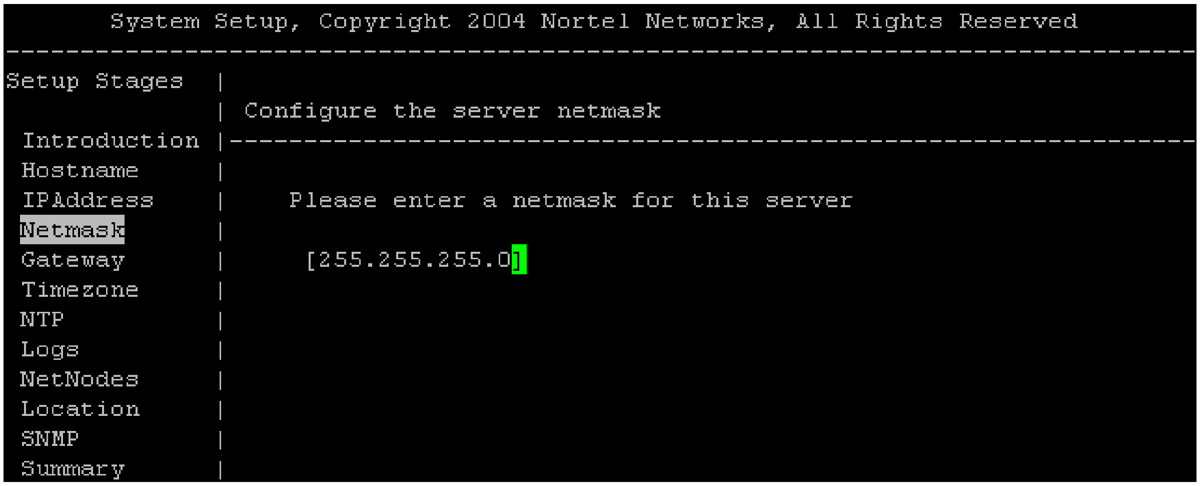
18 If applicable, enter an IP address for this Policy Controller in the following format:

`10.40.102.112`

Note: If necessary, contact your site Network Administrator to acquire the correct IP addresses used in this procedure.

19 Position the cursor on the **Next** button and press **Enter**.

The server netmask configuration screen appears.



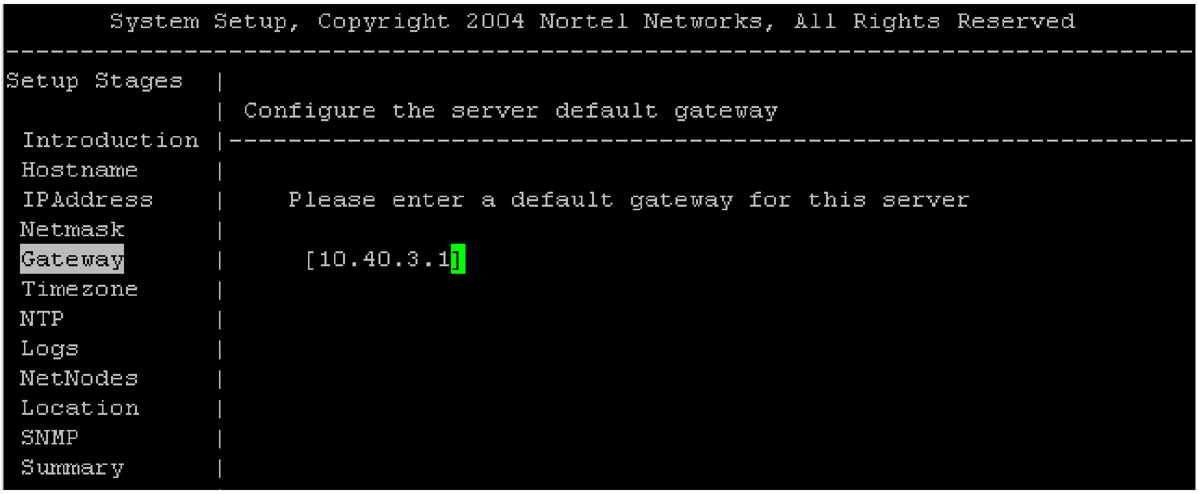
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server netmask
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a netmask for this server
 Netmask      |
 Gateway      |     [255.255.255.0]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
```

20 If applicable, enter the netmask in the format:

`255.255.255.0`

21 Position the cursor on the **Next** button and press **Enter**.

The server default gateway configuration screen appears.

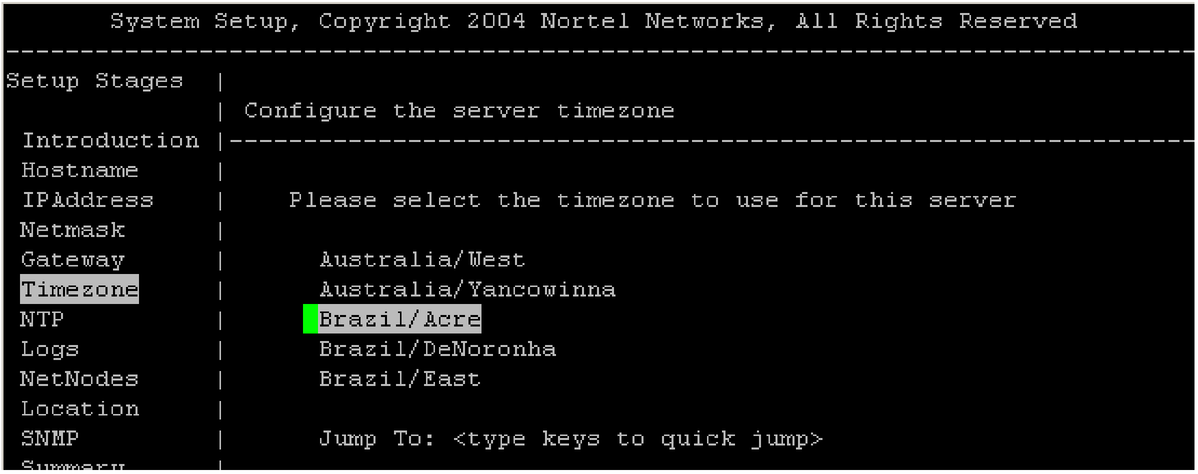


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server default gateway
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a default gateway for this server
 Netmask      |
 Gateway      |     [10.40.3.1]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
```

22 If applicable, enter the IP address of the server default gateway.

23 Position the cursor on the **Next** button and press **Enter**.

The time zone configuration screen appears.



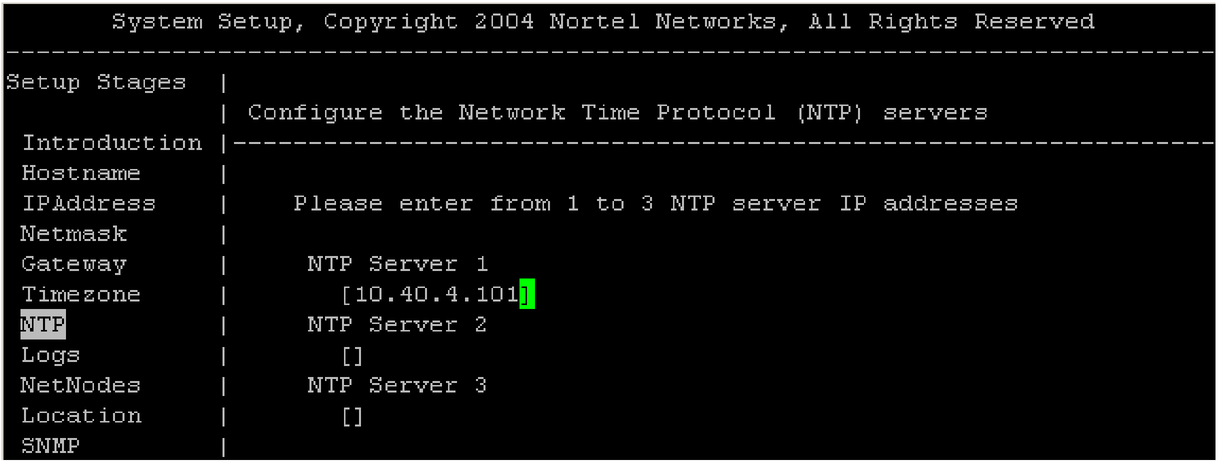
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Setup Stages    |
                | Configure the server timezone
 Introduction   |----------------------------------------------------------------
 Hostname       |
 IPAddress      |    Please select the timezone to use for this server
 Netmask        |
 Gateway        |      Australia/West
 Timezone       |      Australia/Yancowinna
 NTP            |      Brazil/Acre
 Logs           |      Brazil/DeNoronha
 NetNodes       |      Brazil/East
 Location       |
 SNMP           |      Jump To: <type keys to quick jump>
 Summary        |
```

24 If applicable, use the up/down arrow keys to select the correct time zone, or type lower case characters on the keyboard to allow a quick jump to a time zone location in the list.

Note: The quick jump is case sensitive.

25 Position the cursor on the **Next** button and press **Enter**.

The network time protocol (NTP) configuration screen appears.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Setup Stages    |
                | Configure the Network Time Protocol (NTP) servers
 Introduction   |----------------------------------------------------------------
 Hostname       |
 IPAddress      |    Please enter from 1 to 3 NTP server IP addresses
 Netmask        |
 Gateway        |     NTP Server 1
 Timezone       |       [10.40.4.101]
 NTP            |     NTP Server 2
 Logs           |       []
 NetNodes       |     NTP Server 3
 Location       |       []
 SNMP           |
```

