Gateway Controller Configuration Management

What's new in SN08

The following release SN08 features are documented in this NTP. In addition, other changes and enhancements to this NTP for SN08 are noted in this list.

- A00007007 - Session border controller/application layer gateway
- A00007120 - Packet Media Anchor for DPT

  Note: The Packet Media Anchor device replaces the APG functionality, which has been removed in the SN07 release.

- A00007071 - 3rd Party Interop Profiles
- A00007072 - 3rd Party GW Interop Pre-provisioning
- A00007927 - SAM21 EM Enhancements from Bell Canada VO
- A00007394 - Network VCAC - GWC Call Flow
- A00007242 - SESM Support of SPC Topology
- A00007528 - Integration with Nuera 4K GW
- A00009579 - RAS-less H.323 Support
- Q00834467 - Introduction of the Get Load Files button and the drop-down menu (to select a load).
- Q01043260 - Introduction of the Statistics button under the Controller tab of the Provisioning panel (to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC).
- Two new media gateway profiles: MGCP_IAD_40 and NUERA_BTX4K

- PVG naming - The table below lists the names used for certain gateways in Carrier Voice over IP (VoIP) documentation prior to SN07 and provides the new brand names starting in SN07.

Pre-SN07 name	Brand name starting in SN07
Passport Packet Voice Gateway (PVG)	Nortel Media Gateway 7480 or 15000
PVG 7400 or PVG 7K	Nortel Media Gateway 7480
PVG 15000 or PVG 15K	Nortel Media Gateway 15000

Note: The CS 2000 Gateway Controller (GWC) Manager does not reflect these branding changes in SN08. As a result, the Gateway Controller customer documentation does not reflect these changes, as well. This table is being provided to map the names used in GWC documentation to other Carrier VoIP documentation.

Configuration management strategy

Initial Gateway Controller (GWC) configuration is performed by Nortel Networks installation personnel.

The following post installation capabilities are provided to customers:

- re-configuring GWCs (limited capability)
- increasing the GWC capacity in a network
- configuring packet network connections between the GWC and various gateway types

Tools and utilities

The CS 2000 SAM21 Manager graphical user interface is used to provision the base parameters for GWC cards. The datafill specifies such values as the IP address, slot location, node definition, and card provisioning.

ATTENTION

The GWC Manager does not display provisioning data in real time. That is, when two users are changing provisioning data on the same GWC node at the same time, you must refresh your display to see the changes implemented by the other user. Use the Refresh button if available. Otherwise, you may have to select a different GWC node, then re-select again the node that you are updating.

The CS 2000 GWC Manager, a Java-based GUI that runs in a web browser application, is used to configure GWCs and associate GWC nodes with media gateways. The CS 2000 GWC Manager is also used to provision endpoints that enable the GWC node to mediate the bearer path for a call.

Note: Most of the procedures in this NTP are performed using the CS 2000 GWC Manager. You can perform most of the tasks associated with these procedures using either of the following tools:

- the CS 2000 GWC Manager
- the OSSGate application

For details on using the OSSGate application, and to see a list of commands supported using OSSGate, refer to the OSSGate User Guide, NE10004-512.

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (IEMS). In addition, access to the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, is now provided using the IEMS. For more information, refer to the *Integrated EMS Basics* NTP, NN10329-111.

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in the *Integrated EMS Basics NTP*, NN10329-111:

- “Launching GWC Manager”
- “Launching SAM21 Manager”

General GWC configuration procedures

Each general procedure presented in this section refers to multiple individual procedures included in this NTP. The following table lists the general procedures included in this section.

General GWC configuration procedures (Sheet 1 of 2)

Procedures to configure generic functionality:

- Set up network services on page 5
- Add a new GWC node to the network on page 6
- Modify the base configuration of an installed GWC card on page 8

General GWC configuration procedures (Sheet 2 of 2)

- Modify the operating configuration of an installed GWC node on page 9
- Re-configure a GWC node in the network on page 10
- Remove service from a GWC card or node on page 12

Procedures to configure specific items:

- Add QoS collection service on page 12
- Add a media proxy to the network on page 13
- Add an IP-VPN(NAT) zone to the network on page 13
- Configure an IP-VPN(NAT) zone to be shared with another CS 2000 on page 13
- Add an LBL zone to the network on page 14
- Add a composite NAT and LBL zone to the network on page 14
- Add a PEP server to the network on page 15
- Add an ALG to the network on page 15
- Configure a destination for CICM location information and enable change reporting on page 16
- Configure the Packet Media Anchor functionality on an audio controller GWC node on page 16
- Activate Network VCAC on a GWC Manager on page 18
- Configure IP Security (IPSec). For all IPSec-related procedures, refer to the *Gateway Controller Security and Administration* NTP, NN10213-611.

The process of configuring a GWC node and associating the node with a media gateway is similar for all GWC service types and media gateways. Differences in configuration scenarios occur due to the type of gateway used, such as lines, trunks, or VRDN. Differences also occur when network address translator (NAT) devices, policy enforcement point (PEP) servers, application layer gateway (ALG), or limited bandwidth links (LBL) are required.

Use the following general steps to configure a GWC node:

1. Add a GWC node to the GWC database using the CS 2000 GWC Manager and CS 2000 SAM21 Manager.
2. Associate a media gateway to the GWC node (along with any additional devices such as NAT zones).

Note: When necessary, provision trunk tables in the XA-Core using the MAP. For details, refer to the *CS 2000 Configuration Management* NTP for your solution.

Set up network services

When an existing system is expanded, additional GWC nodes may be added as well as other devices that provide network OAM&P services used by one or more GWC nodes. Some of these services include:

- dynamic quality of service (DQoS)
- PEP services using configured middlebox devices
- NAT services provided by NAT zones and media proxy services
- LBL services provided by LBL zones
- application layer gateway (ALG) service

The following list of procedures provides a summary of the services available to be configured, and the order in which these services can be set up in the network, following initial installation.

- Add a network codec profile on page 19
- Configure a recurring data integrity audit on page 59
- Set or change network DQoS configuration parameters on page 55
- Add or change the RMGC default domain on page 63
- Provision advice of charge option on page 53
- Set the call agent identifier on page 67. This procedure is required prior to configuring PEP servers or ALGs, NAT, LBL, or composite NAT-LBL zones.
- Add QoS collection service on page 12; if applicable to your solution.
- Add a PEP server to the network on page 15; if applicable to your solution.
- Add an application layer gateway to the network (cable market) on page 419; if applicable to your solution.
- Add a media proxy to the network on page 13; if applicable to your solution.

- Add an IP-VPN (NAT) zone on page 317; if applicable to your solution.
- Configure resource usage data for limited bandwidth links (LBL) on page 323; if applicable to your solution.

  Note: Resource usage data is used by LBLs. You must complete this procedure only when the Network VCAC status is set to OFF, that is, the virtual call admission control is performed by each GWC (network configuration without the Policy Controller).

- Add a limited bandwidth link (LBL) zone on page 331; if applicable to your solution.
- Configure a destination for CICM location information on page 77; if applicable to your solution.
- Add the Policy Controller on page 83; if applicable to your solution.
- Change the Network VCAC status on page 95; if applicable to your solution.
- Review available network devices on page 99

Add a new GWC node to the network

When new GWC card sets are installed, use the CS 2000 SAM21 Manager to provision the base parameters for the two GWC cards to be defined as the node, then use the CS 2000 GWC Manager to add the GWC node to the GWC Manager database and to enable the call processing parameters and service types (that is, trunk, line, VRDN) on the new GWC node. Complete the following set of procedures, in the order given, to add and configure GWC cards, define GWC nodes, and associate gateways and endpoints.

At the SAM21 shelf and the CS 2000 GWC Manager workstation

1 If adding new GWC hardware to the SAM21 shelf where GWC cards have not been previously installed, install new GWC cards into SAM21 shelf in pairs (two cards for each GWC node) using procedure Install a GWC card on page 101.

or

If adding new GWC hardware to the SAM21 shelf where GWC cards have previously been installed and you want to provision new services without the old provisioning information being assigned to the new GWC cards, perform procedure Remove service from a GWC card on page 111.

2 Use the CS 2000 SAM21 Manager to provision the GWC cards, define the GWC node, and assign service. Follow procedure Assign service to a GWC card on page 105.

3 Add and configure a GWC node in the CS 2000 GWC Manager database. Follow procedure Add and configure a GWC node on page 123.

4 Unlock the GWC cards in the node. Follow procedure Unlock a GWC card on page 523.

5 If necessary, manually return the GWC node to service (RTS) at the CS 2000 GWC Manager. Follow procedure Manually return a GWC node to service on page 527.

6 Associate a gateway type to a GWC node using an appropriate procedure from the following list:

- Associate a trunk media gateway on page 135.
- Configure the domain name for MTA gateways (cable market) on page 145; if required for your solution.
- Associate a small line media gateway (cable market) on page 153.
- Associate a line media gateway (wireline market) on page 161.
- Associate an H.323 media gateway on page 175
- Associate an audio server media gateway on page 193.

7 Add trunk endpoints or line endpoints to the gateway or add V5.2 carriers. Follow procedure Add carriers to a GWC on page 201.

8 If applicable, associate a media proxy to the GWC node. Follow procedure Associate a media proxy with a GWC node on page 373.

9 If applicable, associate a QoS collector to selected gateways assigned to the GWC node. Follow procedure Associate a QoS collector with a GWC node on page 387.

10 If applicable, associate a PEP server or an ALG to selected gateways assigned to the GWC node. Follow one of the following procedures:

- Associate a PEP server with a media gateway on page 405.
- Associate an ALG with a media gateway on page 425

11 Review selected configuration and provisioning data for the GWC node using an appropriate procedure from the following list:

- View carrier provisioning data for a GWC node on page 231.
- View gateway provisioning data for a GWC node on page 245.
- View lines provisioning data for a GWC node on page 253.

- View media proxy configuration data for a GWC node on page 367.
- View QoS collector configuration data for a GWC node on page 393.

Modify the base configuration of an installed GWC card

Use the CS 2000 SAM21 Manager and complete the following set of procedures in the order listed to re-configure base parameters for GWC cards in an existing node. Re-configuration can include the following parameters:

- IP address of the GWC cards that make up the node
- default_router/gateway_IP_address
- subnet mask
- firmware version of the GWC load
- CS 2000 Management Tools server host IP address
- IP address of the CS 2000 Core Manager or Core and Billing Manager (CBM)
- the path to the GWC software load on the CS 2000 Core Manager or CBM
- GWC software load name
- IP addresses of the available domain name servers

At the CS 2000 GWC Manager workstation

1. Manually busy both GWC cards in the node using procedure Busy a GWC node on page 513.
2. Manually re-provision GWC cards on page 115.
3. Manually return the GWC node to service (RTS) at the CS 2000 GWC Manager using procedure Manually return a GWC node to service on page 527.
4. Review selected configuration and provisioning data for the GWC node using an appropriate procedure from the following list:
   - View carrier provisioning data for a GWC node on page 231.
   - View gateway provisioning data for a GWC node on page 245.
   - View lines provisioning data for a GWC node on page 253.

- View media proxy configuration data for a GWC node on page 367.
- View QoS collector configuration data for a GWC node on page 393.

Modify the operating configuration of an installed GWC node

Use the CS 2000 GWC Manager and complete the following set of procedures in the order listed to re-configure operating parameters for a previously configured GWC node. Re-configuration can include the following parameters:

- gateway IP discovery attribute
- PEP server attribute
- ALG attribute
- adjacent network zone attribute
- gateway capacity attribute
- gateway IP or port address
- gateway profile
- the Gateway Controller profile

  Note: In this procedure, you can only change the audio controller Gateway Controller profiles.

- the network codec profile (limited to a new profile using same bearer network as the previous profile)

At the CS 2000 GWC Manager workstation

1 Manually busy both GWC cards in the node using procedure Busy a GWC node on page 513.

2 If changing operating attributes, complete procedure Change gateway attributes on page 277.

3 If applicable, complete procedure Change the service profile of a GWC node on page 259.

  Note: Use this procedure only if you want to change from an Audio Controller profile to an Audio Controller with RMGC profile.

4 If applicable, complete procedure Change the network codec profile for a GWC node on page 299

5 Manually return the GWC node to service (RTS) at the CS 2000 GWC Manager using the procedure Manually return a GWC node to service on page 527.

6 Review selected configuration and provisioning data for the GWC node using an appropriate procedure from the following list:

- View carrier provisioning data for a GWC node on page 231.
- View gateway provisioning data for a GWC node on page 245.
- View lines provisioning data for a GWC node on page 253.
- View media proxy configuration data for a GWC node on page 367.
- View QoS collector configuration data for a GWC node on page 393.

Re-configure a GWC node in the network

Use the CS 2000 GWC Manager to complete the following set of procedures in the order listed to change the Gateway Controller service profile configured on a GWC node.

Note: This procedure allows you to re-configure all aspects of a GWC node, including the Gateway Controller profile and all other relevant characteristics of a node.

At the CS 2000 GWC Manager workstation

1 Manually busy both GWC cards in the node using procedure Busy a GWC node on page 513.

2 If applicable, refer to the *CS 2000 Configuration Management* NTP for your solution to remove line endpoints or V5.2 carriers from the GWC node.

3 Complete procedure Disassociate a media gateway on page 305 for all gateways associated with the node.

4 Lock the GWC cards in the node from the CS 2000 SAM21 Manager card view using procedure Lock a GWC card on page 519.

5 Complete procedure Delete a GWC node on page 309.

6 Add and configure a GWC node in the CS 2000 GWC Manager database using procedure Add and configure a GWC node on page 123.

7 Unlock the GWC cards in the node using procedure Unlock a GWC card on page 523.

8 If necessary, manually return the GWC node to service (RTS) at the CS 2000 GWC Manager using procedure Manually return a GWC node to service on page 527.

9 Associate a gateway type to a GWC node using an appropriate procedure from the following list:

- Associate a trunk media gateway on page 135.
- Configure the domain name for MTA gateways (cable market) on page 145; if required for your solution.
- Associate a small line media gateway (cable market) on page 153.
- Associate a line media gateway (wireline market) on page 161.
- Associate an H.323 media gateway on page 175
- Associate an audio server media gateway on page 193.

10 Add trunk, line, or V5.2 endpoints to the gateway using procedure Add carriers to a GWC on page 201.

11 If applicable, associate a media proxy to the GWC node using procedure Associate a media proxy with a GWC node on page 373.

12 If applicable, associate a QoS collector to selected gateways assigned to the GWC node using procedure Associate a QoS collector with a GWC node on page 387.

13 If applicable, associate a PEP server or an ALG to selected gateways assigned to the GWC node using one of the following procedures:

- Associate a PEP server with a media gateway on page 405.
- Associate an ALG with a media gateway on page 425

14 Review selected configuration and provisioning data for the GWC node using an appropriate procedure from the following list:

- View carrier provisioning data for a GWC node on page 231.
- View gateway provisioning data for a GWC node on page 245.
- View lines provisioning data for a GWC node on page 253.
- View media proxy configuration data for a GWC node on page 367.
- View QoS collector configuration data for a GWC node on page 393.

Remove service from a GWC card or node

Use the CS 2000 GWC Manager to complete the following set of procedures in the order listed to completely remove a GWC node from the database.

At the CS 2000 GWC Manager workstation

1. Manually busy both GWC cards in the node using procedure Busy a GWC node on page 513.
2. If applicable, refer to the *CS 2000 Configuration Management* NTP for your solution to remove line endpoints or V5.2 carriers from the GWC node.
3. Complete procedure Disassociate a media gateway on page 305 for all gateways associated with the node.
4. Lock the GWC cards in the node from the CS 2000 SAM21 Manager card view using procedure Lock a GWC card on page 519.
5. Complete procedure Delete a GWC node on page 309
6. To completely remove the GWC cards from service, complete procedure Remove service from a GWC card on page 111.

Add QoS collection service

Use the following procedures to add a quality of service (QoS) collection device to the network running a QoS collection application, associate GWC nodes with QoS collectors, and enable QoS reporting for specific gateways.

At the CS 2000 GWC Manager workstation

1. Set or change network DQoS configuration parameters on page 55.
2. Add a quality of service (QoS) collector on page 383.
3. Associate a QoS collector with a GWC node on page 387.
4. Enable or disable QoS reporting for a GWC node on page 391.
5. To correlate QoS reporting with billing records, you must enable QoS reporting through table AMAOPT in the XA-Core. Complete procedure “Provisioning in support of QoS reporting” in the *CS 2000 Configuration Management* NTP applicable to your solution.

Add a media proxy to the network

Use the following set of procedures to add one or more media proxies to be made available to perform NAT traversal functions. A media proxy device is used as a real-time transport protocol (RTP) portal to allow a gateway in one domain to communicate with a gateway in another domain. A GWC will select and then set up the media proxy based on call flow.

At the CS 2000 GWC Manager workstation

1 Add a media proxy on page 363.

2 Associate a media proxy with a GWC node on page 373.

Add an IP-VPN(NAT) zone to the network

Use the following procedures to add one or more NAT zones to the network.

At the CS 2000 GWC Manager workstation

1 Set the call agent ID for the CS 2000. Complete procedure Set the call agent identifier on page 67.

Note: Omit this step if the call agent ID is already set.

2 Complete procedure Add an IP-VPN (NAT) zone on page 317.

3 If necessary, review network configuration data using procedure Review available network devices on page 99

Configure an IP-VPN(NAT) zone to be shared with another CS 2000

Use the following procedure to configure a NAT zone to be shared between more that one CS 2000.

Note: A prerequisite to this procedure is procedure Add an IP-VPN (NAT) zone on page 317. This procedure assumes that a NAT zone has already been added on one CS 2000, and that you are adding the same NAT to a different CS 2000.

At the CS 2000 GWC Manager workstation

1 Display the NAT zone ID for the NAT to be shared. Complete procedure View a network zone ID on page 355. Perform this procedure for the CS 2000 on which the NAT was originally configured.

2 If this is the second (or subsequent) CS 2000 on which this shared NAT is being added, complete procedure Add an IP-VPN (NAT) zone on page 317 for a next CS 2000 (different than in step 1). Follow the steps to configure a NAT zone to be shared

between more than one CS 2000 devices. Use the NAT zone ID displayed in step 1 of this procedure.

3 Repeat step 2 for any other CS 2000s required to share the same NAT.

Add an LBL zone to the network

Use the following procedure to configure limited bandwidth links (LBL).

At the CS 2000 GWC Manager workstation

1 Set the call agent ID for the CS 2000. Complete procedure Set the call agent identifier on page 67.

Note: Omit this step if the call agent ID is already set.

2 If applicable, create a resource usage profile for the LBL to use. Complete procedure Configure resource usage data for limited bandwidth links (LBL) on page 323.

Note: This step applies only when the Network VCAC is set to OFF and the virtual call admission control is performed by each GWC (network configuration without a Policy Controller).

3 Complete procedure Add a limited bandwidth link (LBL) zone on page 331

4 If necessary, review network configuration data using procedure Review available network devices on page 99

Add a composite NAT and LBL zone to the network

Use the following procedure to configure a composite network zone - a zone comprising the attributes of both NAT and LBL network zones. Use this option for network sites (zones) that include both NATs and LBLs.

At the CS 2000 GWC Manager workstation

1 Set the call agent ID for the CS 2000. Complete procedure Set the call agent identifier on page 67.

Note: Omit this step if the call agent ID is already set.

2 Complete procedure Add a composite IP-VPN (NAT) and LBL zone on page 343.

3 If necessary, review network configuration data using procedure Review available network devices on page 99

Add a PEP server to the network

Use the following set of procedures to add one or more PEP servers to the network and to associate them to gateways.

At the CS 2000 GWC Manager workstation

1 Set the call agent ID for the CS 2000. Complete procedure Set the call agent identifier on page 67.

Note: Omit this step if the call agent ID is already set.

2 To add a new PEP server to the network, complete procedure Add a policy enforcement point (PEP) server on page 401.

3 To change the IP address of a PEP server, complete procedure Change the attributes of a PEP server on page 409.

4 Associate a PEP server with a media gateway on page 405.

Add an ALG to the network

Use the following set of procedures to add one or more application layer gateways (ALG) to the network and to associate them to gateways.

At the CS 2000 GWC Manager workstation

1 Set the call agent ID for the CS 2000. Complete procedure Set the call agent identifier on page 67.

Note: Omit this step if the call agent ID is already set.

2 To add a new ALG to the network, complete procedure Add an application layer gateway to the network (cable market) on page 419.

3 To change the IP address of an ALG, complete procedure Change the attributes of an ALG on page 423.

4 Associate an ALG with a media gateway on page 425.

Add V5.2 services to a GWC node

Use the following set of procedures to configure V5.2 trunk services on a GWC node.

At the CS 2000 GWC Manager workstation

1. Refer to the *CS 2000 Configuration Management* NTP applicable to your solution and complete the procedures for installing V5.2 services on the XA-Core.
2. Add V5.2 interfaces on page 445.
3. Add a V5 interface provisioning template on page 439.
4. Add a V5 ring template on page 451.
5. Add a V5 signaling template on page 455.

Configure a destination for CICM location information and enable change reporting

Use the following procedures to configure a destination (recipient) for Centrex IP Client Manager (CICM) location information and to enable change reporting on a GWC node.

At the CS 2000 GWC Manager workstation

1. Configure a destination for CICM location information on page 77. This procedure is performed at the network level for the CS 2000.
2. To enable change reporting on a GWC node, complete procedure Enable or disable CICM location change reporting on page 313.
3. Repeat step 2, as required, for other GWC nodes in your system.

Configure the Packet Media Anchor functionality on an audio controller GWC node

Use the following procedures to configure the Packet Media Anchor functionality, which replaces the APG device, on an audio controller GWC node.

Note: For an overview of the Packet Media Anchor functionality, refer to the *Gateway Controller Basics* NTP, NN10189-111.

At the CS 2000 GWC Manager workstation

1 Make sure that the following data is appropriately configured:

- in table SRVSINV, the maximum number of simultaneous calls to support
- on the Media Server 2010 gateway, three BCT and one audio resource for each anchored call

Note: For more information, refer to the solution-level *Configuration Management* NTP applicable to your solution.

2 Verify that the selected audio controller GWC node uses only G.711 u-Law or G.711 a-Law encoding algorithm (codec). If required, refer to procedure View characteristics of a GWC node on page 239. If any other codec is used during a call, the Packet Media Anchor tones and digit collection capability may be affected.

3 If required, change the current network codec profile assigned to the selected GWC to a new profile that supports only G.711 u-Law or G.711 a-Law codec. Follow procedure Change a network codec profile on page 37.

4 Associate the Media Server 2010 gateway, configured with the Packet Media Anchor functionality, to the selected audio controller GWC. Follow procedure Associate an audio server media gateway on page 193.

Note: If the Media Server 2010 gateway that you want to use for this functionality has the UAS profile currently assigned to it, you must complete the following steps:

- Disassociate the gateway from the GWC using procedure Disassociate a media gateway on page 305.
- Re-associate the gateway (using the AMS profile) to the audio controller GWC. Follow procedure Associate an audio server media gateway on page 193.

5 Invoke a cold SwAct (switch of activity) on the GWC node or re-initialize all the Media Server 2010 gateways.

If required, refer to procedure "Invoke a cold manual protection switch (cold swact)" in the *Gateway Controller Security and Administration* NTP, NN10213-611.

Activate Network VCAC on a GWC Manager

Use the following procedures to activate the Network VCAC (virtual call admissions control) functionality using the GWC Manager.

With the Network VCAC activated (Status: ON), the Policy Controller performs VCAC functions; that is, counts available resources across limited bandwidth links (LBL) and makes the connection admission decisions. Gateway Controllers (GWC) communicate with the Policy Controller to determine whether a call can be set up.

For a complete procedure on how to configure the Policy Controller and to implement network VCAC, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

At the CS 2000 GWC Manager workstation

1 Add the Policy Controller on page 83

2 Change the Network VCAC status on page 95

Add a network codec profile

Purpose of this procedure

Use this procedure to add a network codec profile using the CS 2000 GWC Manager.

Starting in SN07, you can configure and use network codec profiles with multiple bearer network fabric types on a CS 2000. You can configure individual codecs that use any of the following bearer network fabric types concurrently on a CS 2000:

- IP
- AAL1
- AAL2

Each GWC node in a CS 2000 must be configured to use one of the available network codec profiles. GWC nodes in a CS 2000 can use different codec profiles configured to operate over different bearer network fabrics. You can define multiple network codec profiles in the system, and then select the desired profile while adding a GWC node to the network.

When to use this procedure

Use this procedure when you need to add a new network codec profile to your CS 2000.

Note: The following procedures related to configuring network codec profiles are also available in this NTP:

- View a network codec profile on page 31
- Change a network codec profile on page 37
- Delete a network codec profile on page 49

Prerequisites and guidelines

Prerequisites

Your CS 2000 Management Tools software (including the CS 2000 GWC Manager) must be upgraded to an SN07 or higher version.

The following table shows a compatibility matrix for the SN08 version of CS 2000 Management Tools software. This software version allows users to configure network codec profiles with multiple bearer network fabric types on a CS 2000.

CS 2000 Management Tools software version	Compatible versions	
	GWC card software	XA-Core software
SN08	SN08	SN08
	SN07	SN07
	SN06.2	SN06.2
	SN06	

General guidelines

The following general guidelines apply to this procedure:

- In SN08, the option to configure network codec profiles using multiple bearer network fabric types is available on the CS 2000 in the North American and international markets.
- If you are adding a profile with a bearer network type that is new to your CS 2000, you must modify the table BEARNETS on the XA-Core to configure a network instance of the new network type. You must modify the BEARNETS table before you can add a GWC node and configure the node to use the new bearer network type.

  Refer to procedure “Specifying the bearer networks served by the CS 2000“ in the *CS 2000 Configuration Management* NTP applicable to your solution.

GWC node guidelines

No matter which network bearer types (IP, AAL1, or AAL2) are configured for a CS 2000 using this procedure, only one bearer network type can be selected for any GWC node.

Network codec profile default guidelines

Only one network codec profile can be set as the *network default*. The network default setting is used in the following circumstances:

- When upgrading from an SN06.2 to an SN08 software load of the CS 2000 Management Tools, the initial SN08 network default codec profile is based on the pre-SN07 network configuration.
- When a CS 2000 data integrity audit finds a configuration mismatch between the CS 2000 GWC Manager database and the Core, the audit process can use the network default codec profile to correct the problem.

Only one *default codec* can be set for each bearer network type (IP, AAL1, or AAL2) defined on your CS 2000. When adding a GWC node using procedure Add and configure a GWC node on page 123, the default codec appears as the default setting for the option “GWC codec profile”, based on the bearer network selected.

The following system behavior applies to adding or changing a network codec profile:

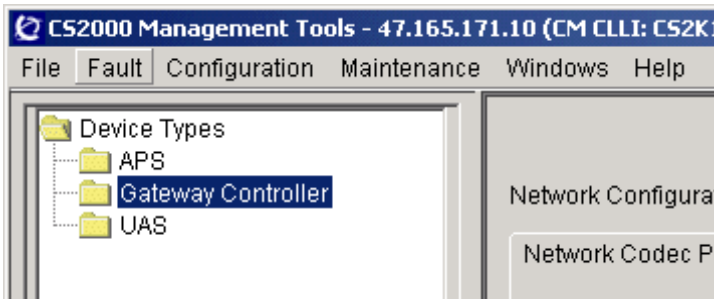
- You can enable the bearer type default setting for a profile when an existing profile using the same network type has the same setting already enabled. If you proceed, the bearer type default setting for the existing profile will be automatically disabled.
- You can enable the network default setting for a profile when an existing profile has the same setting already enabled. If you proceed, the network default setting for the existing profile will be automatically disabled.

Action

At CS 2000 GWC Manager client

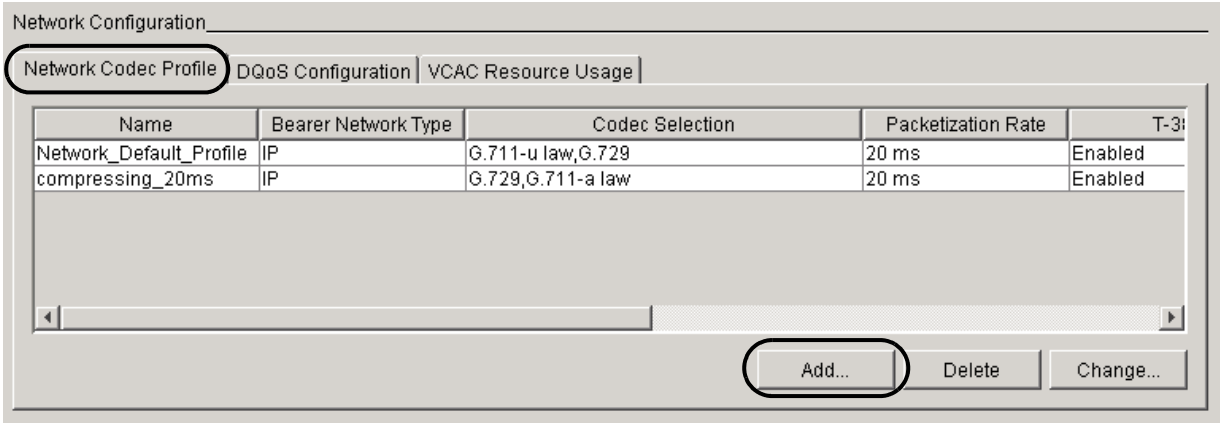
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

The Network Configuration panel is displayed to the right of the Device Types menu.

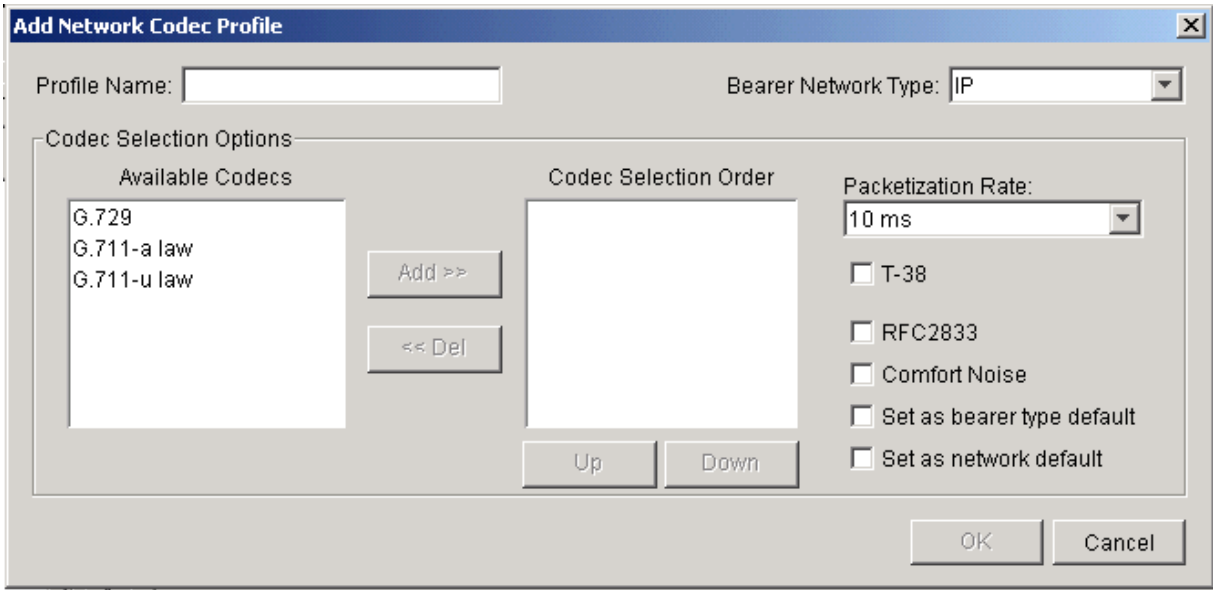


2 From the Network Configuration panel, click the **Network Codec Profile** tab to display the Network Codec Profile pane.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



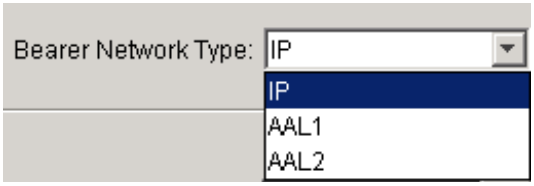
3 Click the **Add** button to display the Add Network Codec Profile dialog box.



4 In the Profile Name field, type a name for the new profile.

The profile name can include any combination of alpha-numeric text.

5 In the Bearer Network Type field, select a bearer network type for the profile using the drop-down menu.



The options are:

- IP - Internet Protocol
- AAL1 - ATM Adaptation Layer 1
- AAL2 - ATM Adaptation Layer 2

Note: The default bearer network is IP.

When you select a bearer network type, the dialog box is automatically updated to reflect the options available for that network type. Available codecs and other options differ depending on whether you select an IP or ATM bearer network.

6 Select a combination of codecs for the new profile.

Note 1: The codecs are used in the order in which they are selected in Codec Selection Order list, from top to bottom.

Note 2: Only certain combinations of codecs are supported, in a certain order.

Refer to table Valid codec combinations for bearer network types at the end of this step to view the valid codec combinations for each bearer network type.

The system applies the following criteria when choosing which codec to use:

- Any GWC node using a profile will initially attempt to communicate with a media gateway using the *first* codec listed.
- If the first codec is not suitable, then the GWC node will use the *second* codec listed (if present).
- If the second codec is also not suitable, then the GWC node will use the *third* codec listed (if present).

Perform the following steps to select a codec combination:

a Select a codec from the list of Available Codecs.

The codecs available depend on the bearer network type you selected previously.

b Click the **Add >>** button to add the codec to the Codec Selection Order list.

If your profile requires more than one codec, select the codecs in the order they will be used.

You can remove a codec from the list by clicking the **<< Del** button.

c If necessary, repeat the previous step until you have selected the codecs required for the profile.

d If necessary, adjust the order of your codecs by selecting a codec in the Codec Selection Order list and clicking the **Up** or **Down** button.

e Repeat the previous steps until you have selected a codec combination for your profile.

The following table lists the valid codec combinations for bearer network types.

Valid codec combinations for bearer network types (Sheet 1 of 2)

Bearer network type	Valid codec combinations (in order)		
	1st	2nd	3rd
IP	G.729	G.711-a law	G.711-u law
	G.729	G.711-u law	G.711-a law
	G.729	G.711-a law	
	G.729	G.711-u law	
	G.711-a law	G.711-u law	G.729
	G.711-u law	G.711-a law	G.729
	G.711-a law	G.729	
	G.711-u law	G.729	
	G.711-a law	G.711-u law	
	G.711-u law	G.711-a law	
	G.711-a law		
	G.711-u law		
AAL1	G.711-u law		

Valid codec combinations for bearer network types (Sheet 2 of 2)

Bearer network type	Valid codec combinations (in order)		
	1st	2nd	3rd
AAL2	G.729	G.711-a law	
	G.729	G.711-u law	
	G.729	G.711-a law	G.711-u law
	G.729	G.711-u law	G.711-a law
	G.726-32	G.711-a law	G.711-u law
	G.726-32	G.711-u law	G.711-a law
	G.726-32	G.711-a law	
	G.726-32	G.711-u law	
	G.711-a law	G.711-u law	
	G.711-u law	G.711-a law	
	G.711-a law		
	G.711-u law		

7 Select a Packetization Rate for the new profile using the drop-down menu.

The packetization rate option is available only on IP bearer networks.

The options are:

- 10 milliseconds (default)
- 20 milliseconds

8 Select the T-38 check box if the new profile supports T-38 real-time facsimile (fax) capability.

T-38 is available only on IP bearer networks.

This option results in the GWC node including T.38 in the list of requested media types to the associated media gateways during call setup. T.38 is the ITU-T standard for real-time transport of Group 3 fax over IP.

T-38 is not selected by default.

Note: T-38, RFC 2833 and Comfort Noise are local control options in which a GWC sends messages to media gateways over NCS and MGCP protocols. Each of these options is available only on IP bearer network types.

9

ATTENTION

RFC 2833 is not currently supported on the CS 2000 for gateways using the NCS protocol. Any GWC node hosting NCS gateways must use a network codec profile that has RFC 2833 disabled (check box not selected).

Select the RFC 2833 check box if the new profile supports the transmission of tones over IP.

RFC 2833 is available only on IP bearer networks.

RFC 2833 indicates whether the profile supports Real-Time Protocol (RTP) payload for Dual-Tone Multifrequency (DTMF) digits, telephony tones and telephony signals.

This option allows each GWC node using the profile to send standard tones to a media gateway during call setup. RFC 2833 is an Internet Engineering Task Force (IETF) standard for the transport of tones over IP.

RFC2833 is not selected by default.

10 Select the Comfort Noise check box if the new profile supports this option.

Comfort noise is available only on IP bearer networks.

This option allows each GWC node using the profile to send comfort noise, a sound that is generated and played to the line when silence suppression is used (when no voice packets are being received). This is to reassure the user that the connection is still active.

Comfort Noise is not selected by default.

11 Select the Set as bearer type default check box if you want the new profile to be the default for the bearer network type (selected previously).

Only one default codec can be set for each bearer network type (IP, AAL1 or AAL2) defined on your CS 2000.

When adding a GWC node using procedure Add and configure a GWC node on page 123, the default codec appears as the default setting for the option “GWC codec profile”, based on the bearer network selected.

This option is not selected by default.

Note: You can enable the bearer type default setting for a new profile when an existing profile using the same network type has the same setting already enabled. If you proceed, the bearer type default setting for the existing profile will be automatically disabled.

12 Select the Set as network default check box if you want the new profile to be the default for the entire network.

Only one network codec profile can be set as the network default. The network default setting is used in the following circumstances:

- When upgrading from an SN06.2 to an SN08 software load of the CS 2000 Management Tools, the initial SN08 network default codec profile is based on the pre-SN07 network configuration.
- When a CS 2000 data integrity audit finds a configuration mismatch between the CS 2000 GWC Manager database and the Core, the audit process can use the network default codec profile to correct the problem.

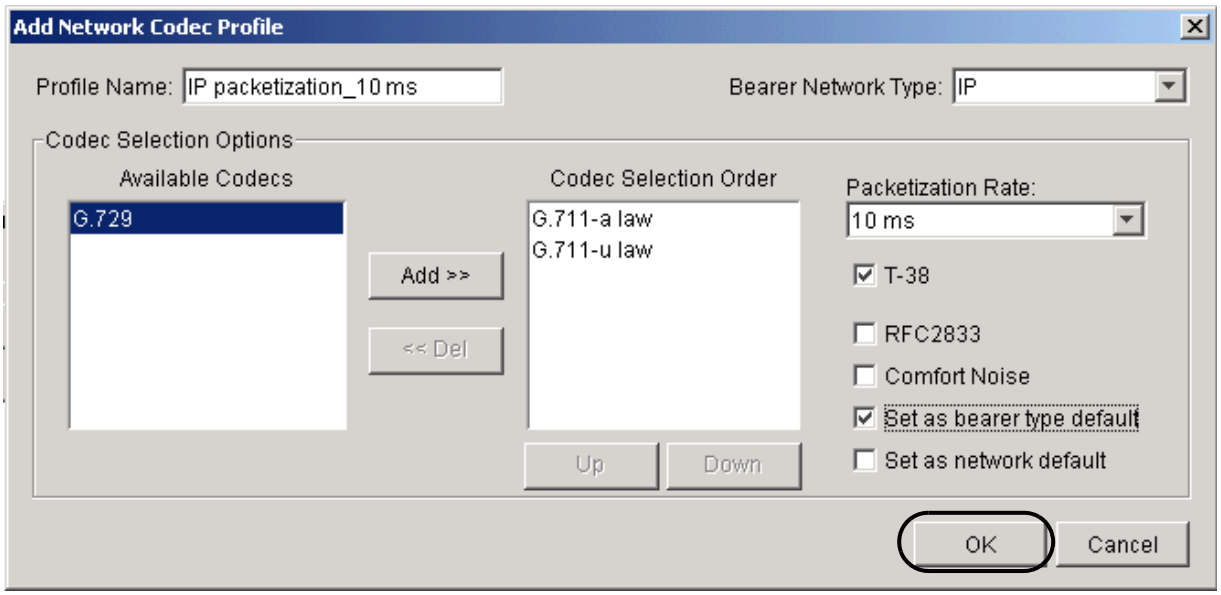
This option is not selected by default.

Note: You can enable the network default setting for a new profile when an existing profile has the same setting already enabled. If you proceed, the network default setting for the existing profile will be automatically disabled.

13 Click the **OK** button when you have finished configuring the profile.

Note 1: If any required settings are missing, the **OK** button will not be available. Ensure that you have selected a Profile Name and at least one codec.

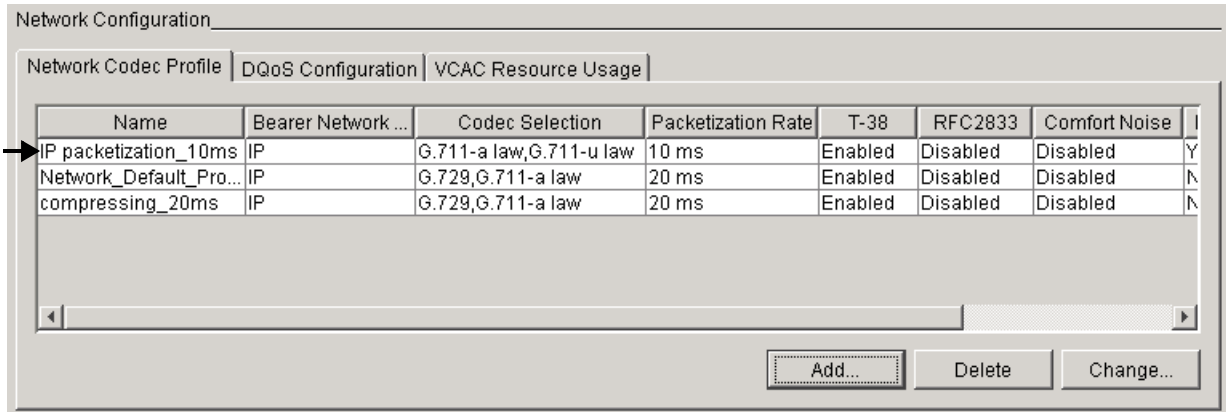
Note 2: If the codec combination you selected is invalid, you will see an error message. Refer to the table Valid codec combinations for bearer network types on page 25.