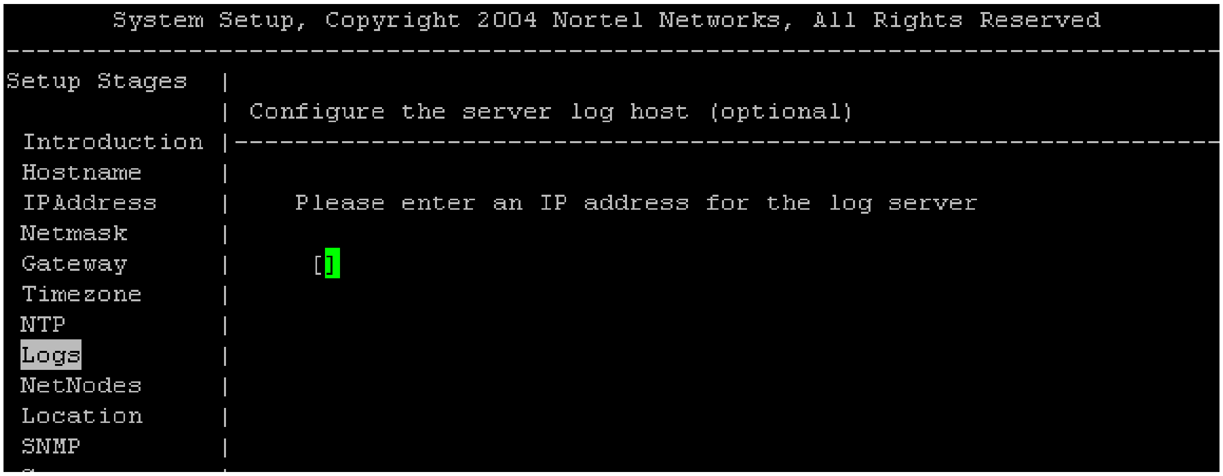
26 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

`10.40.102.112`

> ***Note:*** To be consistent with other component implementations on the CS-LAN, the IP address of the SDM/Core and Billing Manager should be used. The Core and Billing Manager are set up to communicate to the central Stratum-1 NTP server.

27 Position the cursor on the **Next** button and press **Enter**.

The log server configuration screen appears.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server log host (optional)
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter an IP address for the log server
 Netmask       |
 Gateway       |     []
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
```

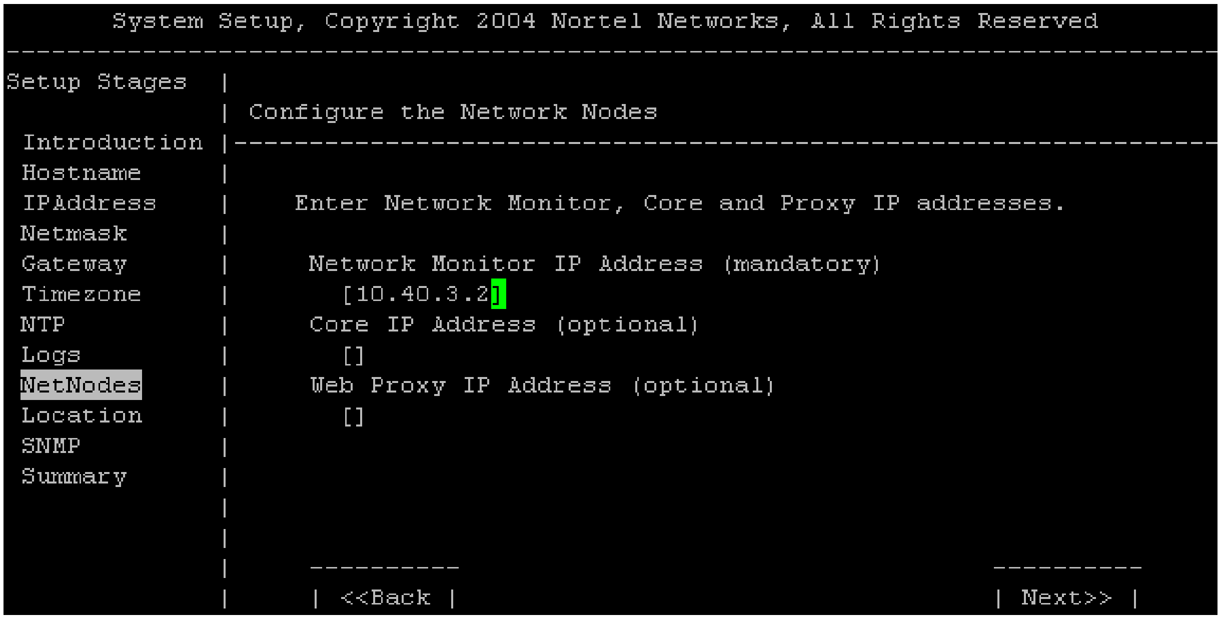
28 Enter the IP address of the log server in the following format:

`192.168.102.112`

> ***Note:*** This should be the IP address of the CS 2000 Management Tools server or another log aggregate server used in your network for collecting logs.

29 Position the cursor on the **Next** button and press **Enter**.

The Network Nodes page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Nodes
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Enter Network Monitor, Core and Proxy IP addresses.
 Netmask       |
 Gateway       |     Network Monitor IP Address (mandatory)
 Timezone      |       [10.40.3.2]
 NTP           |     Core IP Address (optional)
 Logs          |       []
 NetNodes      |     Web Proxy IP Address (optional)
 Location      |       []
 SNMP          |
 Summary       |
               |
               |
               |     ----------                                ----------
               |     | <<Back |                                | Next>> |
```

30 Use the following sub-steps to complete the Network Nodes screen:

a For networks using sites using PP8600 CS-LAN with VRRP running, the Network Monitor should be the VRRP IP address (the default gateway). Consult your site network engineering guidelines to determine the correct IP address of this gateway, then enter the Network Monitor IP address in the following format:

```
10.40.102.112
```

b Do not enter any address values for the Core IP addresses field. This field must remain blank.