14 Verify that the new profile appears on the list of network codec profiles.

Note: If you are adding a profile with a bearer network type that is new to your CS 2000, you must modify the table BEARNETS on the XA-Core to configure a network instance of the new network type. You must modify the BEARNETS table before you can add a GWC node and configure the node to use the new bearer network type.

Refer to procedure “Specifying the bearer networks served by the CS 2000“ in the *CS 2000 Configuration Management* NTP applicable to your solution.



15 If necessary, return to step 2 to add another profile.

16 The procedure is complete.

View a network codec profile

Purpose of this procedure

Use this procedure to verify the existing network codec profile configuration using the CS 2000 GWC Manager.

For an explanation of the supported network codec profile configuration, refer to procedure Add a network codec profile on page 19.

When to use this procedure

Use this procedure when you need to verify the existing network codec profile configuration.

Prerequisites and guidelines

Your CS 2000 Management Tools software (including the CS 2000 GWC Manager) must be upgraded to an SN08 version.

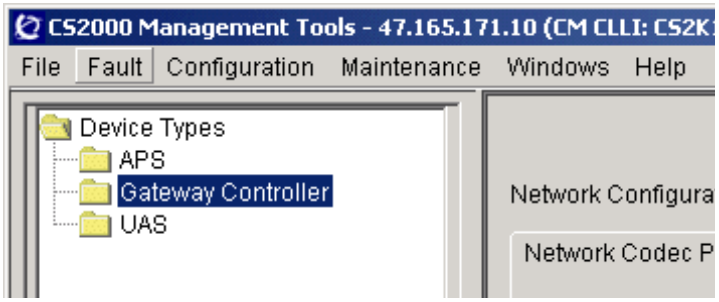
The CS 2000 must be configured with at least one network codec profile.

Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

The Network Configuration panel is displayed to the right of the Device Types menu.

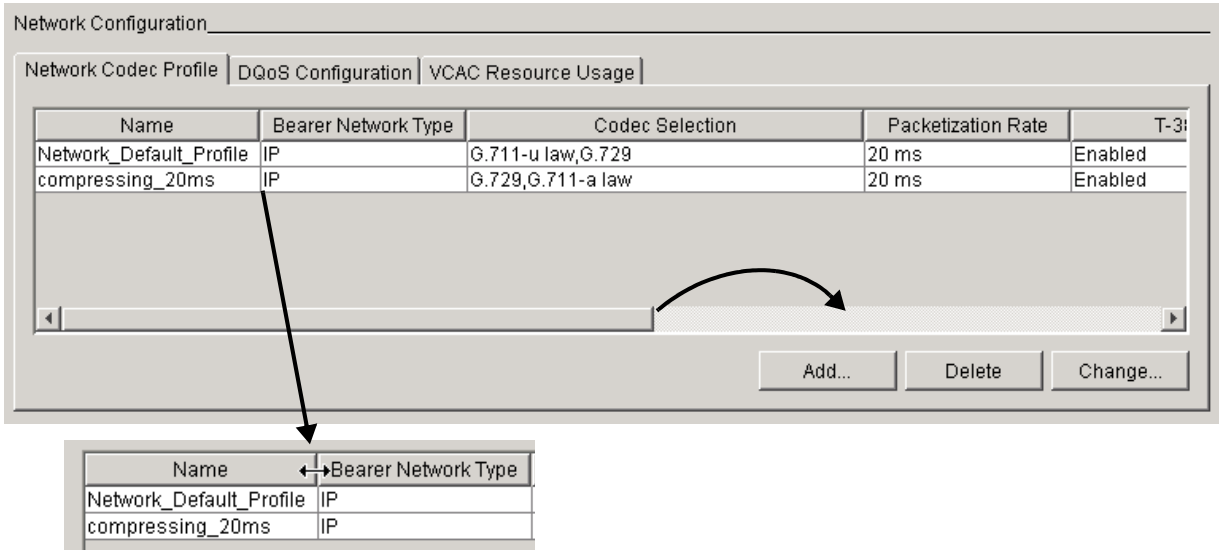


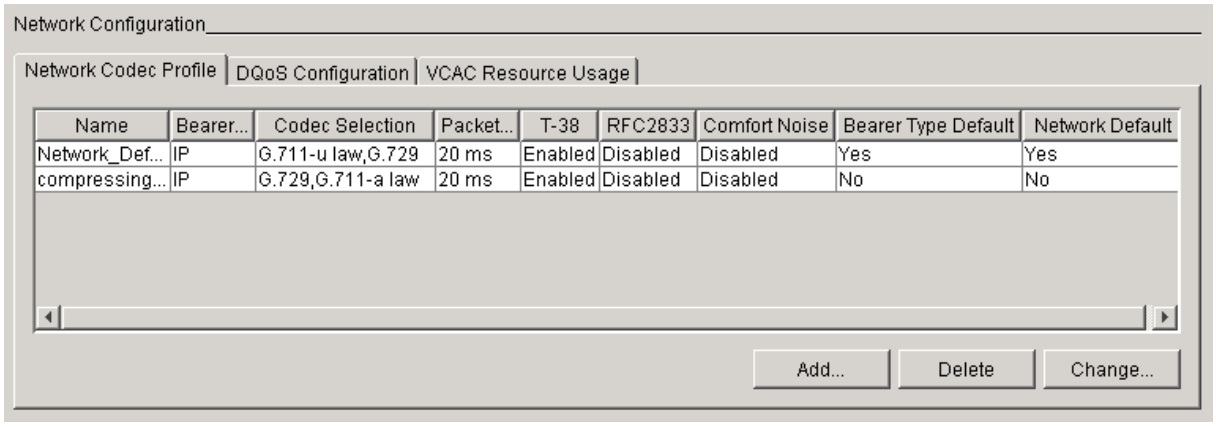
2 From the Network Configuration panel, click the **Network Codec Profile** tab to display the Network Codec Profile pane.

Select the edge of any tab to adjust the display. To view any hidden information, slide the horizontal scroll bar near the bottom of the screen to the right.

Refer to the table Description of network codec profiles on page 33 for an information on the fields describing each codec.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.





3 The procedure is complete.

The following table describes each field in the Network Codec Profile pane.

Description of network codec profiles

Field	Description
Name	User-defined alpha-numeric text string to identify the profile.
Bearer Network Type	Identifies the bearer network fabric type for the profile. The options are: • IP - Internet Protocol (default) • AAL1 - ATM Adaptation Layer 1 • AAL2 - ATM Adaptation Layer 2
Codec Selection	Identifies the codec or codecs selected for the profile. If more than one codec is listed, the codecs appear in the following order in which they will be used: • Any GWC node using a profile will initially attempt to communicate with a media gateway using the *first* codec listed. • If the first codec is not suitable, then the GWC node will use the *second* codec listed (if present). • If the second codec is also not suitable, then the GWC node will use the *third* codec listed (if present).
Packetization Rate	Specifies the packetization rate used by the profile. The options are: • 10 milliseconds (default) • 20 milliseconds Packetization rate is applicable only to IP bearer networks.

Description of network codec profiles

Field	Description
T-38	Indicates whether the profile supports T-38 real-time facsimile (fax) capability. This parameter allows a GWC node to send T-38 messages to an associated media gateway during call setup. T-38 is an International Telephony Union (ITU) standard for the transport of group 3 fax calls over IP. This option is not selected by default. T-38 is available only on IP bearer networks. ***Note:*** T-38, RFC2833 and Comfort Noise are local control options in which a GWC sends messages to media gateways over NCS and MGCP protocols. Each of these options is available only on IP bearer networks.
RFC2833	Indicates whether the profile supports Real-Time Protocol (RTP) payload for Dual-Tone Multifrequency (DTMF) digits, telephony tones and telephony signals. This parameter allows a GWC node to send standard tones to a media gateway during call setup. RFC 2833 is an Internet Engineering Task Force (IETF) standard for the transport of tones over IP. This option is not selected by default. RFC 2833 is available only on IP bearer networks. ***Note:*** RFC 2833 is not currently supported on the CS 2000 for gateways using the NCS protocol. Any GWC node hosting NCS gateways must use a network codec profile that has RFC 2833 disabled (check box de-selected).
Comfort Noise	Indicates whether the profile supports comfort noise. This parameter allows a GWC node to send comfort noise, a sound that is generated and played to the line when silence suppression is used (when no voice packets are being received). This is to reassure the user that the connection is still active. This option is not selected by default. Comfort noise is available only on IP bearer networks.

Description of network codec profiles

Field	Description
Bearer Type Default	Indicates whether the profile is the default for the bearer network type. Only one default codec can be set for each bearer network type (IP, AAL1 or AAL2) defined on your CS 2000. When adding a GWC node using procedure Add and configure a GWC node on page 123, the default codec appears as the default setting for the option “GWC codec profile”, based on the bearer network selected.
Network Default	Indicates whether the profile is the network default. Only one network codec profile can be set as the network default. The network default setting is used in the following circumstances: • When upgrading from an SN06.2 to an SN08 software load of the CS 2000 Management Tools, the initial SN08 network default codec profile is based on the pre-SN07 network configuration. • When a CS 2000 data integrity audit finds a configuration mismatch between the CS 2000 GWC Manager database and the Core, the audit process can use the network default codec profile to correct the problem.

Change a network codec profile

Purpose of this procedure

Use this procedure to change the parameters of an existing network codec profile using the CS 2000 GWC Manager.

For an explanation of the supported network codec profile configuration, refer to procedure Add a network codec profile on page 19.

When to use this procedure

Use this procedure when you need to make changes to an existing network codec profile.

Prerequisites and guidelines

Prerequisites

Your CS 2000 Management Tools software (including the CS 2000 GWC Manager) must be upgraded to an SN08 version.

The CS 2000 must be configured with at least one network codec profile.

General guidelines

CAUTION
Possible service disruption
If you are changing the parameters of a network codec profile that is currently being used by GWC nodes in your network, there is a risk that calls in progress may be affected. This may include:

- Calls that are being set up
- Calls that are currently active or stable

To reduce the risk of calls being affected, change these parameters during a low traffic period.

The following general guidelines apply to this procedure:

- You can change a network codec profile that is currently selected to be used by a GWC unit in your network. In this case, the change is propagated to any GWC units in service. If a unit is out of service, a

warning message will appear, and the changes will be propagated when the card is rebooted.

- You cannot change the profile name or the bearer network type of an existing profile. If you need to do so, delete the profile and add a new profile with the settings you require.

GWC node guidelines

You can change the network codec profile assigned to a GWC node, provided the profile supports the network bearer type already selected for the node.

If you wish to change the bearer network type assigned to a GWC node, refer to the general procedure Re-configure a GWC node in the network on page 10.

Network codec profile default guidelines

Only one network codec profile can be set as the *network default*. The network default setting is used in the following circumstances:

- When upgrading from an SN06.2 to an SN08 software load of the CS 2000 Management Tools, the initial SN08 network default codec profile is based on the pre-SN07 network configuration.
- When you perform a CS 2000 data integrity audit, the system uses this setting to identify and correct any network configuration mismatches between the GWC EM database and the XA-Core

Only one *default codec* can be set for each bearer network type (IP, AAL1 or AAL2) defined on your CS 2000. When adding a GWC node using procedure Add and configure a GWC node on page 123, the default codec appears as the default setting for the option “GWC codec profile”, based on the bearer network selected.

The following system behavior applies to adding or changing a network codec profile:

- You can enable the bearer type default setting for a profile when an existing profile using the same network type has the same setting already enabled. If you proceed, the bearer type default setting for the existing profile will be automatically disabled.
- You can enable the network default setting for a profile when an existing profile has the same setting already enabled. If you proceed, the network default setting for the existing profile will be automatically disabled.

Action

CAUTION
Possible service disruption
If you are changing the parameters of a network codec profile that is currently being used by GWC nodes in your network, there is a risk that calls in progress may be affected. This may include:

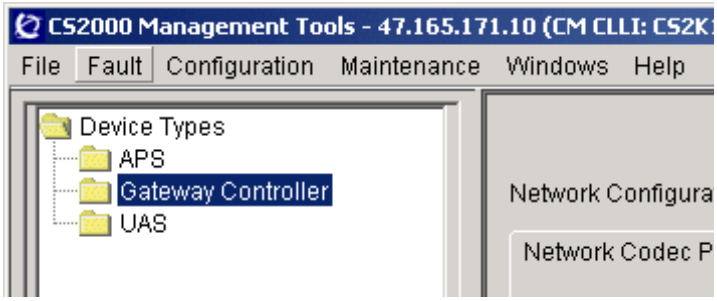
- Calls that are being set up
- Calls that are currently active or stable

To reduce the risk of calls being affected, change these parameters during a low traffic period.

At CS 2000 GWC Manager client

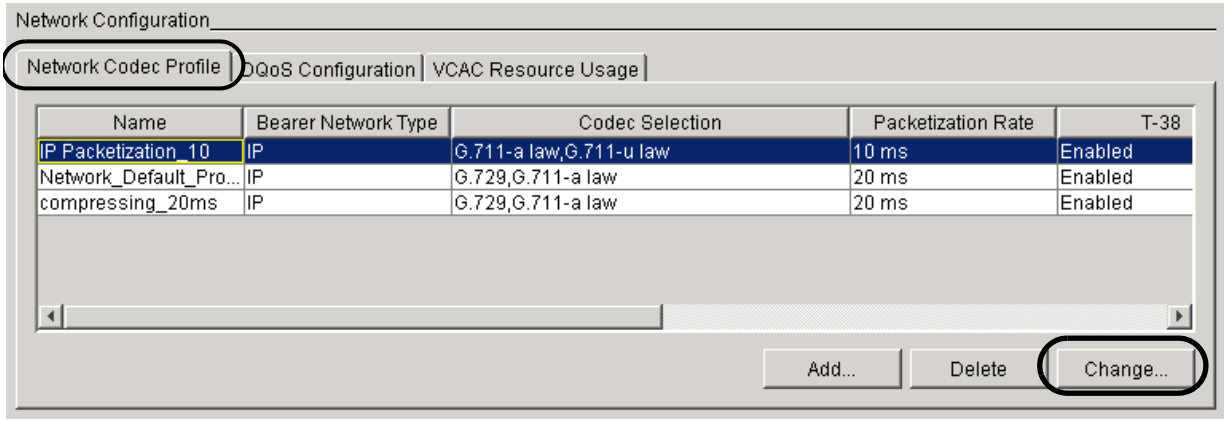
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

The Network Configuration panel is displayed to the right of the Device Types menu.



2 From the Network Configuration panel, click the **Network Codec Profile** tab.

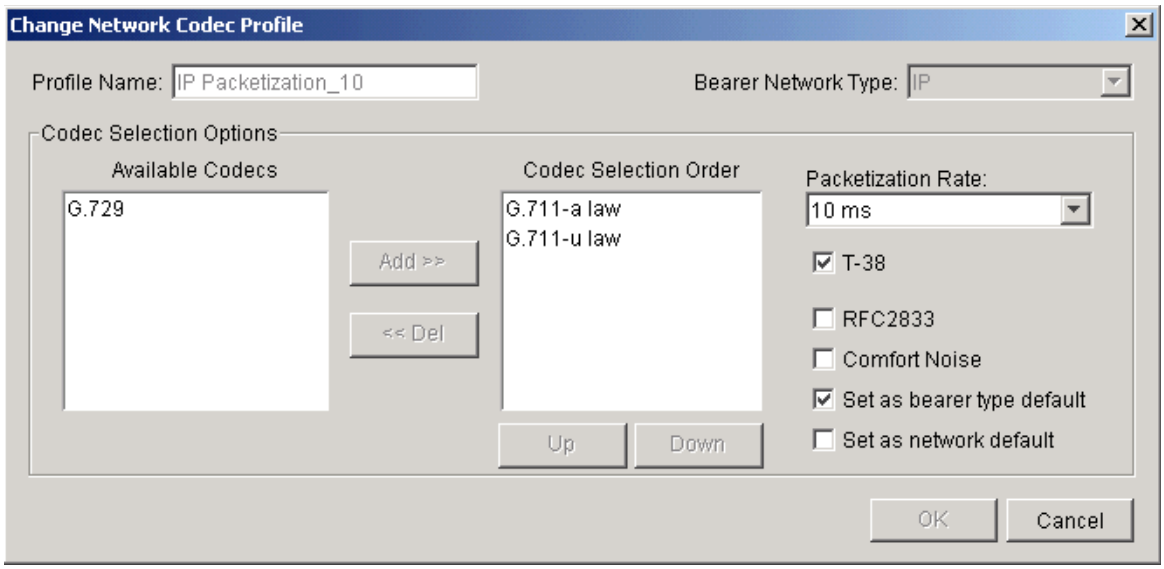
Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



3 Select one of the existing profiles in the list.

Your selection is highlighted.

4 Click the **Change** button to display the Change Network Codec Profile dialog box.



You can change the codec combination or the codec order, or both, as well as any of the options on the right-hand side of the dialog box, under Packetization Rate.

Note: You cannot change the profile name or the bearer network type.

5 If desired, change the codec combination for the new profile.

Note 1: The codecs are used in the order in which they are selected in Codec Selection Order list, from top to bottom.

Note 2: Only certain combinations of codecs are supported, in a certain order.

Refer to the table Valid codec combinations for bearer network types on page 42 to view the valid codec combinations for each bearer network type.

- Any GWC node using a profile will initially attempt to communicate with a media gateway using the *first* codec listed.
- If the first codec is not suitable, then the GWC node will use the *second* codec listed (if present).
- If the second codec is also not suitable, then the GWC node will use the *third* codec listed (if present).

Perform the following steps to select a codec combination:

a Select a codec from the list of available codecs.

The available codecs depend on the bearer network type you selected previously.

b Click the **Add >>** button to add the codec to the Codec Selection Order list.

If your profile requires more than one codec, select the codecs in the order they will be used.

You can remove a codec from the list by clicking the **<< Del** button.

c If necessary, repeat the previous step until you have selected the codecs required for the profile.

d If necessary, adjust the order of your codecs by selecting a codec in the Codec Selection Order list and clicking the **Up** or **Down** button.

e Repeat the previous steps until you have selected the codecs for your profile.

The following table lists the supported codec combinations for each bearer network type.

Valid codec combinations for bearer network types (Sheet 1 of 2)

Bearer network type	Valid codec combinations (in order)		
	1st	2nd	3rd
IP	G.729	G.711-a law	G.711-u law
	G.729	G.711-u law	G.711-a law
	G.729	G.711-a law	
	G.729	G.711-u law	
	G.711-a law	G.711-u law	G.729
	G.711-u law	G.711-a law	G.729
	G.711-a law	G.729	
	G.711-u law	G.729	
	G.711-a law	G.711-u law	
	G.711-u law	G.711-a law	
	G.711-a law		
	G.711-u law		
AAL1	G.711-u law		

Valid codec combinations for bearer network types (Sheet 2 of 2)

Bearer network type	Valid codec combinations (in order)		
	1st	2nd	3rd
AAL2	G.729	G.711-a law	
	G.729	G.711-u law	
	G.729	G.711-a law	G.711-u law
	G.729	G.711-u law	G.711-a law
	G.726-32	G.711-a law	G.711-u law
	G.726-32	G.711-u law	G.711-a law
	G.726-32	G.711-a law	
	G.726-32	G.711-u law	
	G.711-a law	G.711-u law	
	G.711-u law	G.711-a law	
	G.711-a law		
	G.711-u law		

6 If desired, change the Packetization Rate for the profile using the drop-down menu.

The packetization rate option is available only on IP bearer networks.

The options are:

- 10 milliseconds (default)
- 20 milliseconds

7 If desired, select (or de-select) the T-38 check box to change whether the profile supports T-38 real-time facsimile (fax) capability.

T-38 is available only on IP bearer networks.

This option results in the GWC node including T.38 in the list of requested media types to the associated media gateways during call setup. T.38 is the ITU-T standard for real-time transport of Group 3 fax over IP.

T-38 is not selected by default.

Note: T-38, RFC2833 and Comfort Noise are local control options in which a GWC sends messages to media gateways over NCS and MGCP protocols. Each of these options is available only on IP bearer network types.