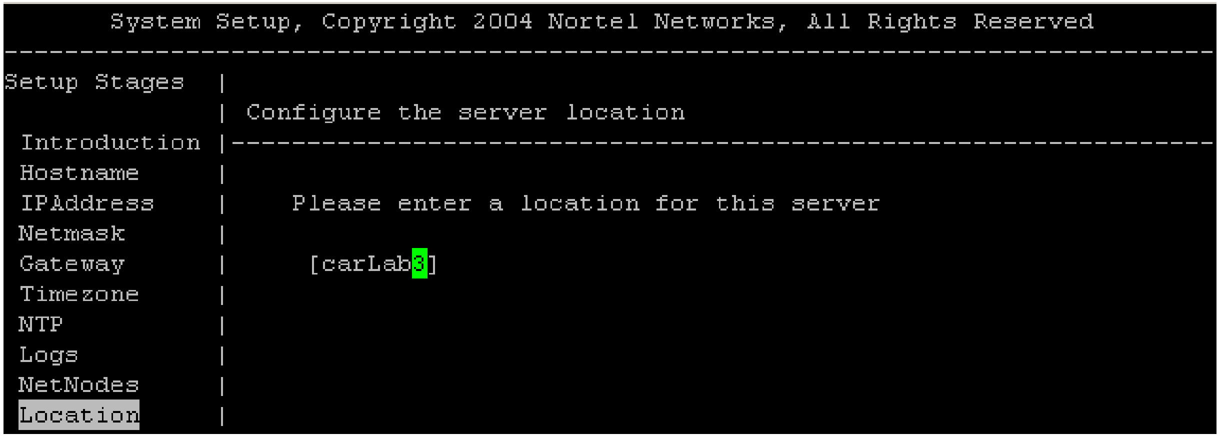
c Enter the IP address of the SSPFS server for the Web Proxy IP Address in the following format:

```
10.40.102.112
```

Note: Use the IP address of the SSPFS platform residing on the CS 2000 Management Tools server.

31 Position the cursor on the **Next** button and press **Enter**.

The server location page is displayed.

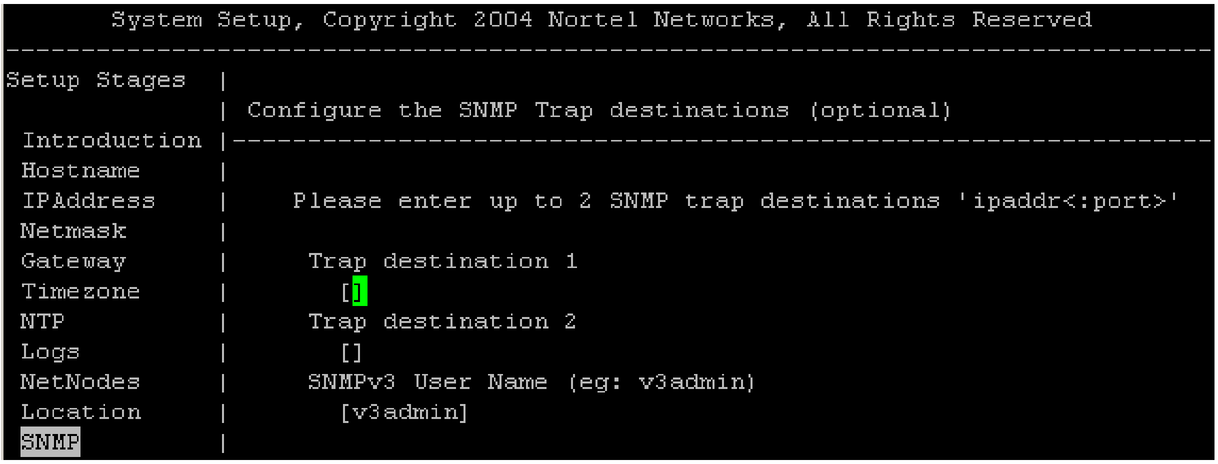


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server location
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a location for this server
 Netmask      |
 Gateway      |     [carLab3]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
```

32 If applicable, enter a location identifier for this Policy Controller location.

33 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the SNMP Trap destinations (optional)
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter up to 2 SNMP trap destinations 'ipaddr<:port>'
 Netmask      |
 Gateway      |     Trap destination 1
 Timezone     |       []
 NTP          |     Trap destination 2
 Logs         |       []
 NetNodes     |     SNMPv3 User Name (eg: v3admin)
 Location     |       [v3admin]
 SNMP         |
```

34 If applicable, enter the IP address of the Integrated EMS server for Trap destination 1 in the following format:

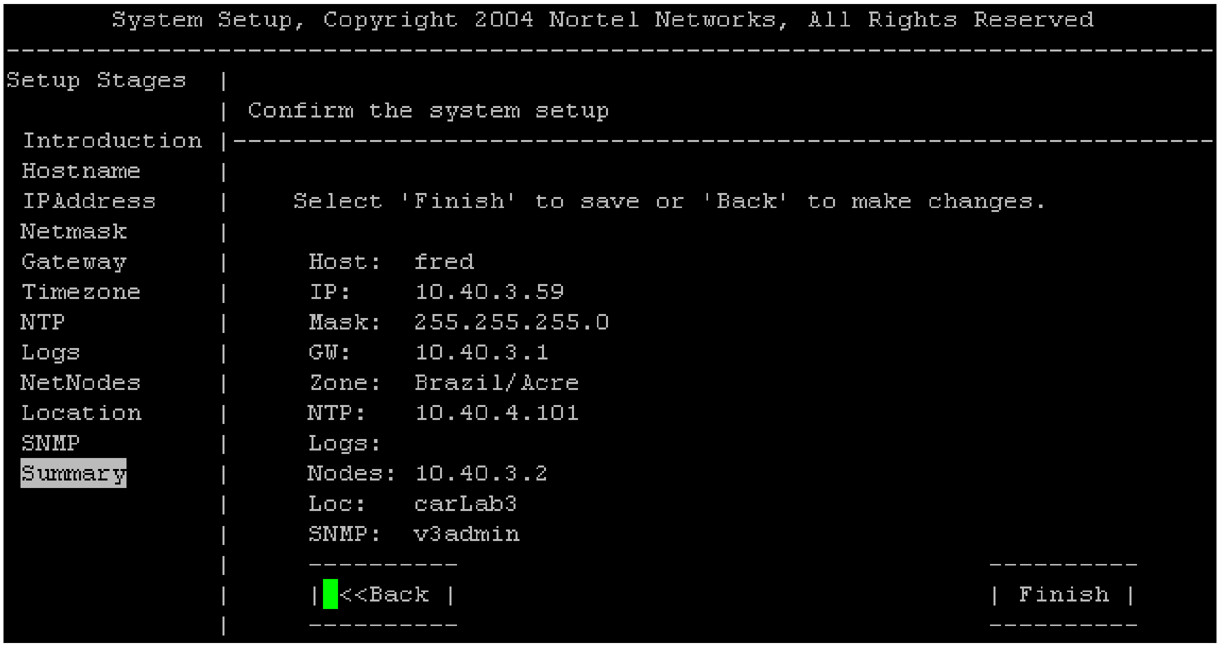
`10.40.102.112`

Note 1: Use the IP address of the Integrated EMS application residing on the CS 2000 Management Tools server.

Note 2: Do not enter values for the Trap destination2 and SNMPv3 User Name fields.

35 Position the cursor on the **Next** button and press **Enter**.

The summary screen is displayed



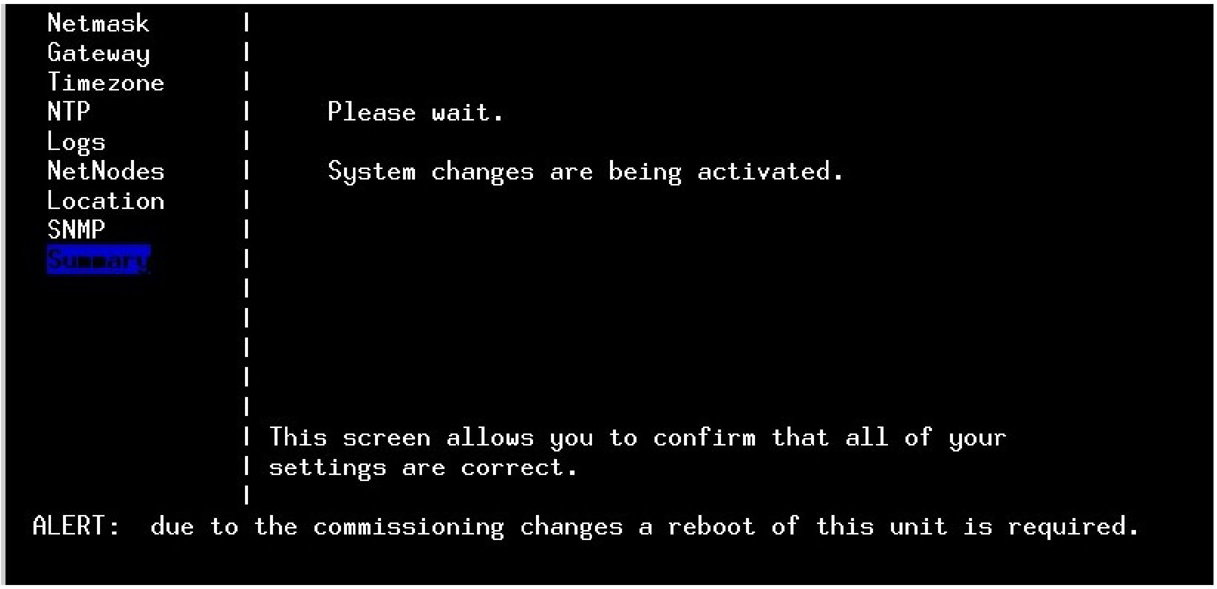
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               |  Confirm the system setup
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |     Select 'Finish' to save or 'Back' to make changes.
 Netmask       |
 Gateway       |      Host:   fred
 Timezone      |      IP:     10.40.3.59
 NTP           |      Mask:   255.255.255.0
 Logs          |      GW:     10.40.3.1
 NetNodes      |      Zone:   Brazil/Acre
 Location      |      NTP:    10.40.4.101
 SNMP          |      Logs:
 Summary       |      Nodes:  10.40.3.2
               |      Loc:    carLab3
               |      SNMP:   v3admin
               |      ----------                                       ----------
               |      | <<Back |                                       | Finish |
               |      ----------                                       ----------
```

36 Eject the CD/DVD disk from the DVD drive. You must eject the disk before finishing with the commish tool to ensure that the unit boots from the hard drive and not the DVD drive.

37 Position the cursor on the **Finish** button and press **Enter**.

The system configures itself based upon the supplied settings.

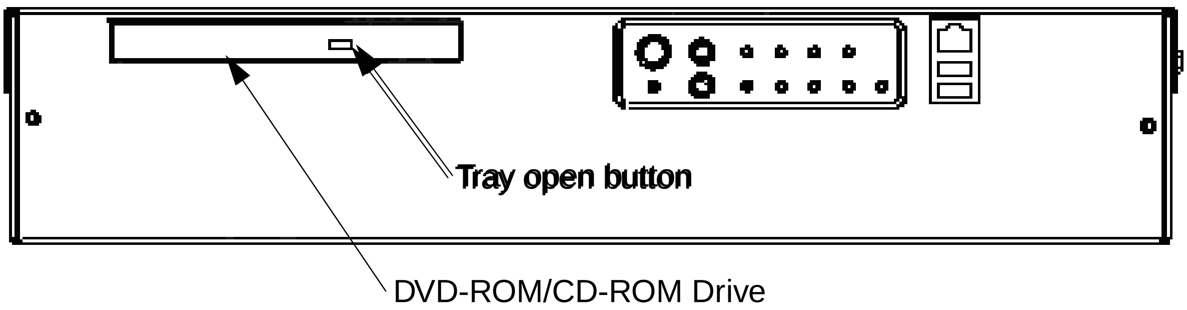
After this procedure is completed, the unit automatically reboots. Allow the unit to boot normally.



```
  Netmask      |
  Gateway      |
  Timezone     |
  NTP          |     Please wait.
  Logs         |
  NetNodes     |     System changes are being activated.
  Location     |
  SNMP         |
  Summary      |
               |
               |
               |
               |
               |
               | This screen allows you to confirm that all of your
               | settings are correct.
               |
 ALERT:  due to the commissioning changes a reboot of this unit is required.
```

38 Press the tray open button on the DVD-ROM drive and remove the NCGL CD/DVD disk.

Policy Controller Front Panel



39 Verify that the all of the commish settings made for this unit match those of the mate unit.

40 The procedure is complete.

Modify NCGL platform provisioning

Purpose of this procedure

Use this procedure when you need to modify the NGCL provisioning values that were set up during initial commissioning activities. Provisioning values that can be changed using this procedure include:

- change the IP address of the proxy server (default gateway)
- change the IP address or netmask of the Policy Controller
- change the hostname of the Policy Controller
- change the time zone setting for the Policy Controller
- change the IP addresses of the network time protocol servers
- change the IP address of the log server to spool log files to
- change the SSPFS web proxy server address
- change the IP addresses to allow access by the Integrated EMS

Limitations and restrictions

ATTENTION

This procedure must be performed on both Policy Controller units; however, because a reboot and SwAct of the Policy Controller units is required in order for changes made to take effect, you can only perform this procedure on the standby Policy Controller unit.

Prerequisites

Before performing this procedure, the Policy Controller unit must first be jammed using procedure Inhibit a system SwAct (Jam), found in NTP *Policy Controller Security and Administration*, NN10434-611.

Ensure the console interface is connected to the rear of the Policy Controller for which you are modifying provisioning.

Action

At a Policy Controller command line interface (CLI)

1 Log onto the standby Policy Controller unit.

2 At the prompt change to the root user by typing

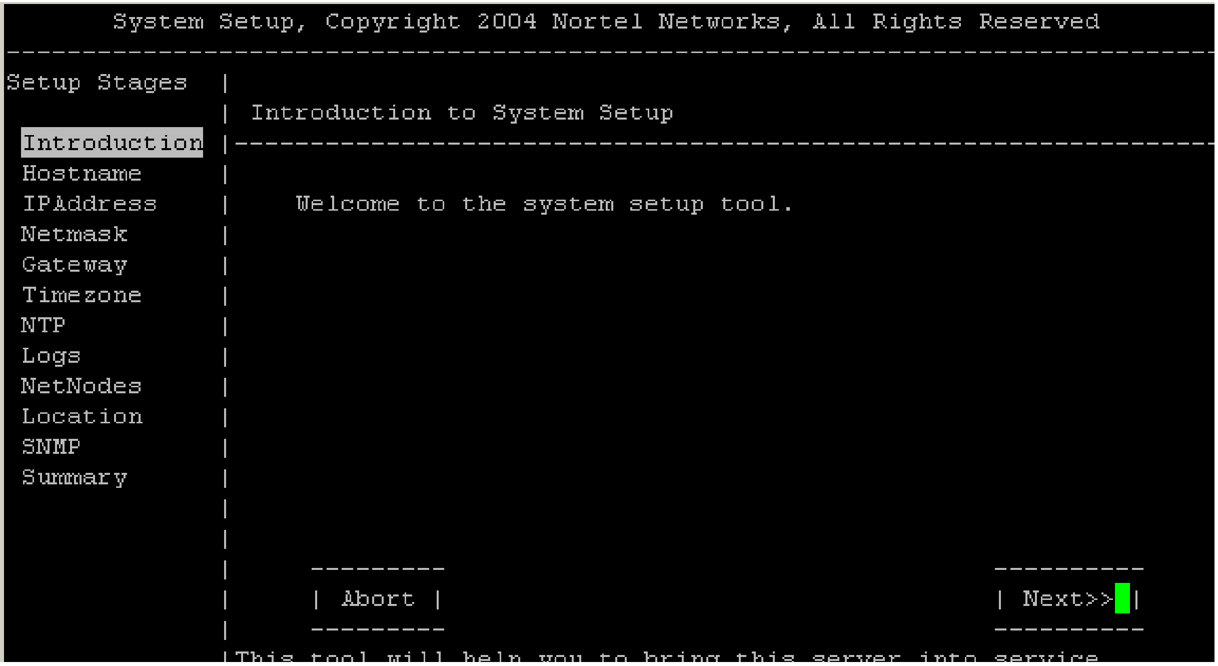
```
$ su - root
```

and pressing **Enter**.

3 Start the platform commissioning tool by typing

```
commish
```

After a few seconds the Introduction screen is displayed.