8

ATTENTION

RFC 2833 is not currently supported on the CS 2000 for gateways using the NCS protocol. Any GWC node hosting NCS gateways must use a network codec profile that has RFC 2833 disabled (check box not selected).

If desired, select (or de-select) the RFC2833 check box to change whether the profile supports the transmission of tones over IP.

RFC 2833 is available only on IP bearer networks.

RFC 2833 indicates whether the profile supports Real-Time Protocol (RTP) payload for Dual-Tone Multifrequency (DTMF) digits, telephony tones and telephony signals.

This allows each GWC node using the profile to send standard tones to a media gateway during call setup. RFC 2833 is an Internet Engineering Task Force (IETF) standard for the transport of tones over IP.

RFC2833 is not selected by default.

9 If desired, select (or de-select) the Comfort Noise check box to change whether the profile supports this option.

Comfort noise is available only on IP bearer networks.

This allows each GWC node using the profile to send comfort noise, a sound that is generated and played to the line when silence suppression is used (when no voice packets are being received). This is to reassure the user that the connection is still active.

Comfort noise is not selected by default.

10 If desired, select (or de-select) the Bearer Type Default check box to change whether the profile is the default for the bearer network type (selected previously).

Only one default codec can be set for each bearer network type (IP, AAL1 or AAL2) defined on your CS 2000.

When adding a GWC node using procedure Add and configure a GWC node on page 123, the default codec appears as the default setting for the option “GWC codec profile”, based on the bearer network selected.

This option is not selected by default.

Note: You can enable the bearer type default setting for a profile when an existing profile using the same network type has the same setting already enabled. If you proceed, the bearer type default setting for the existing profile will be automatically disabled.

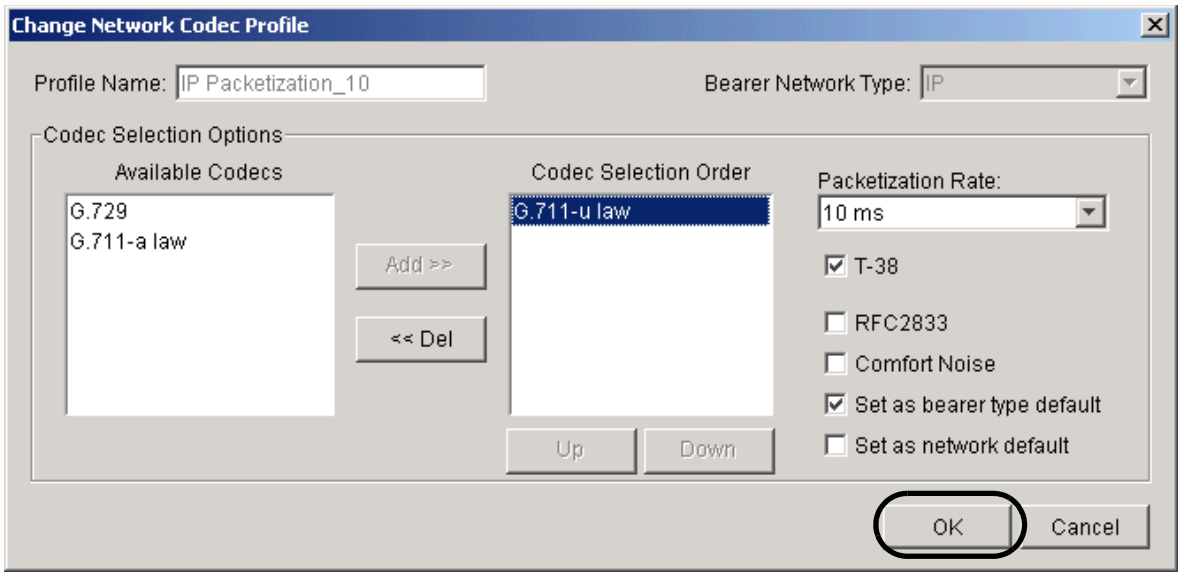
11 If desired, select (or de-select) the Network Default check box to change whether the profile is the default for the entire network.

Only one network codec profile can be set as the network default. The network default setting is used in the following circumstances:

- When upgrading from an SN06.2 to an SN08 software load of the CS 2000 Management Tools, the initial SN08 network default codec profile is based on the pre-SN07 network configuration.
- When you perform a CS 2000 data integrity audit, the system uses this setting to identify and correct any network configuration mismatches between the GWC EM database and the XA-Core

This option is not selected by default.

Note: You can enable the network default setting for a profile when an existing profile has the same setting already enabled. If you proceed, the network default setting for the existing profile will be automatically disabled.

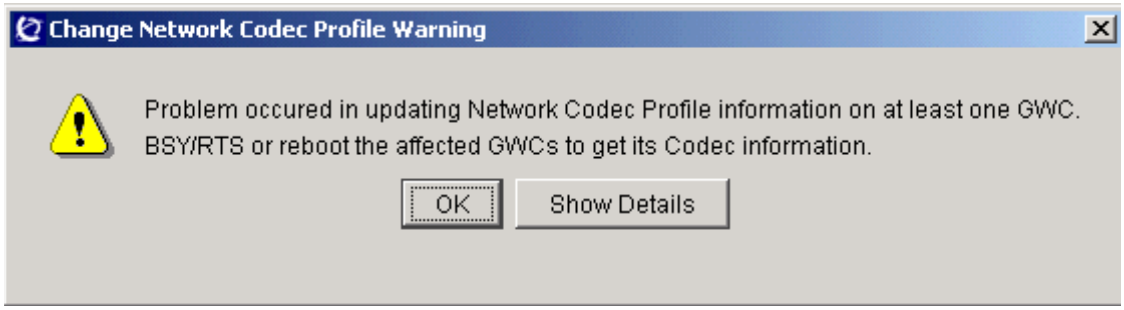


12 Click the **OK** button when you have finished changing the profile.

Note 1: If the profile is unchanged, or if any required settings are missing, the **OK** button will not be available.

Note 2: If you have changed the codec combination to an invalid setting, you will see an error message. Refer to the table Valid codec combinations for bearer network types on page 42.

The changes to the profile are propagated to any GWC units that are configured to use the profile. The changes are immediately propagated to GWC units in service. If any GWC units are out of service, a warning message will appear (see below), and the changes will be propagated when the card is rebooted.



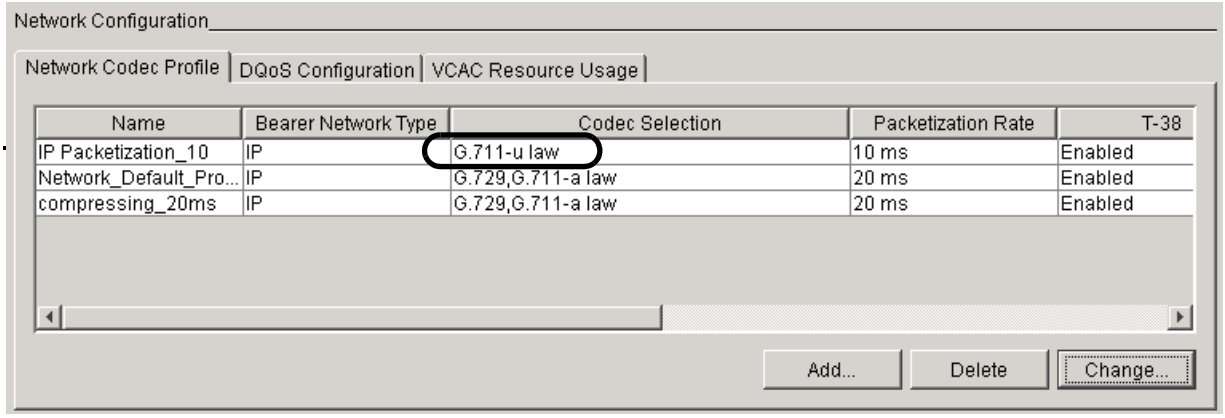
This warning is an information message only. The change will appear in the list of network codec profiles.

Click the **Show Details** button to identify the GWC unit(s) that must be rebooted. Click the **OK** button to close the message

Reboot a unit using the following steps:

1. Perform procedure “Disable (Busy) GWC card services” in the *Gateway Controller Security and Administration* NTP, NN10213-611, to busy the inactive unit.
2. Perform procedure Lock a GWC card on page 519 in this NTP to lock the inactive unit
3. Perform procedure Unlock a GWC card on page 523 in this NTP to unlock the inactive unit. The card is booted and provisioning data is downloaded following the unlock operation.
4. Perform procedure “Enable (RTS) card GWC services” in the *Gateway Controller Security and Administration* NTP, NN10213-611, to return the inactive unit to service.
5. If necessary, perform procedure “Invoke a manual protection switch (warm swact)” in the *Gateway Controller Security and Administration* NTP, NN10213-611, to swact the GWC cards in the node.
6. If necessary, repeat step 1 through step 4 in this list for the mate GWC unit (now inactive) in the node.

13 Verify that the change to the profile appears on the list of network codec profiles.



14 If necessary, return to step 2 to change the parameters of another profile.

15 The procedure is complete.

Delete a network codec profile

Purpose of this procedure

Use this procedure to delete a network codec profile using the CS 2000 GWC Manager.

For an explanation of the supported network codec profile configuration, refer to procedure Add a network codec profile on page 19.

When to use this procedure

Use this procedure when you need to delete an existing network codec profile.

Note: You cannot change the profile name or the bearer network type of an existing profile. If you need to do so, use this procedure to delete the profile and then refer to procedure Add a network codec profile on page 19 to add a new profile with the settings you require.

Prerequisites and guidelines

Prerequisites

Your CS 2000 Management Tools software (including the CS 2000 GWC Manager) must be upgraded to an SN08 version.

The CS 2000 must be configured with at least one network codec profile.

Guideline

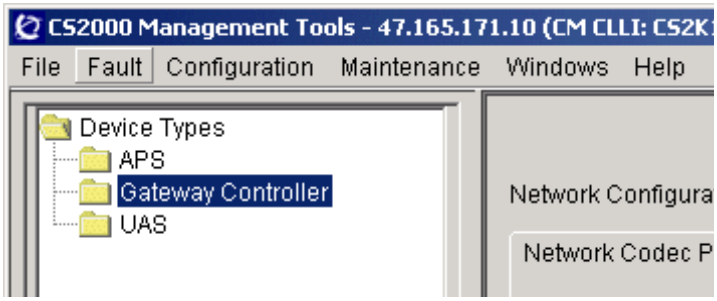
You cannot delete a network codec profile that is currently selected to be used by a GWC unit in your network. You must first remove the profile from any GWC units that are currently using the profile.

Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

The Network Configuration panel is displayed to the right of the Device Types menu.

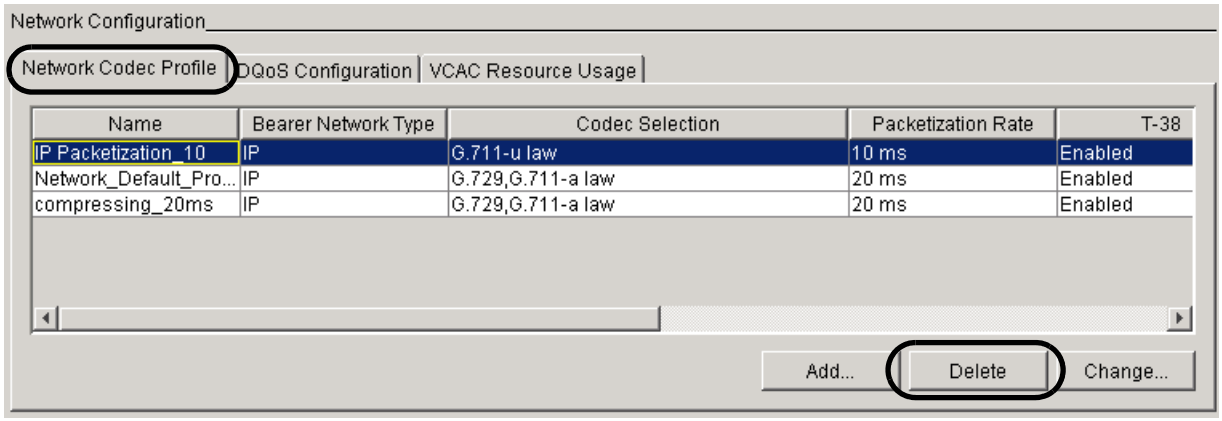


2 From the Network Configuration panel, click the **Network Codec Profile** tab to display the Network Codec Profile pane.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.

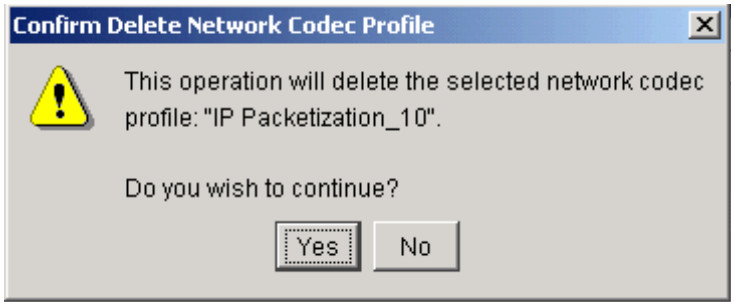
3 Select one of the existing profiles in the list.

Your selection is highlighted.



4 Click the **Delete** button to remove the profile.

5 At the prompt, click **Yes** to confirm the deletion.



Note: The following error message is displayed if you try to delete a profile that is currently used on one or more GWC nodes.

6 If necessary, return to step 2 to delete another profile.

7 The procedure is complete.

Provision advice of charge option

Purpose of this procedure

Complete this procedure if you want GWCs to support advice of charge (AOC) functionality. To provision such support, you must add the AOC option to the SERVTOPTS field in table SERVRINV in the XA-Core.

Note: The AOC option applies only to the international market.

When to use this procedure

Perform this procedure as required to add the AOC option.

Prerequisites and guidelines

The GWCs must have already been provisioned, using the CS 2000 GWC Manager. You must know the names of the GWCs for which you are going to provision the AOC option. The GWC names are specified during GWC provisioning.

This procedure does not refer to any common procedures.

Action

At the MAP terminal

1 Start the table editor. At the user interface prompt on any MAP screen type

>TABLE SERVRINV

and press the **Enter** key.

Example of system response:

```
TABLE: SERVRINV
```

2 Use the POS command to move to the tuple that you want to edit. Type

>POS <gwc-name>

and press the **Enter** key.

For example, if the name of the GWC is GWC 22, type

>POS GWC 22

and press the **Enter** key.

Example of system response:

```
GWC 22 IP 172 16 0 112 (POTS POTSEX)
(ABTRK DTCEX) $UK100 $
```

3 Indicate that you intend to change the value of the SERVROPTS field in the tuple. Type

>CHA SERVROPTS

and press the **Enter** key.

Example of system response:

```
SERVROPTS:
```

4 Specify the AOC option. Type

>AOC

and press the **Enter** key.

Example of system response:

```
TUPLE TO BE CHANGED:

GWC 22 IP 172 16 0 112 (POTS POTSEX)
(ABTRK DTCEX) $UK100 AOC

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

5 Confirm the change. Type

>Y

and press the **Enter** key.

Example of system response:

```
TUPLE CHANGED:
```

6 Repeat steps 2 through 5 for every GWC card that requires the AOC option.

7 Exit from the table editor. Type

>QUIT

and press the **Enter** key.

8 Busy (disable) and switch call processing activity (SwAct) each GWC card on which you have provisioned the AOC option.

Refer to the *Gateway Controller Security and Administration* NTP, NN10213-611 for the applicable procedures.

Note: This causes the XA-Core to send the updated information to each affected GWC.

9 The procedure is complete.

Set or change network DQoS configuration parameters

Purpose of this procedure

Use this procedure to configure network-level dynamic quality of service (DQoS) for cable access networks.

DQoS is a mechanism by which cable gateways (modems and multimedia terminal adapters [MTA]) negotiate with the GWC to gain access to the cable access network. In the process, the cable gateways also specify how much bandwidth they need based on the type of connection requested (voice, video, data). The service is called dynamic QoS because the negotiation is done for each call or connection. This prevents some theft of service scenarios, allows more efficient management of cable access bandwidth since bandwidth is allocated based on the type and requirements of the connection.

When to use this procedure

Use this procedure after you have performed initial network setup using procedure Add a network codec profile on page 19.

Prerequisites and guidelines

The following guidelines apply to using this procedure:

- The DQoS configuration can be set or changed, but once set, it cannot be disabled.
- A policy enforcement point (PEP) server must be configured in the network. Refer to procedure Add a policy enforcement point (PEP) server on page 401 to accomplish this task.

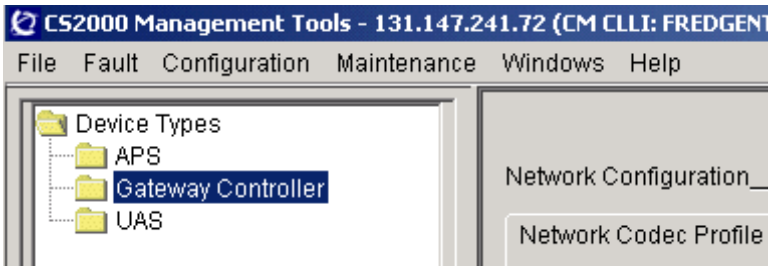
Factors that affect whether calls processed through a cable gateway are subject to DQoS processing include:

- policy information used by the PEP device
- the state of the DQoS capability on the media gateway

Action

At the CS 2000 GWC Manager client

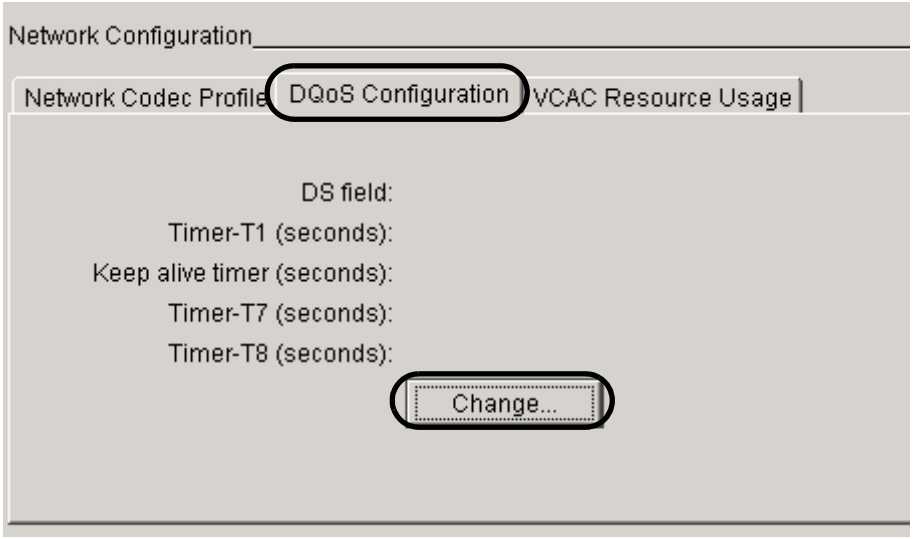
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



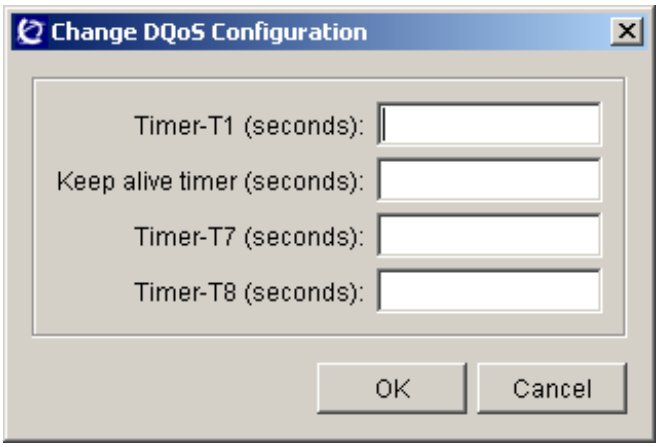
2 In the Network Configuration panel, click the **DQoS Configuration** tab to display the current DQoS configuration (if applicable).

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.

3 Click the **Change** button to view the Change DQoS Configuration dialog box.



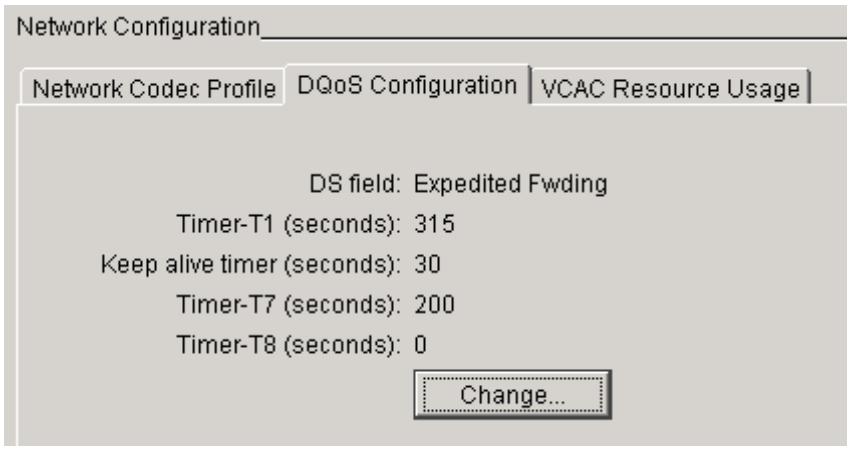
4 Enter or change information inside the appropriate field according to the values specified in the following table, then click the **OK** button.



Field	Values	Description
Timer-T1 (seconds):	0 - 32,767	Described in the DQoS Specification. There is no default value. Suggested value: 315
Keep alive timer (seconds):	1 - 2,147,483,647	Specifies the maximum time interval over which Common Open Policy Service (COPS) message must be sent or received. A value of 0 implies infinity. There is no default value. Suggested value: 30
Timer-T7 (seconds):	0 - 32,767	Described in the DQoS Specification. There is no default value. Suggested value: 200
Timer-T8 (seconds):	0 - 32,767	Described in the DQoS Specification. There is no default value. Suggested value: 0

5 At the confirmation dialog box, click **OK** to continue. If one or more GWCs fail during the update, click the **Show Details** button to view the detailed results.

The subscriber information is displayed in the DQoS Configuration panel, as shown below.



6 The procedure is complete

Configure a recurring data integrity audit

Purpose of this procedure

Use this procedure to configure data integrity audits to occur at specified times. You can schedule any of the following audits:

- line audit
- trunk audit
- V5.2 audit
- CS 2000 (CS2K) data integrity audit

For more information about each audit, refer to the appropriate procedure describing how to perform the on-demand audit. Refer to these procedures in the *Gateway Controller Fault Management* NTP, NN10202-911.

When to use this procedure

Use this procedure to schedule audits as required.

Note: If you are scheduling data integrity audits, remember that only one audit of any specific type can be in progress at one time. For example, an in-progress line data integrity audit blocks any attempt to run an on-demand line audit. Similarly, if you run an on-demand trunk audit, and if that audit is still in progress at the start time of a scheduled trunk audit, the scheduled audit will not occur.

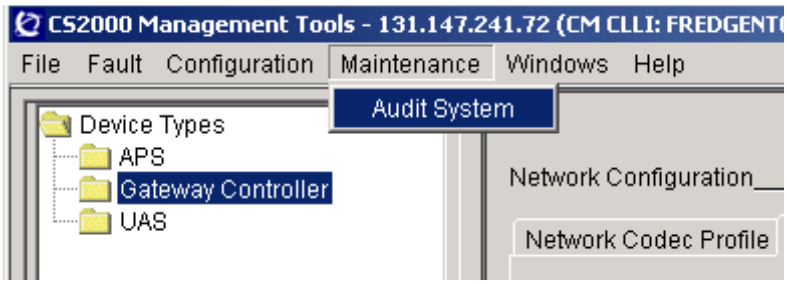
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

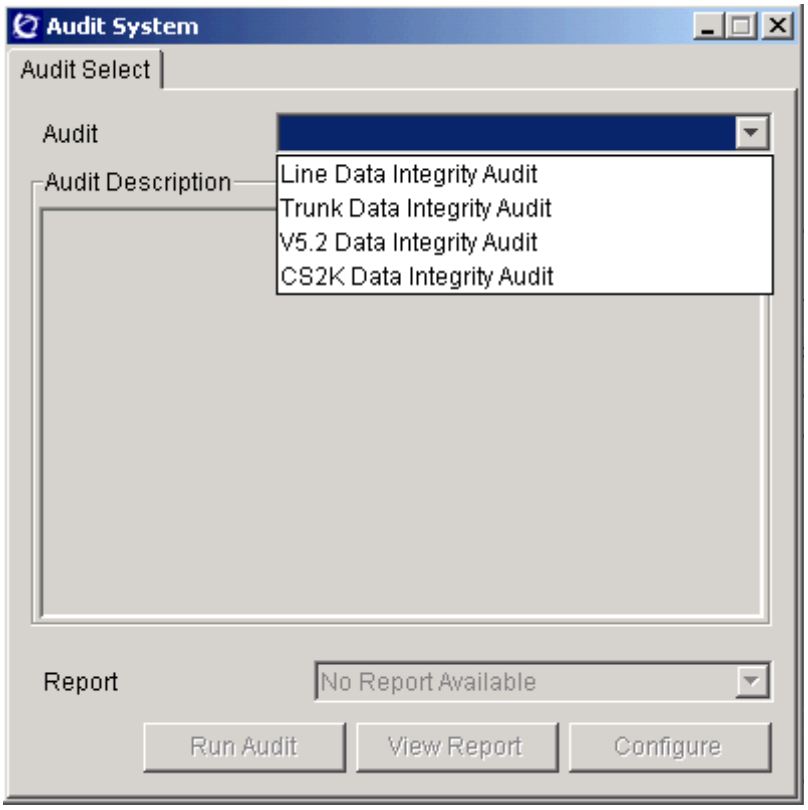
Action

At the CS 2000 GWC Manager client

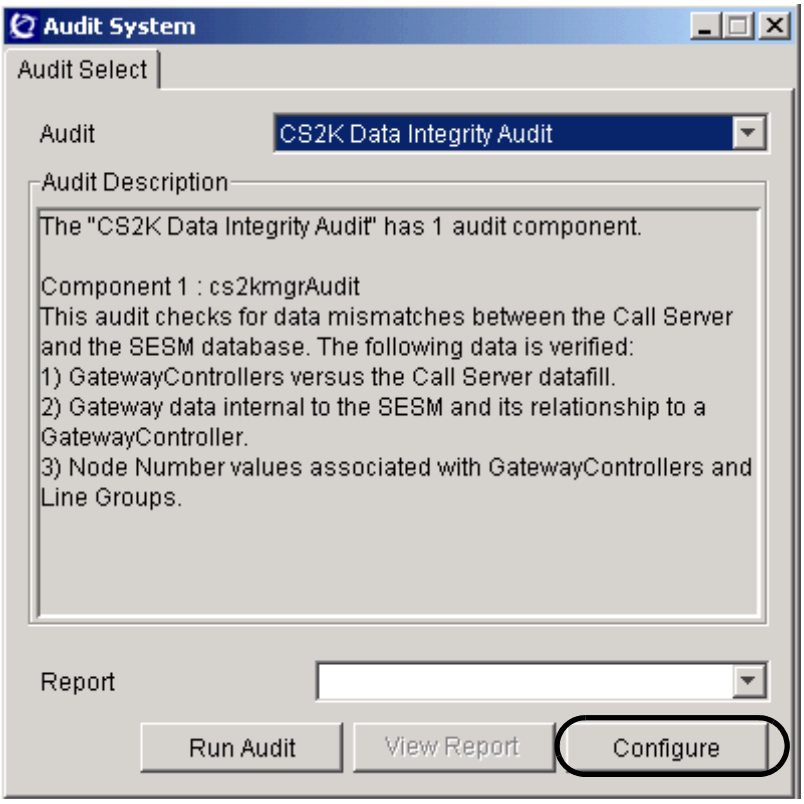
1 At the CS 2000 Management Tools window, click on the **Maintenance** menu and select **Audit System**.



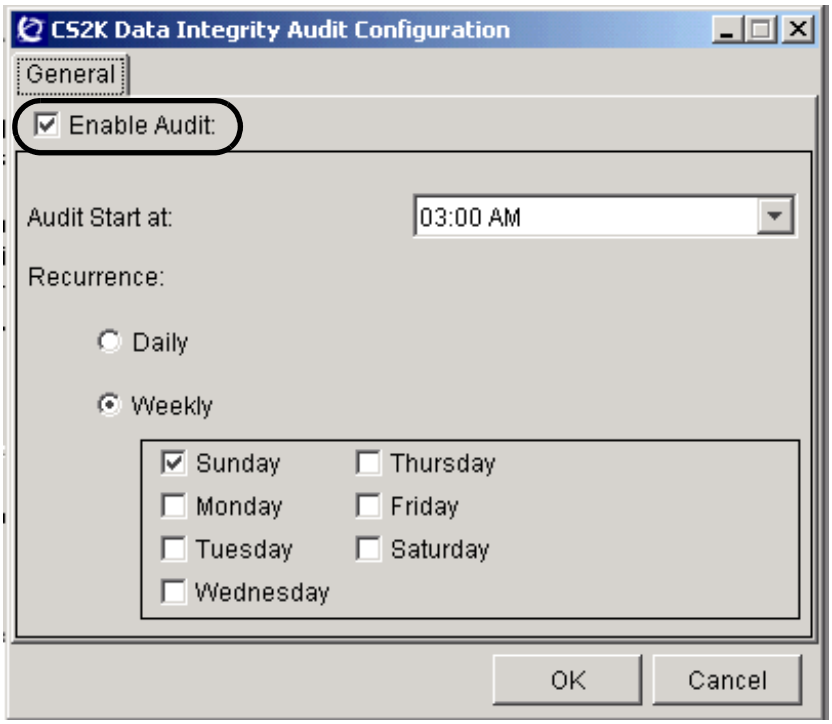
2 At the Audit System dialog box, select any one of the audits from list displayed in the drop-down menu.



3 Click the **Configure** button.



4 In the Data Integrity Audit Configuration dialog box, specify the desired schedule, including the start time and recurrence details.



5 Ensure that the Enable Audit check box is selected.

6 Click the **OK** button.

7 The procedure is complete.

Add or change the RMGC default domain

Purpose of this procedure

This procedure explains how to add or change the default domain name for the redirecting media gateway controller (RMGC) used in a network. A network may have one or more RMGCs configured.

RMGC functionality allows small line gateways to be pre-configured to reference a default address for the CS 2000.The RMGC application is a registration agent that enables MGCP and NCS gateways to obtain the IP address or fully qualified domain name (FQDN) of their associated GWC from the RMGC, rather than having it pre-configured. The default domain name is used by NCS and MGCP gateways to obtain the IP address or FQDN of their associated media GWC from the RMGC.

When to use this procedure

Use this procedure when you are adding or changing the RMGC capability to your network and you wish to change the default domain name.

Domain name service (DNS) is required only for configuring an HTTPS security certificate or an RMGC. You need to enter a GWC domain name only if you are using either of these features. For information on configuring HTTPS, refer to CS 2000 Management Tools information in the *ATM/IP Solution-level Configuration Management* NTP, NN10409-500.

Prerequisites and guidelines

The following guidelines apply to using the RMGC service:

- You must configure a GWC node in the CS 2000 with the Gateway Controller service profile AUDCNTL_RMGC or AUDCNTL_RMGCINTL. This node is referred to as an RMGC. Refer to procedure Add or change the RMGC default domain on page 63.
- Each RMGC capacity is limited to 115,000 gateways.
- Only MGCP and NCS media gateway protocols are supported with the RMGC application.
- In order to use the RMGC application, the FQDNs of media GWCs must be in the following format: <gwcname>.<cmshortCLLI>.<domain-name>

The media GWC name can consists of up to seven characters and it is typically in the format of: GWC-XXX.

The cmshortCLLI value is datafilled in table OFCENG as office parameter OFFICE-CLLI-NAME. It is also used to configure the CS 2000 Core Manager or Core and Billing Manager (CBM) and is used as the CM HOSTNAME when configuring the CS 2000 Management Tools Server. The value is made up of RFC1034 compliant characters. Entering invalid or non-RFC1034 compliant characters (such as the underscore character) while provisioning these tables could render the RMGC application unusable and would be very difficult to change later.

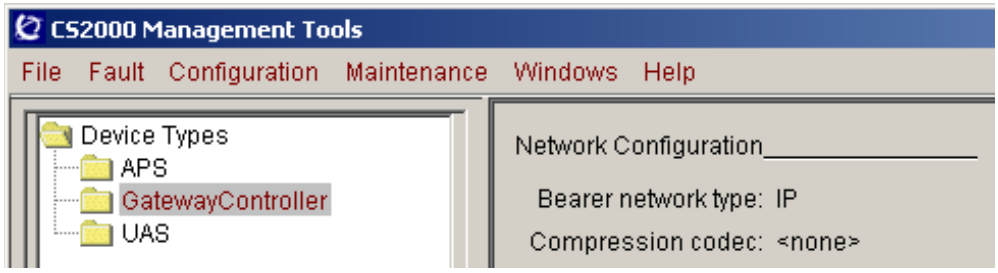
Typically only one RMGC is required for each CS 2000 network. If required, it is possible to configure multiple RMGCs. However, all RMGCs will use the same GWC default domain name.

The decision to use the RMGC capability depends on your deployment strategy for the small line gateways. If it is adequate to configure each small line gateway to reference the correct GWC, then the RMGC function may not be required. If it is difficult to configure the small line gateways to reference the correct GWC, then the RMGC capability would be desirable.

Action

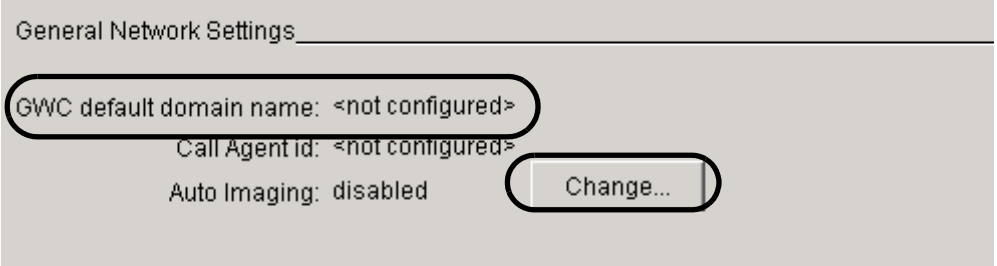
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 Look at the current status of GWC default domain name in the General Network Settings area at the bottom of the screen.

The default setting is <not configured>.

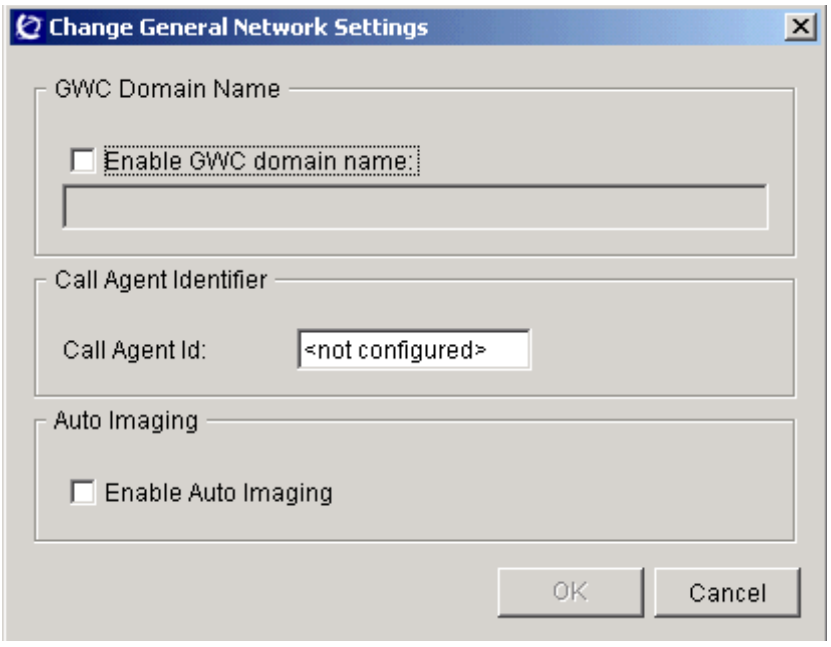


See the following links for information on how to configure the other network settings:

- Call Agent Identifier - Refer to procedure Set the call agent identifier on page 67
- Auto Imaging - Refer to procedure Enable or disable GWC software auto-imaging on page 73.

3 Click the **Change** button under General Network Settings at the bottom of the screen.

The Change General Network Settings dialog box is displayed.



4

CAUTION

Do not use invalid or non-RFC1034 compliant characters, such as the underscore character, while configuring GWC domain name in the GWC database.

Check the cmshortCLLIname in the XA-Core OFCENG table before the upgrade begins to determine if it uses any non-RFC-1034 characters. Correct this value before upgrading. Refer to the applicable *Office Parameter Reference Manual*, NTP 297-8001-855 or NTP 297-9051-855 for assistance with this task.

Select the Enable GWC domain name check box and enter a default domain name in the field below using the format shown in the following table.

Default domain naming convention
<domain-name> where <domain-name> is the IP domain name of the office site. **Example:** nortel.net ***Note:*** Ensure that your domain name uses only RFC1034 compliant characters. Consult with your site system administrator for assistance in determining the domain name for your site.

Note: You can change or remove the gateway domain name. To remove a domain name, de-select the Enable GWC domain name check box and click the **OK** button. A check is then performed for RMGCs. If an RMGC is found, the system will reject the request to remove the domain name.

5 An information box is displayed. Note any errors described in the box, then click the **OK** button.