```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
---------------------------------------------------------------------------------
Setup Stages  |
              | Introduction to System Setup
 Introduction |------------------------------------------------------------------
 Hostname     |
 IPAddress    |    Welcome to the system setup tool.
 Netmask      |
 Gateway      |
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
              |
              |
              |     ---------                                          ----------
              |     | Abort |                                          | Next>> |
              |     ---------                                          ----------
              |This tool will help you to bring this server into service
```

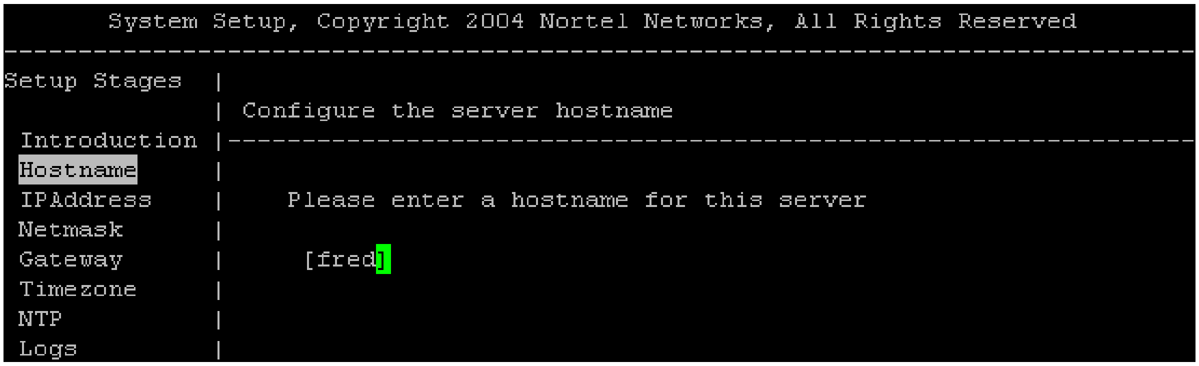
If the commish tool does not start and you receive the following message, complete procedure “Invoke a maintenance SwAct of the Policy Controller platform” in the Policy Controller Security and Administration NTP, NN10434-611.

```
Commissioning start:
   Local unit 0 is active, enabled.
   Mate unit 1 is standby, enabled.
Aborted: This unit is active. Recommissioning
cannot be performed on the active unit. When
appropriate, switch unit activity and try again.
```

4 Position the cursor on the Next button and press **Enter**.

> ***Note:*** In general, use the **Tab** key to navigate between fields on the screen and use **Enter** to select a field or entry.

The server hostname screen appears.

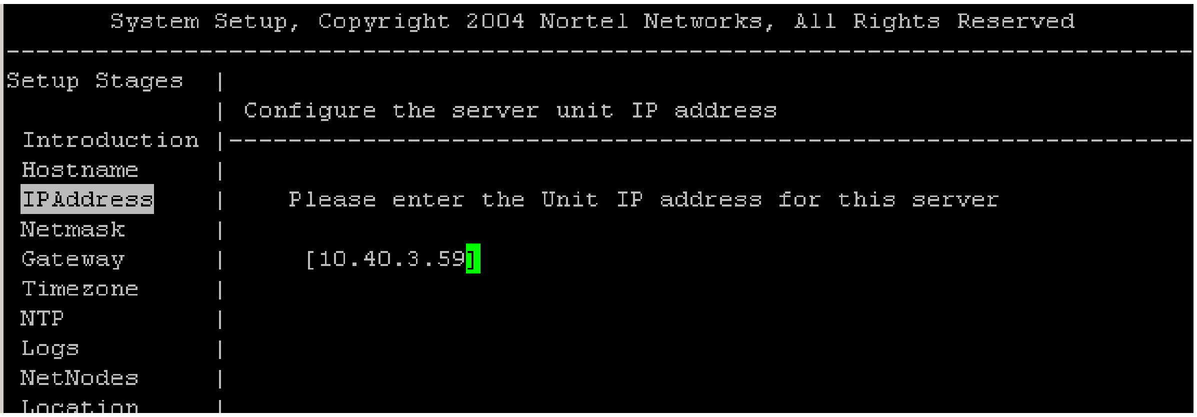


```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server hostname
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a hostname for this server
 Netmask      |
 Gateway      |     [fred]
 Timezone     |
 NTP          |
 Logs         |
```

5 If applicable, enter a hostname for this Policy Controller unit using up to 60 alphanumeric characters. Hyphens, underscores are allowed. Periods are not allowed.

6 Position the cursor on the **Next** button and press **Enter**.

The IP address configuration screen appears.



```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server unit IP address
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter the Unit IP address for this server
 Netmask      |
 Gateway      |     [10.40.3.59]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
```

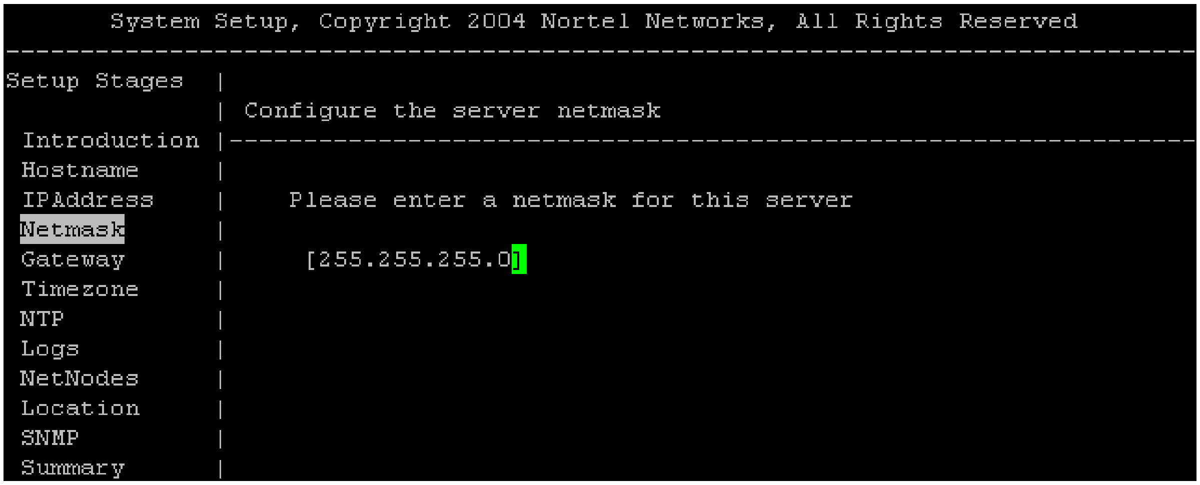
7 If applicable, enter an IP address for this Policy Controller in the following format:

`192.168.102.112`

> ***Note:*** If necessary, contact your site Network Administrator to acquire the correct IP addresses used in this procedure.

8 Position the cursor on the **Next** button and press **Enter**.

The server netmask configuration screen appears.



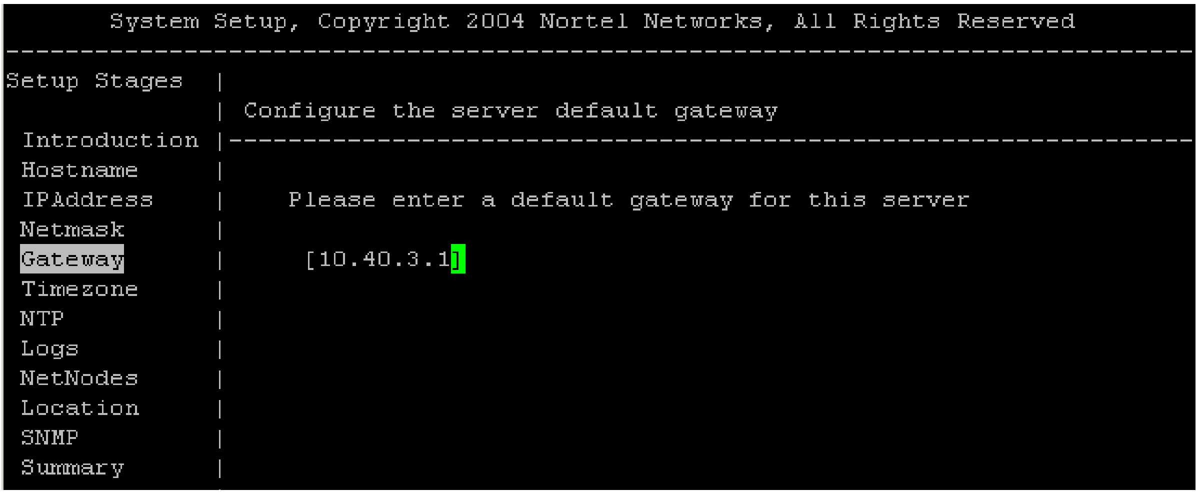
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages    |
                | Configure the server netmask
 Introduction   |-----------------------------------------------------------------
 Hostname       |
 IPAddress      |    Please enter a netmask for this server
 Netmask        |
 Gateway        |     [255.255.255.0]
 Timezone       |
 NTP            |
 Logs           |
 NetNodes       |
 Location       |
 SNMP           |
 Summary        |
```