6 The procedure is complete.

Set the call agent identifier

Purpose of this procedure

This procedure allows you to set a unique call agent identifier (ID) for each Communication Server 2000 (CS 2000) in the network.

Setting the call agent ID for a CS 2000 distinguishes it from other CS 2000 devices in your network. It also permits the automatic assignment of a unique zone ID for each network address translator (NAT)-type network zone configured in your network. When configuring a NAT zone, the system generates a zone ID (previously referred to as middlebox ID). Starting in SN07, the call agent ID is incorporated in this automatically generated number. This ensures the uniqueness of all NAT zone IDs across more than one CS 2000.

Note: It is your responsibility to ensure that the call agent ID assigned to each CS 2000 in the network is unique.

The presence of unique IDs for each CS 2000 and for each NAT zone in the network allows inter-CS 2000 trunks to be configured as intra-domain SIP-T trunks. Therefore, NAT Virtual Private Network (VPN) information for both ends of the call can be communicated and compared. This enables the flow of information between gateways hosted on different CS 2000s through the insertion of media proxies, as required. NAT information can be compared even if the gateways reside in different VPNs.

In addition to NATs, the following IDs are also automatically generated using the CS 2000 call agent ID:

- zone IDs for limited bandwidth links (LBL) and composite NAT and LBL zones
- middlebox IDs for policy enforcement points (PEP) servers and application layer gateways (ALG)

This procedure also allows you to change a CS 2000 call agent ID.

Note: Do not change the call agent ID after it has been set.

When to use this procedure

Use this procedure if you are installing a new CS 2000 in SN08. Use the procedure upon initial installation of your system or if you are adding a new CS 2000 to an existing system. The call agent ID value must be set before you can configure any of the following network components:

- NATs; refer to procedure Add an IP-VPN (NAT) zone on page 317.
- PEP servers; refer to procedure Add a policy enforcement point (PEP) server on page 401.
- LBLs; refer to procedure Add a limited bandwidth link (LBL) zone on page 331.
- ALGs; refer to procedureAdd an application layer gateway to the network (cable market) on page 419
- composite NAT and LBL zones; refer to procedure Add a composite IP-VPN (NAT) and LBL zone on page 343

Note: If you are upgrading to SN08, you may need to set the call agent ID as part of an upgrade procedure. Refer to the *Upgrading a Carrier Voice over IP Network*, NN10440-450.

You may also use this procedure if you need to change the call agent ID for a CS 2000. This should not be required for the normal operation of your network.

Note: Do not change the call agent ID after it has been set.

CAUTION
Possible downgrade problems
Changing the call agent ID will make it more difficult to rollback (downgrade) your GWC cards to an earlier software load.

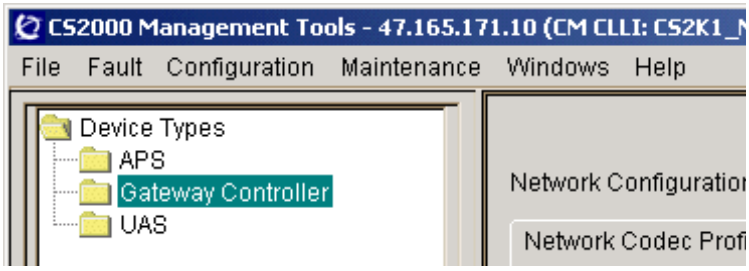
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

Action

At the CS 2000 GWC Manager client

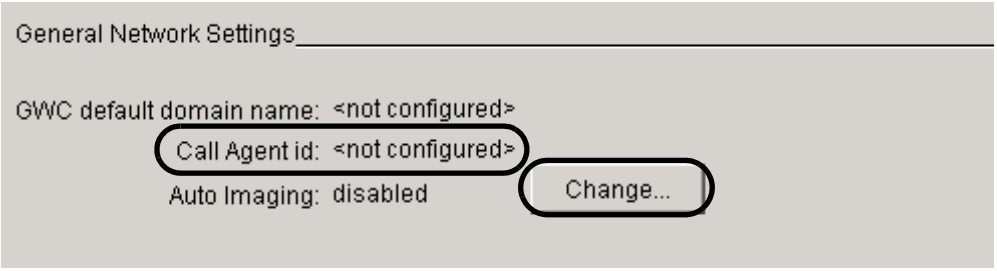
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



Look at the current Call Agent id: status in the General Network Settings area at the bottom of the screen.

Call Agent id: will have one of the following values:

- <not configured> - default
- a unique number between 1 and 255 inclusive



See the following links for information on how to configure the other network settings:

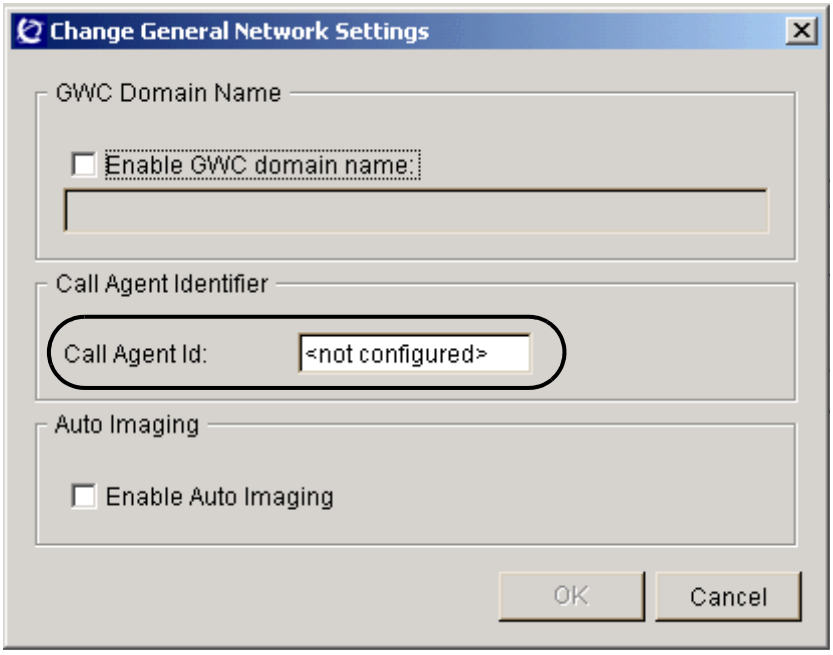
- For GWC domain name, refer to procedure Add or change the RMGC default domain on page 63.
- For auto imaging, refer to procedure Enable or disable GWC software auto-imaging on page 73.

2 Determine your next step using the following table.

If you wish to	Do
set the call agent ID for the first time	go to step 3
change a call agent ID that has already been set	go to step 4

3 Perform the following steps to set the call agent ID for the first time.

a Click the **Change** button at the bottom of the network screen to display the Change General Network Settings window.



b Click in the Call Agent id field and assign a call agent ID value.

The range of valid values is between 1 and 255 inclusive. Contact your site system administrator to determine the call agent ID you should be using.

Note 1: If the value typed is invalid, the text field is outlined in red and the OK button is disabled. If this happens, simply type a valid value in the field.

Note 2: The system does not check for call agent IDs that are already used in your network. Ensure that the call agent ID you are assigning is not already used by another CS 2000.

c Click the **OK** button.

The first time the Call Agent ID is set, the system automatically updates NAT zones which have already been configured to incorporate the new call agent ID into the NAT zone IDs. GWC units which need to be synchronized to this new data will be identified by having data synchronization alarms raised against them.

Note: To resolve a data synchronization problem, busy (BSY) and return to service (RTS) the inactive unit. When the inactive is back in service, perform a warm swact of the units in the node. Refer to the *Gateway Controller Security and Administration* NTP, NN10213-611, for supporting procedures.

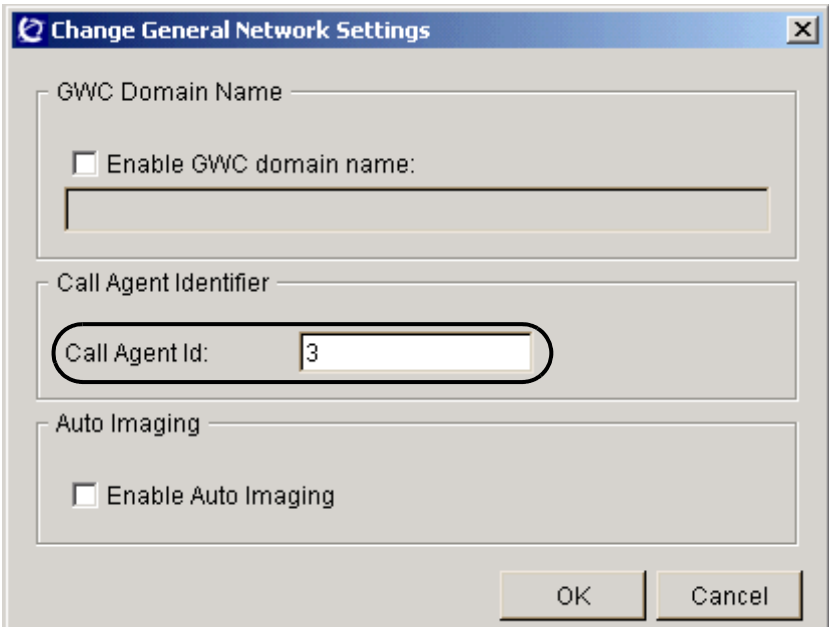
d Go to step 5.

4

CAUTION
Possible downgrade problems
Changing the call agent ID will make it more difficult to rollback (downgrade) your GWC cards to an earlier software load.

Perform the following steps to change the call agent ID.

a Click the **Change** button at the bottom of the network screen to display the Change General Network Settings window.



b Click in the Call Agent id: field and assign a new call agent ID.

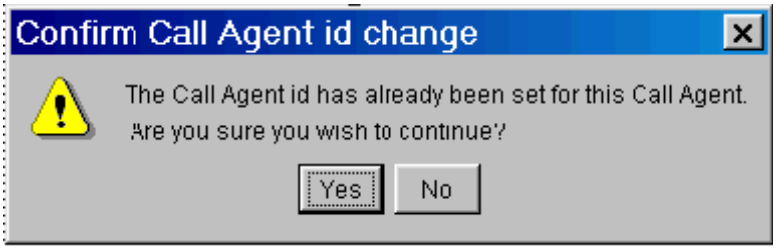
The range of valid values is between 1 and 255 inclusive. Contact your site system administrator to determine the call agent ID you must use.

Note 1: If the value typed is invalid, the text field is outlined in red and the OK button is disabled. If this happens, re-type a valid value in the field.

Note 2: The system does not check for call agent IDs that are already used in your network. Ensure that the call agent ID you are assigning is not already used by another CS 2000.

c Click the **OK** button.

When changing the call agent id for a CS 2000, the system displays the following message:



d Click **Yes** to continue with the change.

The new call agent ID will only be used in the zone ID for NATs configured after the change has been made. The zone IDs of previously configured NATs are not modified. This ensures consistency, in case some NATs have been configured into more than one CS 2000.

5 The procedure is complete.

Enable or disable GWC software auto-imaging

Purpose of this procedure

Use this procedure to enable or disable the auto-imaging of a GWC software load. Auto-imaging provides a mechanism to automatically save an up-to-date image of GWC software loads once daily to the CS 2000 Core Manager or Core and Billing Manager (CBM). For more information, refer to GWC software imaging in “Patching procedures” in *Upgrading the Gateway Controller*, NN10196-461.

Note: A procedure also exists for taking a manual GWC software image. Refer to “Take a manual GWC software image” in *Upgrading the Gateway Controller*, NN10196-461.

When to use this procedure

Use this procedure when you want to be certain that a new image of a GWC device is saved to the CS 2000 Core Manager or CBM after the device is patched. Auto-imaging is useful in an office where you apply and activate the same patches to all GWCs with the same load.

Note: Auto-imaging is not designed for an office in which different patches are applied to GWCs using the same load.

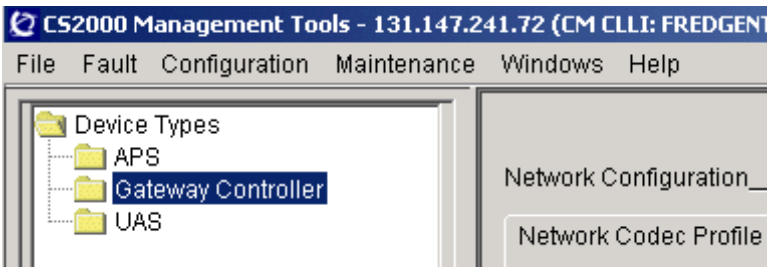
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

Action

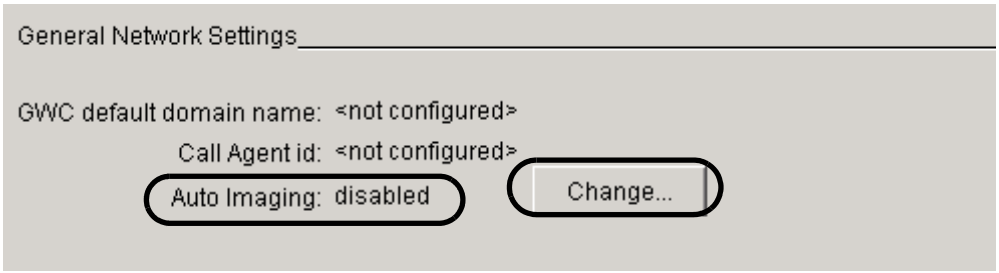
At the CS 2000 GWC Manager client

1 Select Gateway Controller from the Device Types menu.



Look at the current status of Auto Imaging in the General Network Settings area at the bottom of the screen.

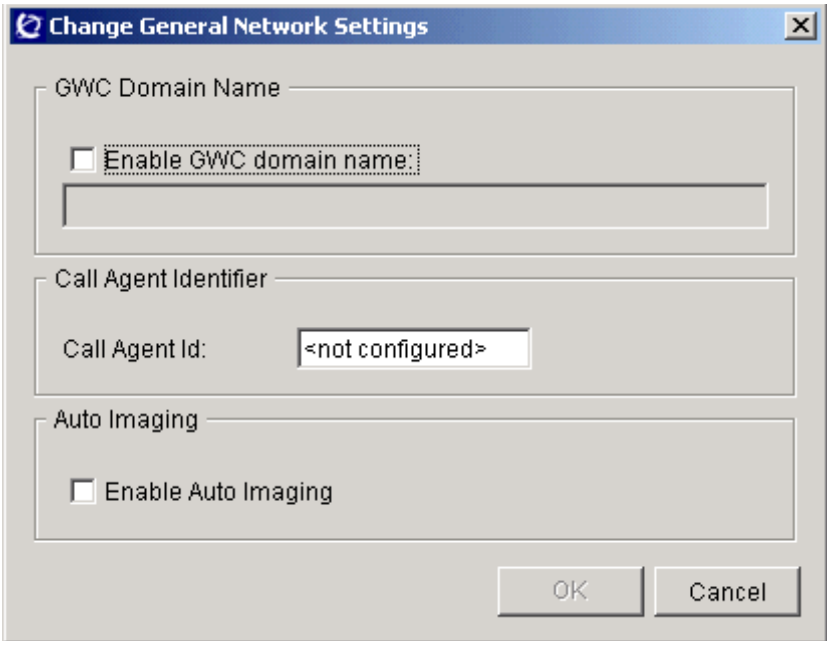
The default setting is “disabled”.



See the following links for information on how to configure the other network settings:

- GWC domain name - refer to procedure Add or change the RMGC default domain on page 63
- call agent idenifier - refer to procedure Set the call agent identifier on page 67

2 Click the **Change** button display the Change General Network Settings dialog box.



3 Select the Enable Auto Imaging check box and click **OK**. An Auto Imaging Enabled message is displayed. Click **OK** to confirm the change.

4 If necessary, you can disable auto-imaging by clicking the **Change** button. At the Change Maintenance Settings dialog box, de-select the “Auto Image Enabled” check box and click **OK**. Click **OK** at the message to confirm the change.

5 The procedure is complete.

Configure a destination for CICM location information

Purpose of this procedure

Use this procedure to configure a destination (recipient) for the location identification information of Centrex IP Client Manager (CICM) telephony clients. Location information for CICM telephony clients is used for emergency call services.

Since the location of a CICM telephony client user is not fixed in an enterprise network, the Dynamic Host Configuration Protocol (DHCP) server provides location information to the CICM client. Once the location information is available, the CICM gateway can then request the information from the CICM client. A CICM gateway reports the location information of CICM telephony clients to the Gateway Controller (GWC) over H.248 protocol.

Location information is reported to the GWC in the following sequence:

1. A CICM user logs in.
2. CICM informs the GWC of the log in.
3. If location identification reporting is enabled on the GWC, then the GWC requests CICM for location information.
4. An application running on the GWC re-packages the information and reports it to a location recipient application or device.

When to use this procedure

Use this procedure when you need to identify a destination (location recipient application or device) for the location identification information of CICM telephony clients. You can also use this procedure to disable location identification reporting to GWCs in your installation.

Perform this procedure in one of the following situations:

- You already have CICM gateways in your network. Starting in SN07, the gateways provide location information to the GWC nodes which must be forwarded to a location recipient.
- You are adding CICM gateways in your network which will provide location information to GWC nodes and you need to forward this information to a location recipient.

You can use this procedure to do the following:

- Configure the parameters for location recipient for the first time. The initial default value for each parameter is <not configured>.
- Change the values of location information recipient parameters that are currently configured.
- Reset the parameters to <not configured>

Prerequisites and guidelines

The following prerequisite applies to this procedure:

- In order for the location information to be available for forwarding to a recipient, you must have a CICM gateway in your network.
- If there are GWC nodes reporting location information, you must disable the reporting on all applicable GWC nodes before changing the values for location information recipient.

The following guidelines apply to this procedure:

- The values for a location information recipient cannot be changed if location information reporting is currently enabled on a GWC node. If there are GWC nodes reporting location information, you need to disable the reporting on all applicable GWC nodes. You can then change the values for a location information recipient and re-enable reporting.
- If the location recipient parameters are set to <not configured>, do not enable location change reporting on a GWC node.

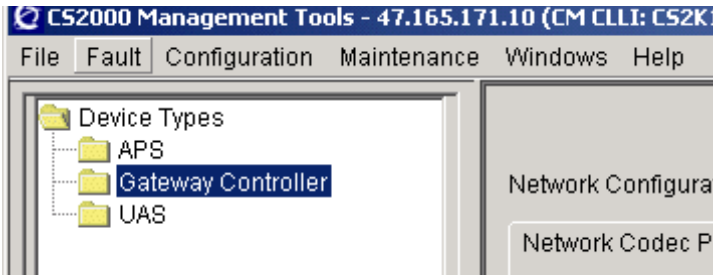
Note:

- The recipient of CICM client location information is configured at the network level for all GWC nodes in your installation.
- You can enable (or disable) location change reporting on each individual GWC node in your network. Refer to procedure Enable or disable CICM location change reporting on page 313

Action

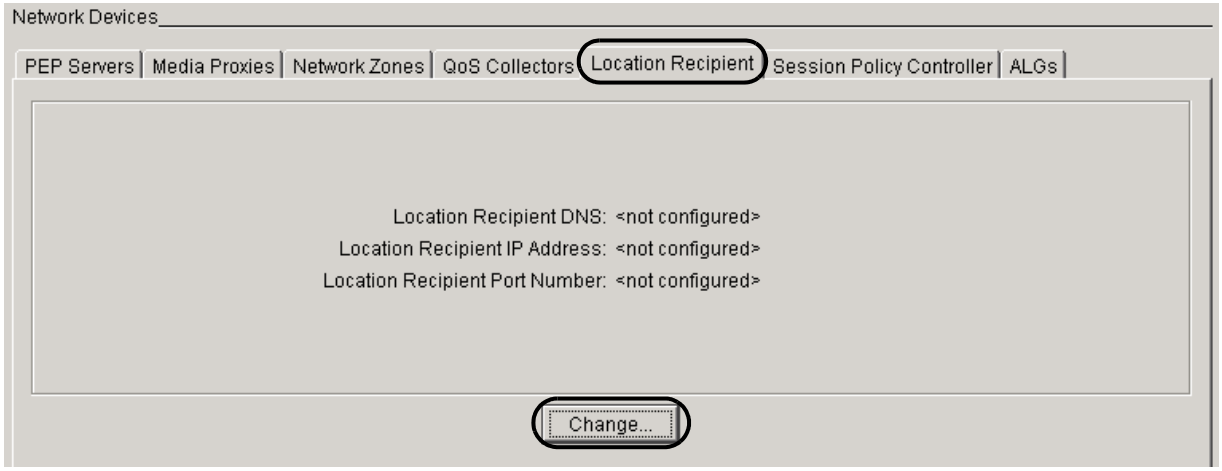
At the CS 2000 GWC Manager client

1 Select Gateway Controller from the Device Types menu.

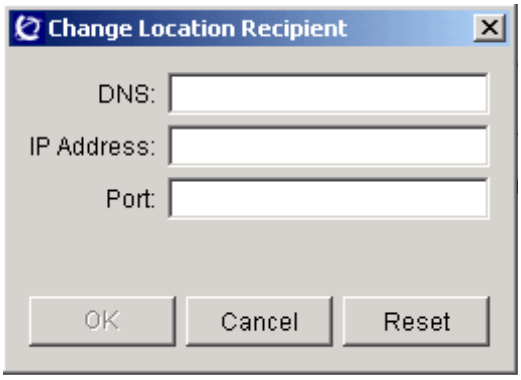


2 From the Network Devices panel, click the **Location Recipient** tab to display the current location recipient configuration.

The current settings for the location recipient are provided. The default setting for each parameter is <not configured>.



3 Click the **Change** button to display the Change Location Recipient dialog box.



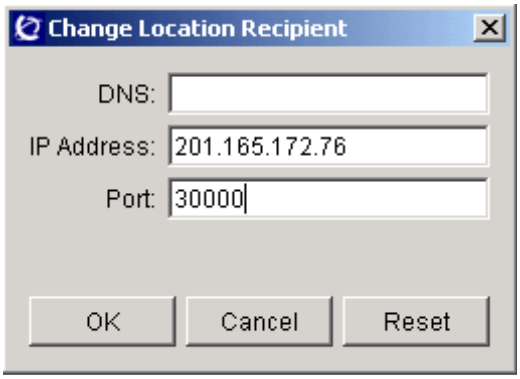
4 Determine your next step using the following table:

If you wish to	Do
change the current values for the CICM location information recipient	go to step 5
reset the current values for CICM location information recipient to <not configured>	go to step 8

5 Type new values in the following fields to specify the recipient of CICM location information.

Note: Enter text in either the DNS: field or the IP Address: field, but not both.

- In the DNS: field, type a character string representing a valid domain name server (DNS) for the location information recipient.
- In the IP Address: field, type an IP address for the location information recipient. Use the format <0-255>.<0-255>.<0-255>.<0-255>
- In the Port: field, type a port number for the location information recipient. Valid values are from 0 to 65535 inclusive.



6 Click the **OK** button to confirm changes to the location information recipient settings.

7 Go to step 10.

8 Click the **Reset** button to change the current settings for location recipient, including DNS, IP address and port, to <not configured>.

9 Click the **OK** button to confirm the changes to the location information recipient settings.

10 Confirm that the settings for location recipient have changed on the Network Devices panel.

11 The procedure is complete.

Add the Policy Controller

Purpose of this procedure

This procedure describes how to add the Policy Controller information into the CS 2000 system.

Policy Controller is a network component that provides the capability to apply policies during call processing. The information for this component must be added to the Gateway Controllers (GWC) to implement the Network VCAC (virtual call admissions control) functionality. With the Network VCAC activated, the Policy Controller, instead of each GWC, performs VCAC functions; that is, counts available resources across limited bandwidth links (LBL) and makes the connection admission decisions. GWCs communicate with the Policy Controller to determine whether a call can be set up.

For information on the Network VCAC and the Policy Controller configuration, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

For information on how to activate the Network VCAC functionality through the GWC Manager, refer to procedure Change the Network VCAC status on page 95.

When to use this procedure

Use this procedure when you need to add the Policy Controller information to the GWC nodes.

Prerequisites and guidelines

The following prerequisites and guidelines apply to this procedure:

- All network component must be upgraded to SN08.
- The Policy Controller must be commissioned and appropriately configured.

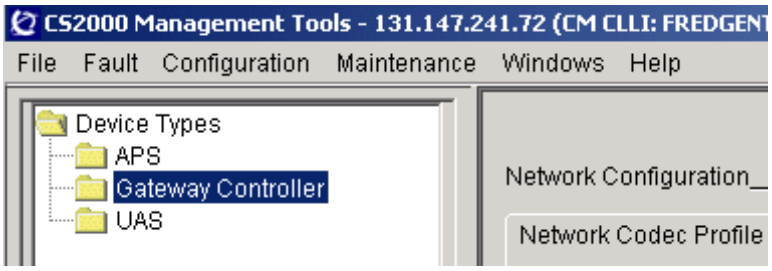
  Note: For more information, refer to the *Policy Controller Configuration Management* NTP, NN10432-511

- In SN08, only one Policy Controller can be added to each CS 2000.

Action

At the CS 2000 GWC Manager client

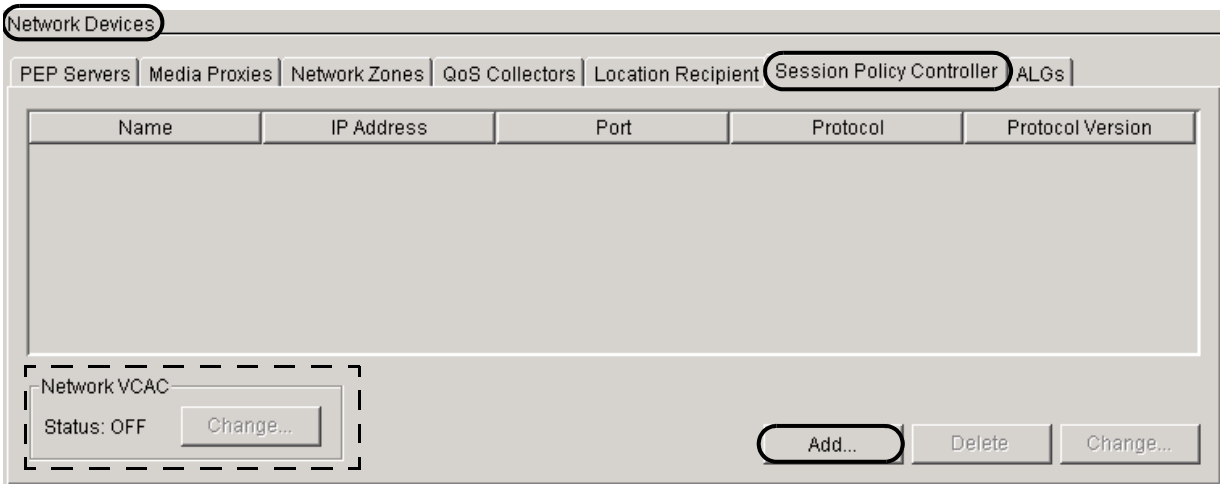
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 In the Network Devices area, click the **Session Policy Controller** tab.

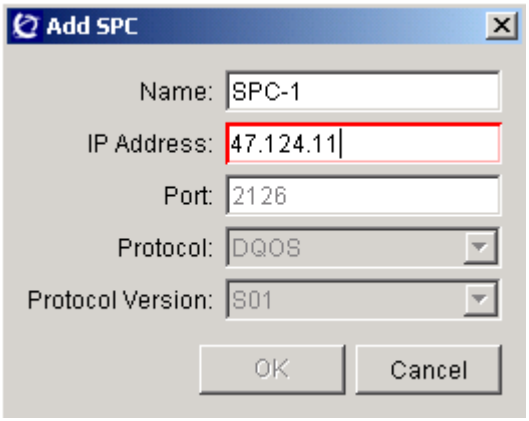
3 Click the **Add** button to display the Add SPC dialog box.

Note: In the Network VCAC section, the status is OFF and the **Change** button is disabled. It will be enabled once you complete this procedure.



4 At the Add SPC dialog box, type the applicable configuration information as described below.

Note: If you enter invalid data, the appropriate field is outlined in red and the **OK** button is disabled.



a In the Name: field, type the network name of the Policy Controller, in a fully qualified domain name (FQDN) format.

Use a domain name in the form of an absolute domain name including the host name of the device, suitable for lookup using Domain Name Service (DNS).

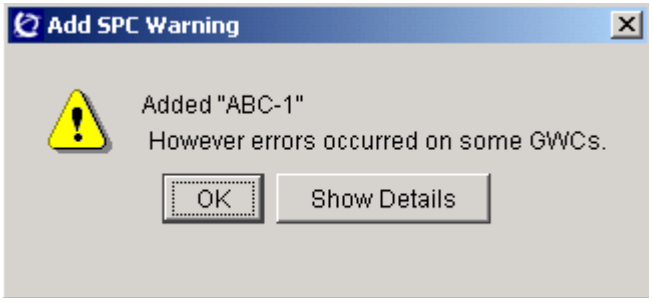
b In the IP Address: field, type the IP address of the Policy Controller in the format of:
<0-255>.<0-255>.<0-255>.<0-255>

c The Port: field is predefined with the default value of 2126. You cannot change this value.

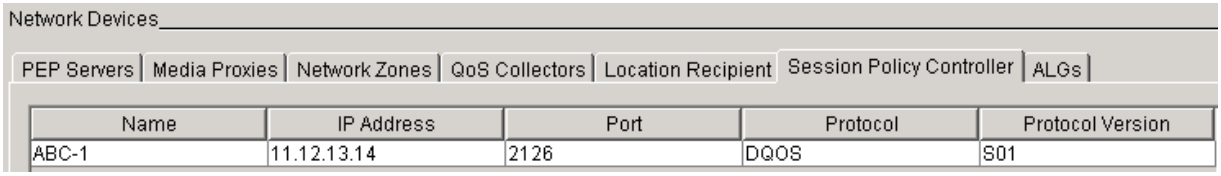
d The Protocol: and Protocol Version: fields are predefined. You cannot change these values.

5 Click the **OK** button to apply the configuration values.

Note: If the Policy Controller is not successfully provisioned on all GWC units, the system displays the following warning. Click the **Show Details** button and note all GWCs that had the error, then contact your next level of support.



6 Verify that the Policy Controller you added appears in the Session Policy Controller list.



Note: Once the Policy Controller is added, the **Add** button becomes disabled. You cannot add more than one Policy Controller.

7 The procedure is complete.

Change the attributes of the Policy Controller

Purpose of this procedure

Use this procedure to change the following information for the Policy Controller configured on the Gateway Controllers (GWC):

- name
- IP address

When to use this procedure

Use this procedure when you need to change the name or the IP address of the Policy Controller, or both.

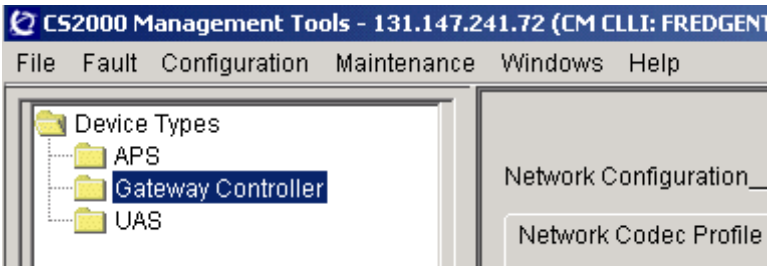
Prerequisites and guidelines

The Policy Controller must be installed and configured on the CS 2000 system.

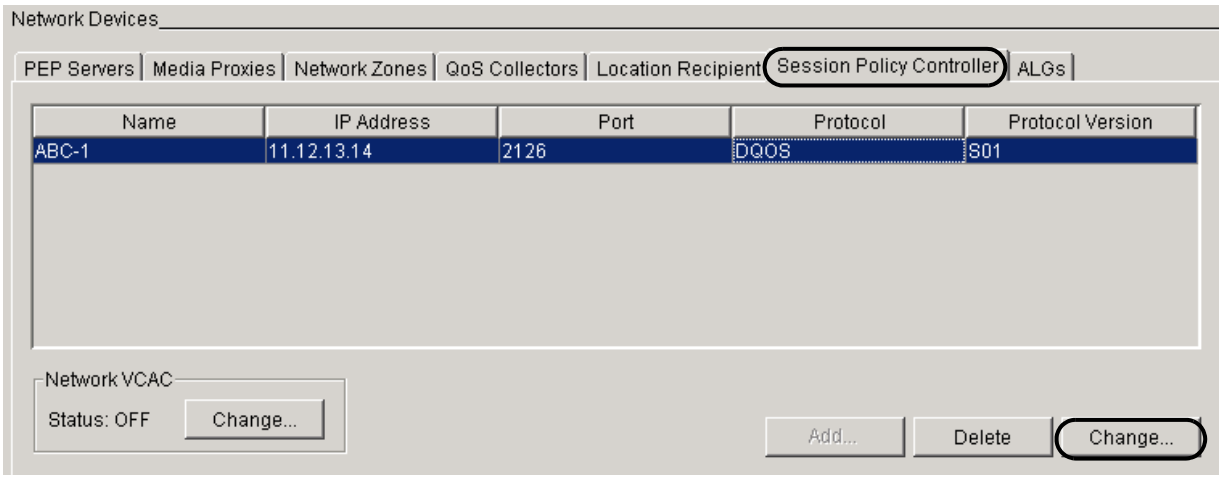
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

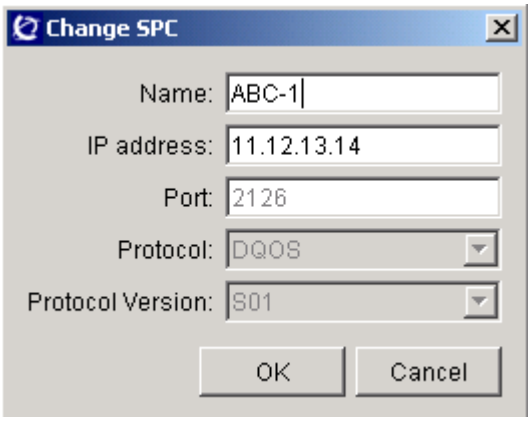


2 In the Network Devices section, click the **Session Policy Controller** tab, then click the entry in the Session Policy Controller table.



3 Click the **Change** button.

The Change SPC dialog box is displayed.

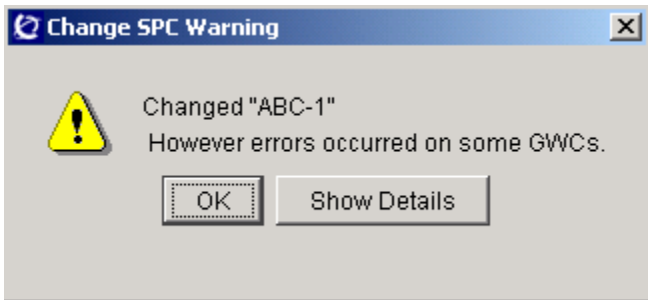


4 At the Change dialog box, enter the new data in one or both of the following fields:

- In the Name: field, enter the new name, in a fully qualified domain name (FQDN) format.
- In the IP address: field, enter the new IP address of the Policy Controller, in the format of:
  <0-255>.<0-255>.<0-255>.<0-255>

5 Click the **OK** button.

6 The Session Policy Controller table entry is updated following a successful change. If the change has not been successful on any on the Gateway Controllers, the following warning message is displayed before the entry is updated.



Click the **Show Details** button and note all GWCs that had the error, then contact your next level of support.

7 The procedure is complete.

Delete the Policy Controller

Purpose of this procedure

This procedure describes how to delete the Policy Controller information from the CS 2000 system.

When to use this procedure

Use this procedure when you need to remove the Policy Controller information from the CS 2000 system.

Prerequisites and guidelines

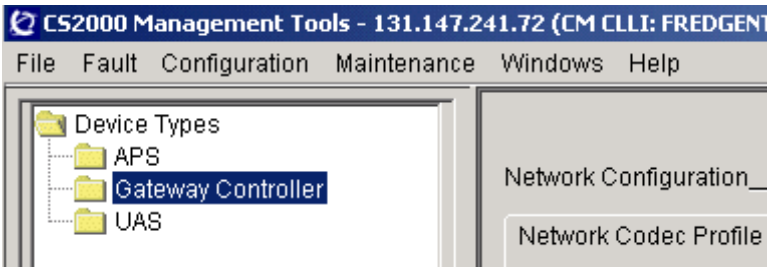
The following prerequisites apply to this procedure:

- The Policy Controller must be installed and configured on the CS 2000 system.
- You must first change the Network VCAC status to OFF. Refer to procedure Change the Network VCAC status on page 95.

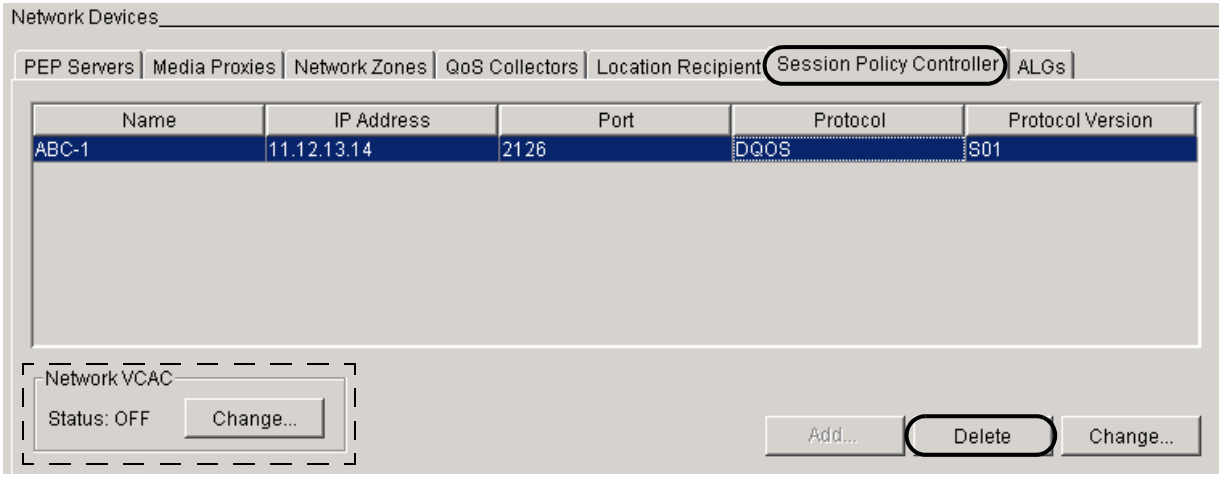
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 In the Network Devices section, click the **Session Policy Controller** tab and select the Policy Controller from the list.

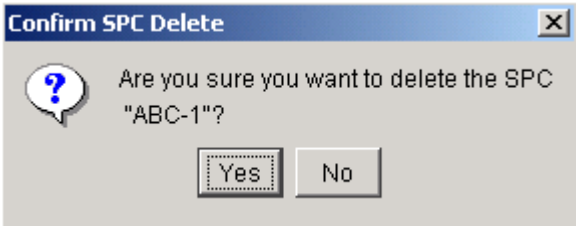


3 Click the **Delete** button.

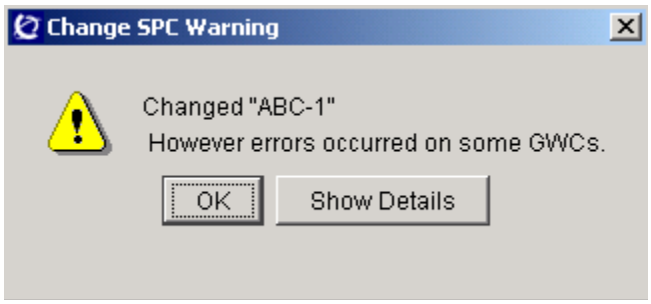
Note: Make sure that the Network VCAC status if OFF. Otherwise, the **Delete** button is disabled. If required, refer to procedure Change the Network VCAC status on page 95.

4 When prompted, click **Yes** to confirm the delete operation.

Note: If you wish to cancel the request, click **No**.