9 If applicable, enter the netmask in the format:

`255.255.255.0`

10 Position the cursor on the **Next** button and press **Enter**.

The server default gateway configuration screen appears.

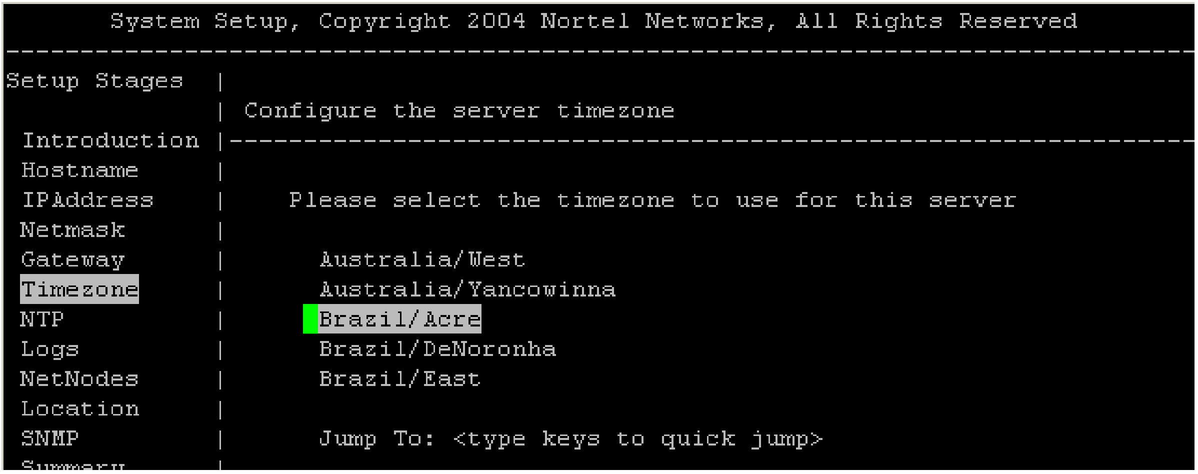


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages    |
                | Configure the server default gateway
 Introduction   |-----------------------------------------------------------------
 Hostname       |
 IPAddress      |    Please enter a default gateway for this server
 Netmask        |
 Gateway        |     [10.40.3.1]
 Timezone       |
 NTP            |
 Logs           |
 NetNodes       |
 Location       |
 SNMP           |
 Summary        |
```

11 If applicable, enter the IP address of the server default gateway.

12 Position the cursor on the **Next** button and press **Enter**.

The time zone configuration screen appears.



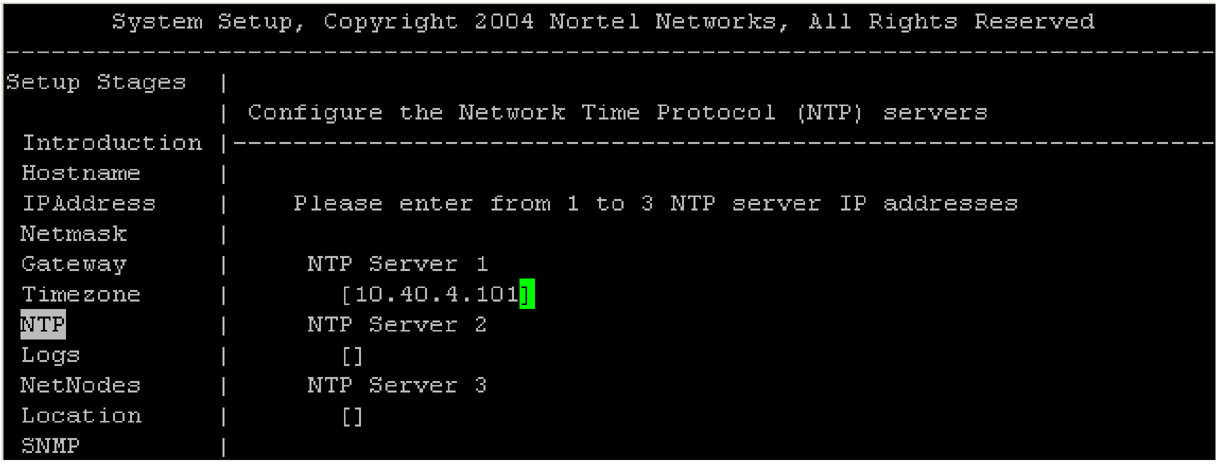
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server timezone
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please select the timezone to use for this server
 Netmask      |
 Gateway      |      Australia/West
 Timezone     |      Australia/Yancowinna
 NTP          |      Brazil/Acre
 Logs         |      Brazil/DeNoronha
 NetNodes     |      Brazil/East
 Location     |
 SNMP         |      Jump To: <type keys to quick jump>
 Summary      |
```

13 If applicable, use the up/down arrow keys to select the correct time zone, or type lower case characters on the keyboard to allow a quick jump to a time zone location in the list.

Note: The quick jump is case sensitive.

14 Position the cursor on the **Next** button and press **Enter**.

The network time protocol (NTP) configuration screen appears.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the Network Time Protocol (NTP) servers
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter from 1 to 3 NTP server IP addresses
 Netmask      |
 Gateway      |     NTP Server 1
 Timezone     |       [10.40.4.101]
 NTP          |     NTP Server 2
 Logs         |       []
 NetNodes     |     NTP Server 3
 Location     |       []
 SNMP         |
```

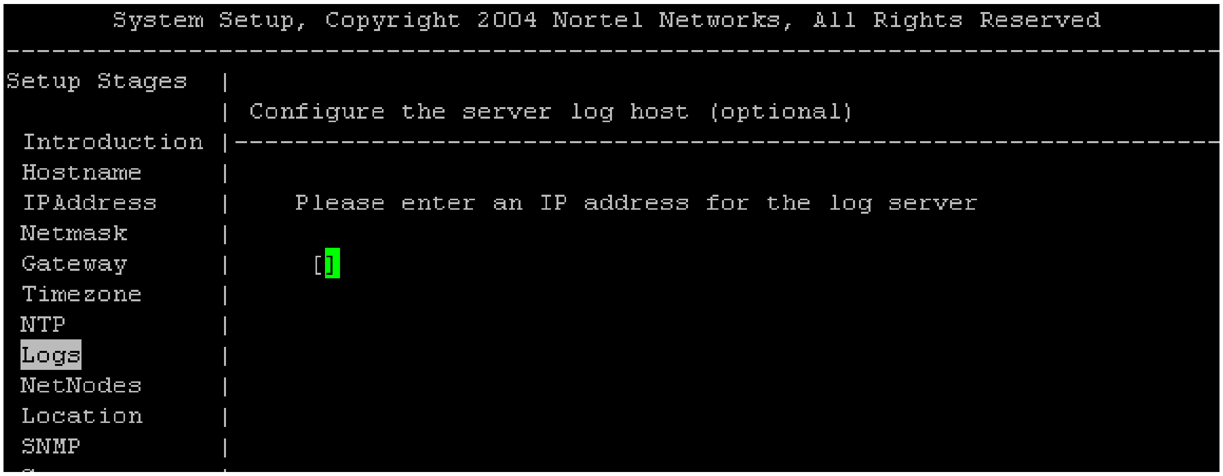
15 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

`192.168.102.112`

> ***Note:*** To be consistent with other component implementations on the CS-LAN, the IP address of the SDM/ Core and Billing Manager should be used. The SDM/ Core and Billing Manager are set up to communicate to the central Stratum-1 NTP server.

16 Position the cursor on the **Next** button and press **Enter**.

The log server configuration screen appears.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server log host (optional)
 Introduction  |----------------------------------------------------------------
 Hostname      |
 IPAddress     |   Please enter an IP address for the log server
 Netmask       |
 Gateway       |     []
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
```

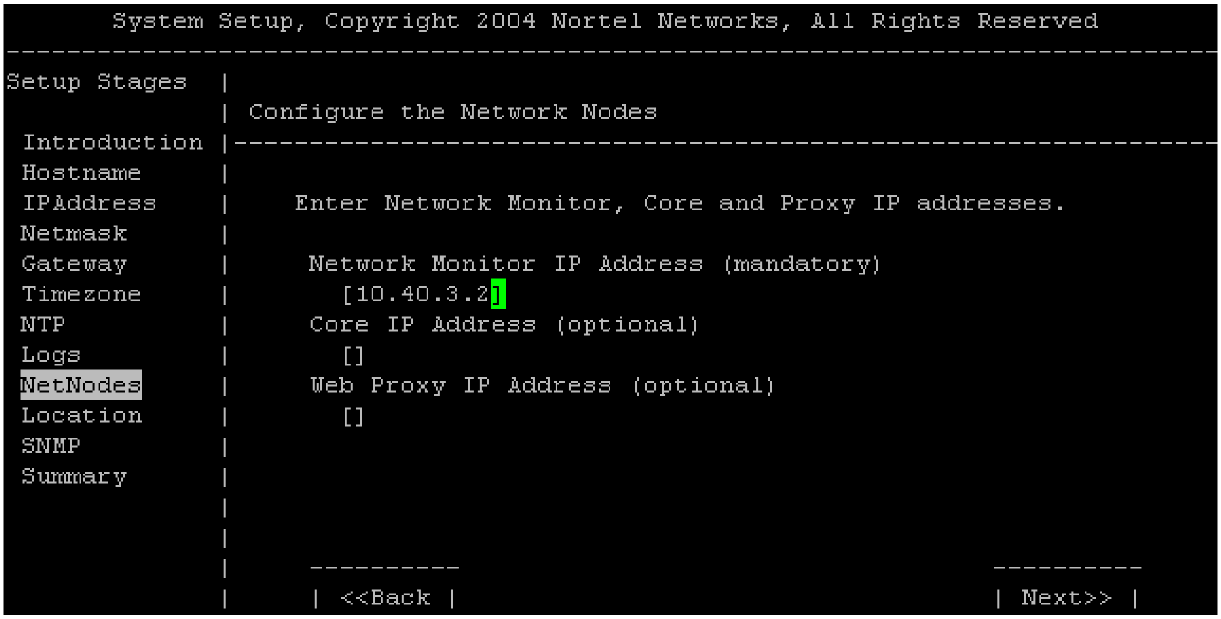
17 Enter the IP address of the log server in the following format:

`192.168.102.112`

> ***Note:*** This should be the IP address of the CS 2000 Management Tools server or it may be another log aggregate server used in your network for collecting logs.

18 Position the cursor on the **Next** button and press **Enter**.

The Network Nodes page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Nodes
 Introduction  |----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Enter Network Monitor, Core and Proxy IP addresses.
 Netmask       |
 Gateway       |     Network Monitor IP Address (mandatory)
 Timezone      |       [10.40.3.2]
 NTP           |     Core IP Address (optional)
 Logs          |       []
 NetNodes      |     Web Proxy IP Address (optional)
 Location      |       []
 SNMP          |
 Summary       |
               |
               |
               |     ----------                                  ----------
               |     | <<Back |                                  | Next>> |
```

19 Use the following sub-steps to complete the Network Nodes screen:

a For networks using sites using PP8600 CS-LAN with VRRP running, the Network Monitor should be the VRRP IP address (the default gateway). Consult your site network engineering guidelines to determine the correct IP address of this gateway, then enter the Network Monitor IP address in the following format:

`192.168.102.112`

b Do not enter any address values for the Core IP addresses field. This field must remain blank.

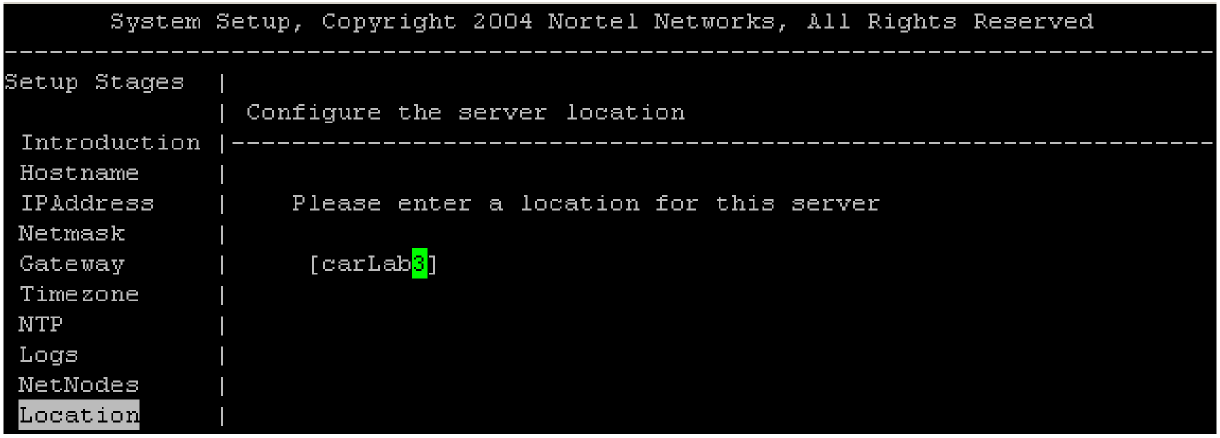
c Enter the IP address of the SSPFS server for the Web Proxy IP Address in the following format:

`192.168.102.112`

Note: Use the IP address of the SSPFS platform residing on the CS 2000 Management Tools server.

20 Position the cursor on the **Next** button and press **Enter**.

The server location page is displayed.

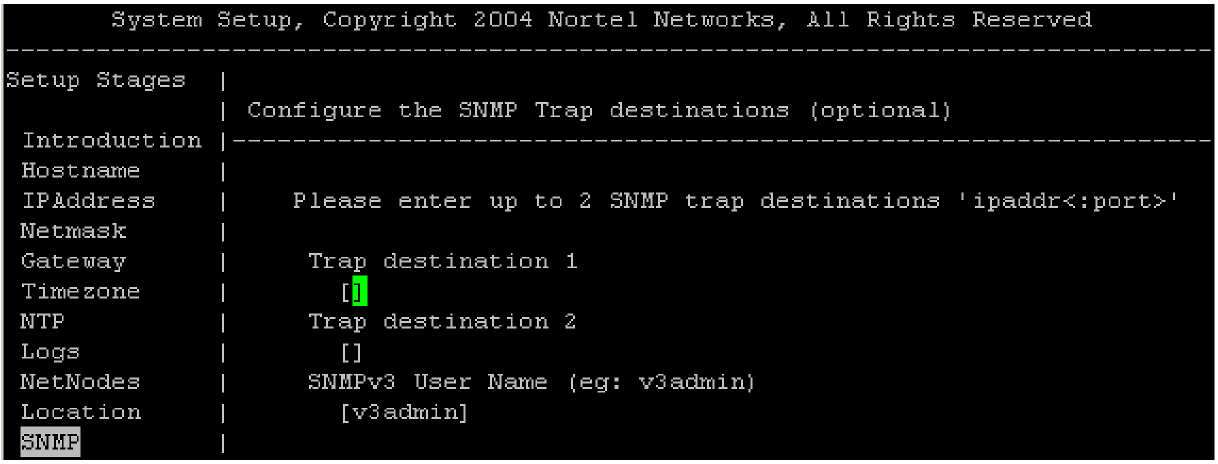


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server location
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a location for this server
 Netmask      |
 Gateway      |     [carLab3]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
```

21 If applicable, enter a location identifier for this Policy Controller location.

22 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the SNMP Trap destinations (optional)
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter up to 2 SNMP trap destinations 'ipaddr<:port>'
 Netmask      |
 Gateway      |     Trap destination 1
 Timezone     |       []
 NTP          |     Trap destination 2
 Logs         |       []
 NetNodes     |     SNMPv3 User Name (eg: v3admin)
 Location     |       [v3admin]
 SNMP         |
```

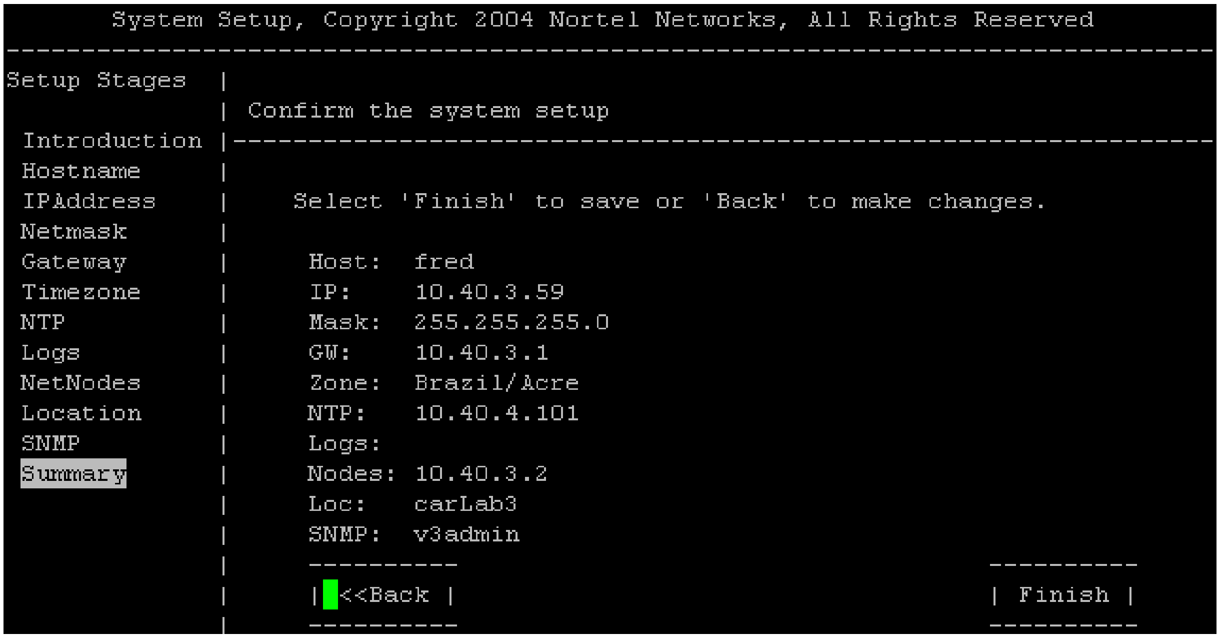
23 If applicable, enter the IP address of the Integrated EMS server for Trap destination 1 in the following format:

`192.168.102.112`

> ***Note 1:*** Use the IP address of the Integrated EMS application residing on the CS 2000 Management Tools server.
>
> ***Note 2:*** Do not enter values for the Trap destination2 and SNMPv3 User Name fields.

24 Position the cursor on the **Next** button and press **Enter**.

The summary screen is displayed

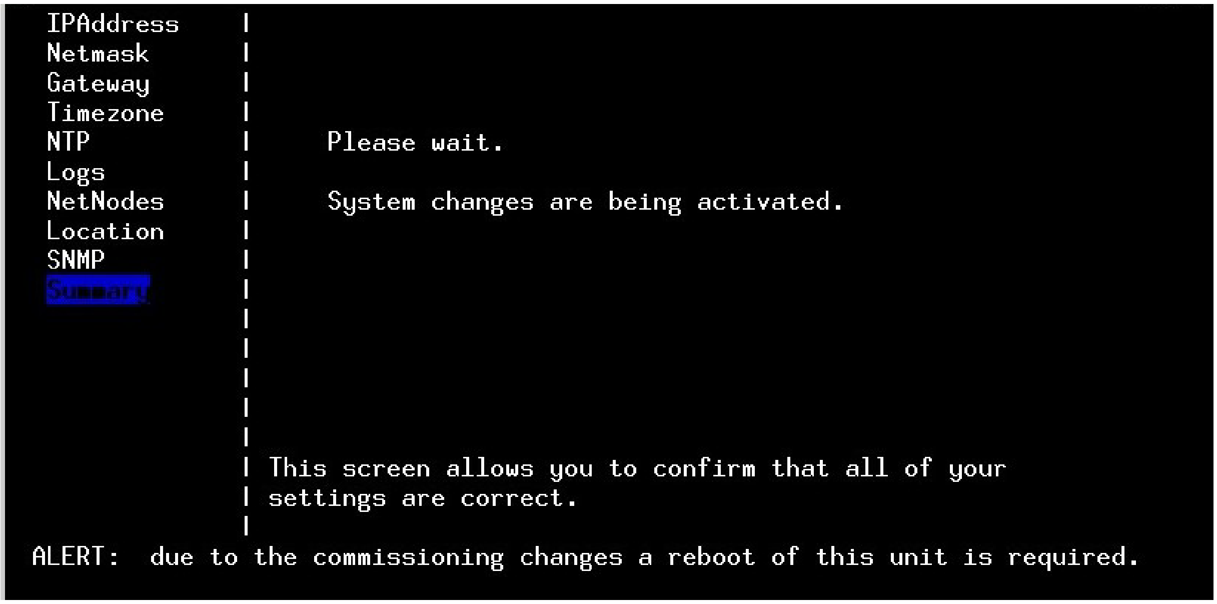


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Confirm the system setup
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Select 'Finish' to save or 'Back' to make changes.
 Netmask       |
 Gateway       |     Host:  fred
 Timezone      |     IP:    10.40.3.59
 NTP           |     Mask:  255.255.255.0
 Logs          |     GW:    10.40.3.1
 NetNodes      |     Zone:  Brazil/Acre
 Location      |     NTP:   10.40.4.101
 SNMP          |     Logs:
 Summary       |     Nodes: 10.40.3.2
               |     Loc:   carLab3
               |     SNMP:  v3admin
               |     ----------                                    ----------
               |     | <<Back |                                    | Finish |
               |     ----------                                    ----------
```

25 Position the cursor on the **Finish** button and press **Enter**.

The system configures itself based upon the supplied settings.

After this procedure is completed, the unit may automatically reboot. Allow the unit to boot normally.



```
  IPAddress    |
  Netmask      |
  Gateway      |
  Timezone     |
  NTP          |     Please wait.
  Logs         |
  NetNodes     |     System changes are being activated.
  Location     |
  SNMP         |
  Summary      |
               |
               |
               |
               |
               |
               | This screen allows you to confirm that all of your
               | settings are correct.
               |
 ALERT:  due to the commissioning changes a reboot of this unit is required.
```

26 After the unit has rebooted, verify the Policy Controller unit is unjammed using procedure Enable a system SwAct (Unjam), found in NTP *Policy Controller Security and Administration*, NN10434-611.

27 SwAct the units by performing procedure Invoke a maintenance SwAct of the Policy Controller platform found in NTP *Policy Controller Security and Administration*, NN10434-611.

28 Repeat this procedure on the other Policy Controller unit (now in standby).

29 Use procedure View the operational status of a Policy Controller NCGL platform in NTP *Upgrading the Policy Controller*, NN10431-461 to verify that both units are in operational service and that no new alarms have been raised.

30 The procedure is complete.