5 If the operation is successful, the Policy Controller is removed from the list. If the Policy Controller is not successfully deleted from all the GWC units, the following warning is displayed before the list is updated.



Click the **Show Details** button and note all GWCs that had the error, then contact your next level of support.

6 The procedure is complete.

Change the Network VCAC status

Purpose of this procedure

This procedure describes how to activate or de-activate the Network VCAC (virtual call admissions control) functionality.

With the Network VCAC activated (Status: ON), the Policy Controller performs VCAC functions; that is, counts available resources across limited bandwidth links (LBL) and makes the connection admission decisions. Gateway Controllers (GWC) communicate with the Policy Controller to determine whether a call can be set up.

When the Network VCAC status is OFF, basic VCAC functionality is active; that is, all VCAC functions are performed by each GWC.

For more information on the Policy Controller configuration and the migration from basic VCAC to Network VCAC, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

When to use this procedure

Use this procedure when you want to activate the Network VCAC, following the successful addition and configuration of the Policy Controller.

CAUTION
Possible service disruption
This procedure also describes how to de-activate Network VCAC. However, this operation does not guarantee that all basic VCAC functions will be restored properly.

Once the Network VCAC is ON, do not turn it OFF. If necessary, contact your next level of support before proceeding.

Prerequisites and guidelines

ATTENTION

To make sure that the Network VCAC functions correctly, all network zones must be configured identically; first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller.

The following additional prerequisites and guidelines apply to this procedure:

- All network component must be upgraded to the SN08 load.
- The Policy Controller information must be added to the CS 2000 system.

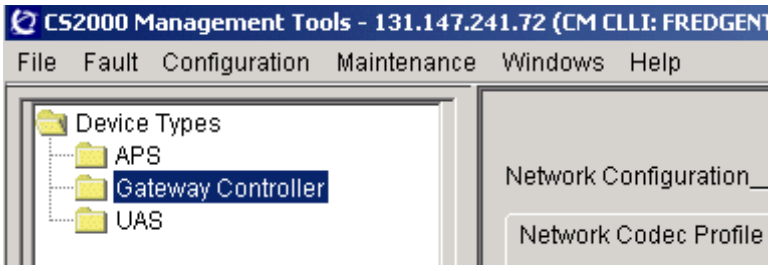
  Note: If required, refer to procedure Add the Policy Controller on page 83.

- Activating Network VCAC is network-wide. You cannot operate both Basic VCAC and Network VCAC on your CS 2000 network.
- Make sure that all connection links between GWCs and the Policy Controller are properly established and no alarms exist.
- Perform this procedure during slow traffic, when few calls are in progress.

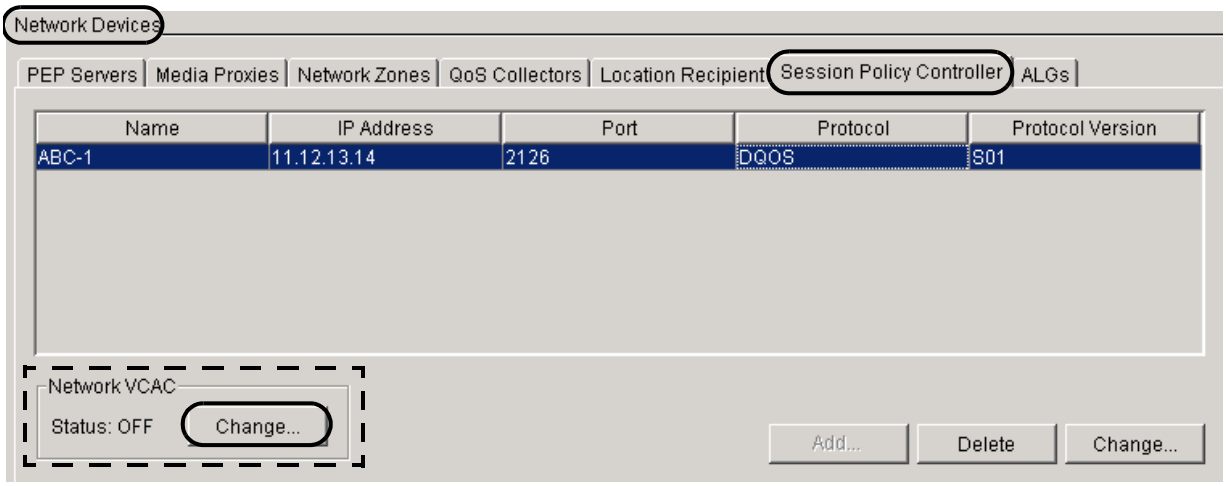
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



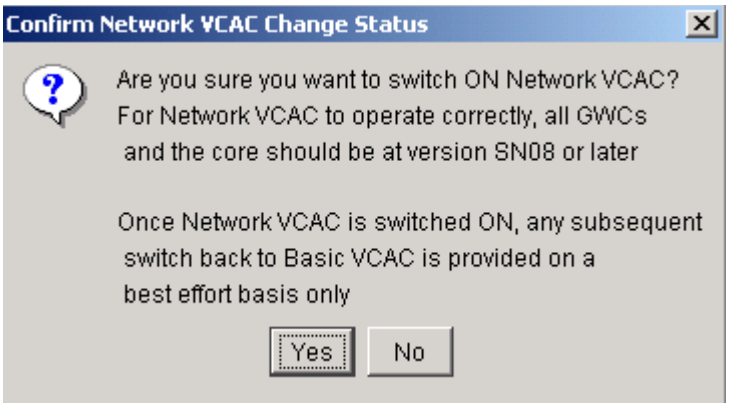
2 In the Network Devices area, click the **Session Policy Controller** tab. In the Network VCAC section, click the **Change** button.



Use the following table to determine your next step.

If you are changing the Network VCAC status to	Do
ON	go to step 3
OFF	go to step 4

3 The system displays the following confirmation message:



Click **Yes** to confirm the request and continue with step 5.

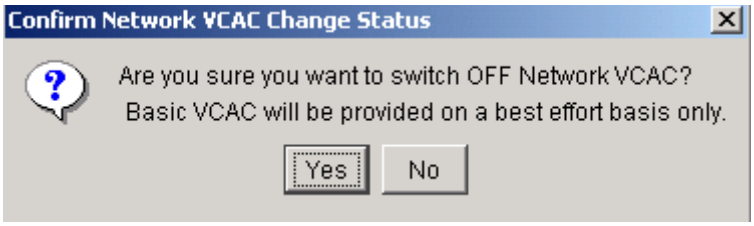
Note: If you wish to cancel your request, click **No**.

4

CAUTION
Possible service disruption
Changing the status of the Network VCAC to OFF does not guarantee that all basic VCAC functions will be restored properly.

Contact your next level of support before proceeding**.**

The system displays the following confirmation message:



Click **Yes** to confirm the request.

Note: If you wish to cancel your request, click **No**.

5 The Network VCAC Status: display is updated.

Note: If the Network VCAC status does not successfully change on all GWCs, a warning message is presented before the display is updated. Click the **Show Details** button and note all GWCs that had the error, then contact your next level of support.

6 The procedure is complete.

Review available network devices

Purpose of this procedure

Use this procedure to view the status and availability of a network devices and resources in the CS 2000 GWC Manager database. You can view the following devices or resources using this procedure:

- policy enforcement point (PEP) servers
- media proxies
- network address translator (NAT) network zones
- limited bandwidth link (LBL) network zones
- composite NAT-LBL network zones
- quality of service (QoS) collectors
- location recipient - for CICM client location ID information
- Policy Controller
- Network VCAC (virtual call admission control) status
- application layer gateway (ALG)

Note: All information available using this procedure is applicable to the entire network, rather than any specific GWC node.

When to use this procedure

Use this procedure when you need information about a specific network resource.

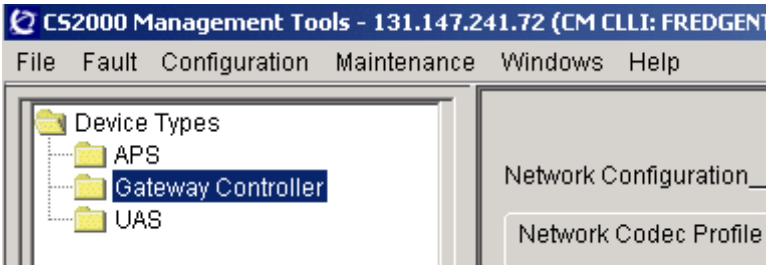
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

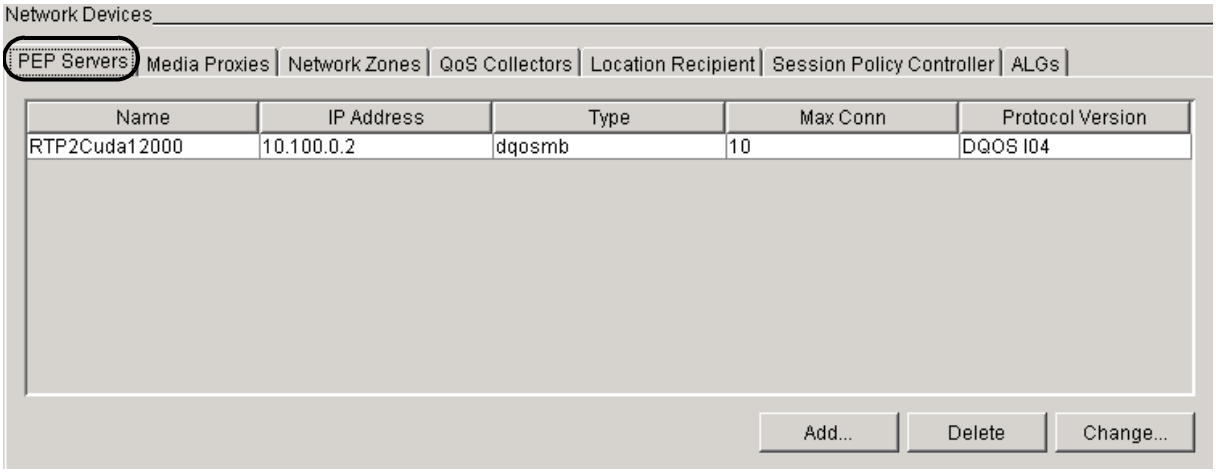
Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



The Network Devices section is available in the middle of the main screen.



2 Click any one of the tabs to display the devices available for that network resource.

Example
To review any PEP servers configured in your system, click the PEP Servers tab.

Note 1: To view NAT, LBL, or composite NAT and LBL zones, click the Network Zones tab, then click the IP-VPN(NAT) Zone, LBL Zone, or NAT&LBL Zone tab.

Note 2: To view the Network VCAC status, click the Session Policy Controller tab. The Network VCAC section is located in the lower right corner of the display.

3 The procedure is complete.

Install a GWC card

Purpose of this procedure

Use this procedure to add a new Gateway Controller (GWC) card in the front slots of the SAM21 chassis.

To replace a GWC card, refer to the procedure “Replace and re-provision a GWC card” in the *Gateway Controller Fault Management* NTP, NN10202-911

When to use this procedure

Use this procedure when you need to add a GWC card to your system.

Prerequisites and guidelines

The following guidelines apply to this procedure:

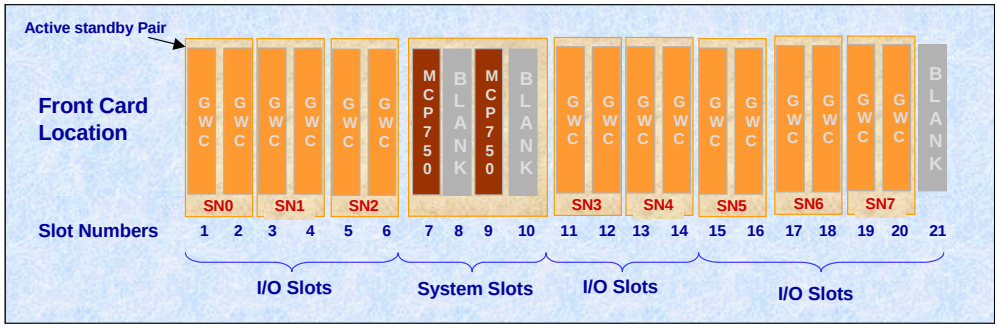
- Do not use this procedure to perform initial installation of GWC cards in a new SAM21 shelf. This activity is performed by Nortel Networks installation personnel.
- GWC cards can be inserted while the power switch for the SAM21 chassis is ON.
- If installing additional GWC nodes, the recommended configuration is for a GWC card for each node to be installed in separate SAM21 or Call Agent shelves.

  Note 1: The two cards that together form a GWC node do not need to be adjacent to each other in the SAM21 shelf. They can occupy any of the slots reserved for GWC cards. A GWC node comprises two cards, but it is not physically a twin-card unit.

  Note 2: To help ensure carrier grade reliability, the cards may be housed in two different SAM21 shelves within the same frame.

- Add the GWC cards to the right of existing GWC cards. Do not install GWC cards in slots 7, 8, 9, 10, and 21.

Possible GWC card locations at the front of the SAM21 shelf



- In the CS 2000 - Compact environment, the CS 2000 Compact Call Agent Shelf is used to house the GWC cards, although GWC card positioning may vary. Refer to the *Call Agent Configuration Management* NTP, NN10109-511, for GWC card positioning details.

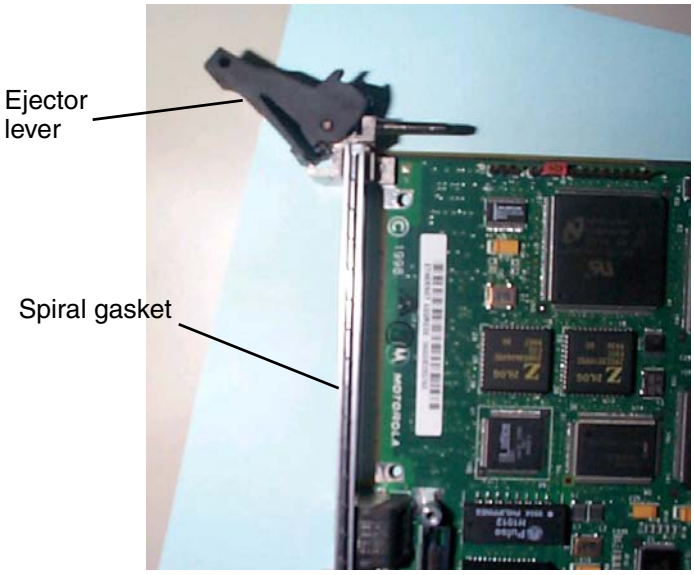
Action

CAUTION
Possible service outage
Use care when inserting and removing cards from the SAM21 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to an electrical short circuit.

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the SAM21 shelf cabinet when handling a GWC card. This protects the card against damage caused by static electricity.

At the front of a SAM21 shelf cabinet

1 Examine the circuit packs prior to inserting them in the SAM21 chassis to ensure that the spiral gasket is seated and not loose.



2 Install the GWC card using the following steps:

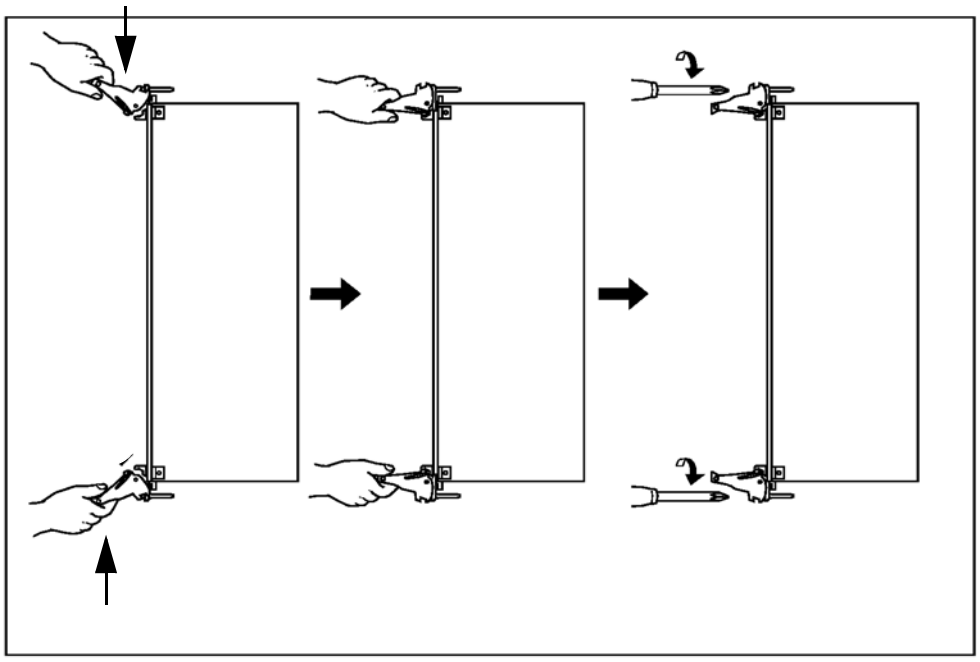
a While holding the ejector levers, press and hold the levers outward.

Note: Do not push on the faceplate of the card. Insert the card by holding the ejector levers.

b Slide the card into the slot until the ejector levers contact the chassis rails.

c Observe that a solid blue light on the card appears. Keep pushing the card into the slot until the blue light turns off.

d Close the ejector levers inward as shown below.



3 If the GWC card does not power up, eject the card, return to step 2 and repeat the steps, or contact your next level of support.

4 Secure the card by tightening the captive screws at the top and bottom of the panel.

5 Repeat this procedure for other GWC cards you wish to install in the SAM21 shelf.

6 The procedure is complete.

Assign service to a GWC card

Purpose of this procedure

Use this procedure to introduce a new Gateway Controller (GWC) node into the SAM21 shelf. GWC cards are added to the SAM21 shelf in pairs. Each pair makes up a single GWC node.

When to use this procedure

Use this procedure after installing new GWC cards into the SAM21 shelf, into a slot that has not previously had a GWC card provisioned.

To replace a previously installed faulty GWC card using the same card provisioning information, refer to procedure “Replace and re-provision a GWC card” in the *Gateway Controller Fault Management* NTP, NN10202-911.

Prerequisites and guidelines

When adding a new GWC card pair for a new node, ensure that a block of four contiguous IP addresses is available for assignment to the card pair. If replacing an existing card, use the same IP addresses assigned to the card being replaced.

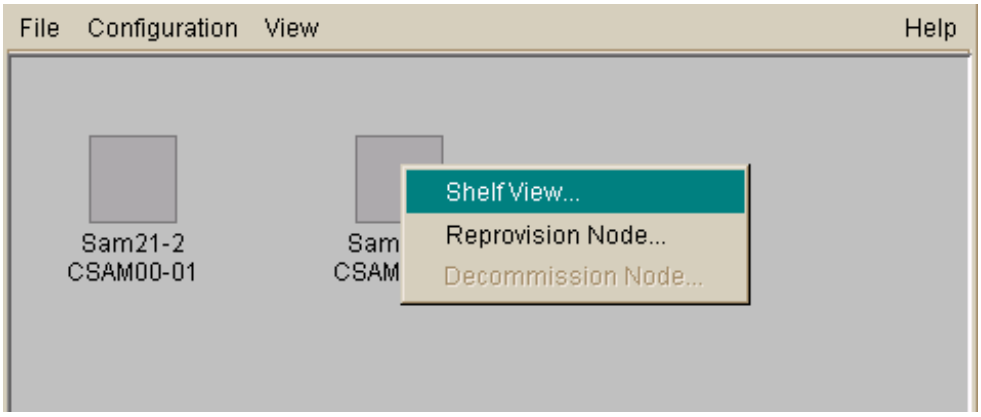
ATTENTION

Each GWC card can be assigned its own unique load image file to boot from on the CS 2000 Core Manager or Core and Billing Manager (CBM).

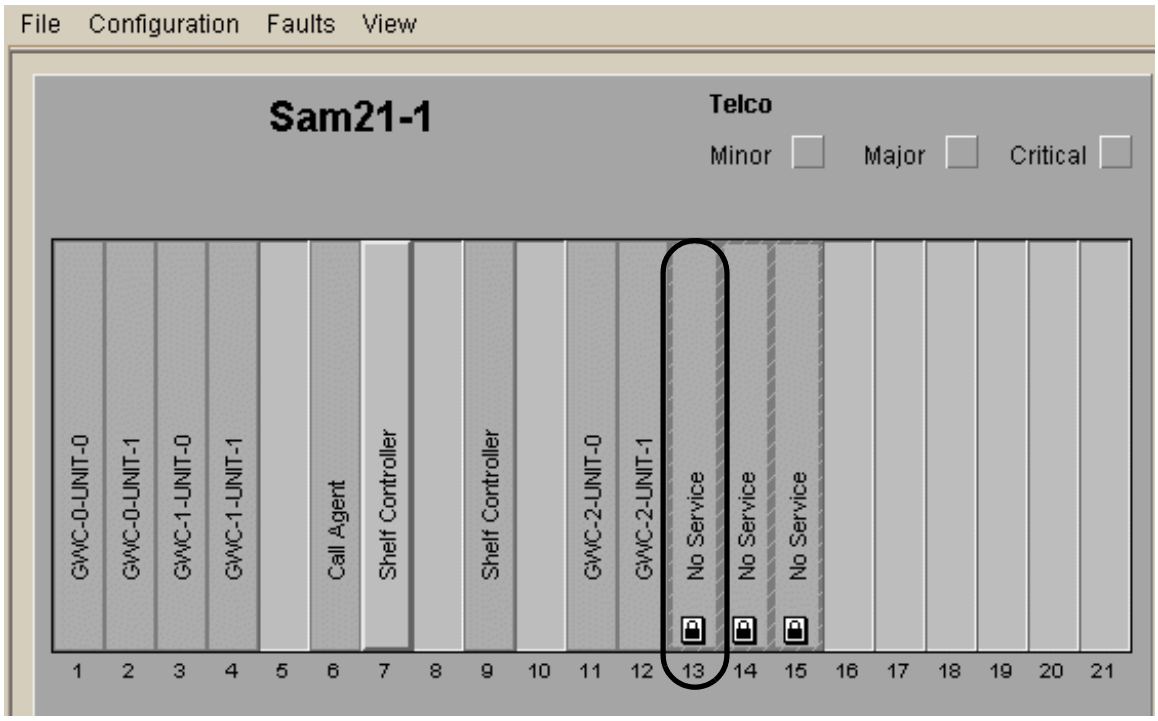
Action

At the CS 2000 SAM21 Manager client

1 Right-click the SAM21 shelf icon containing the Gateway Controller cards you wish to provision, and select **Shelf View** from the pop-up menu.

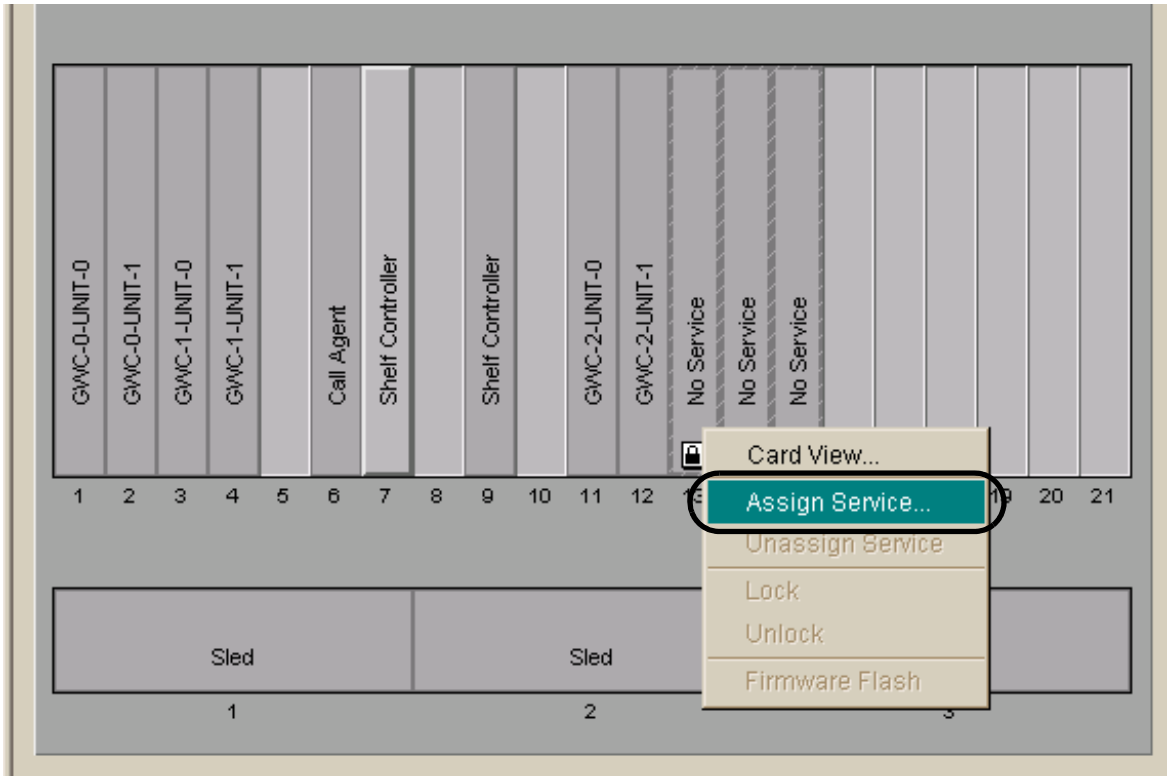


2 Locate the GWC card you wish to provision. Unprovisioned cards are labelled as having No Service, as shown in the following figure.

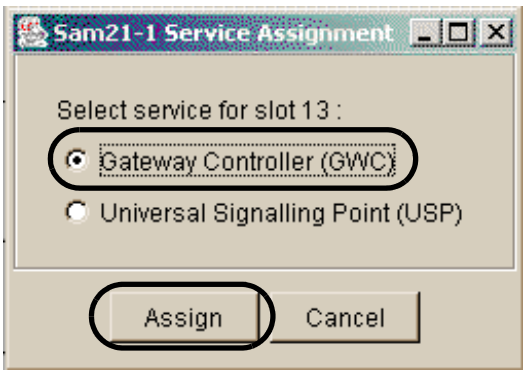


3 If the card is not already locked, refer to the procedure Lock a GWC card on page 519 to lock the card.

4 Right-click the unprovisioned card slot from the Shelf View window and select **Assign Service** from the pop-up menu.



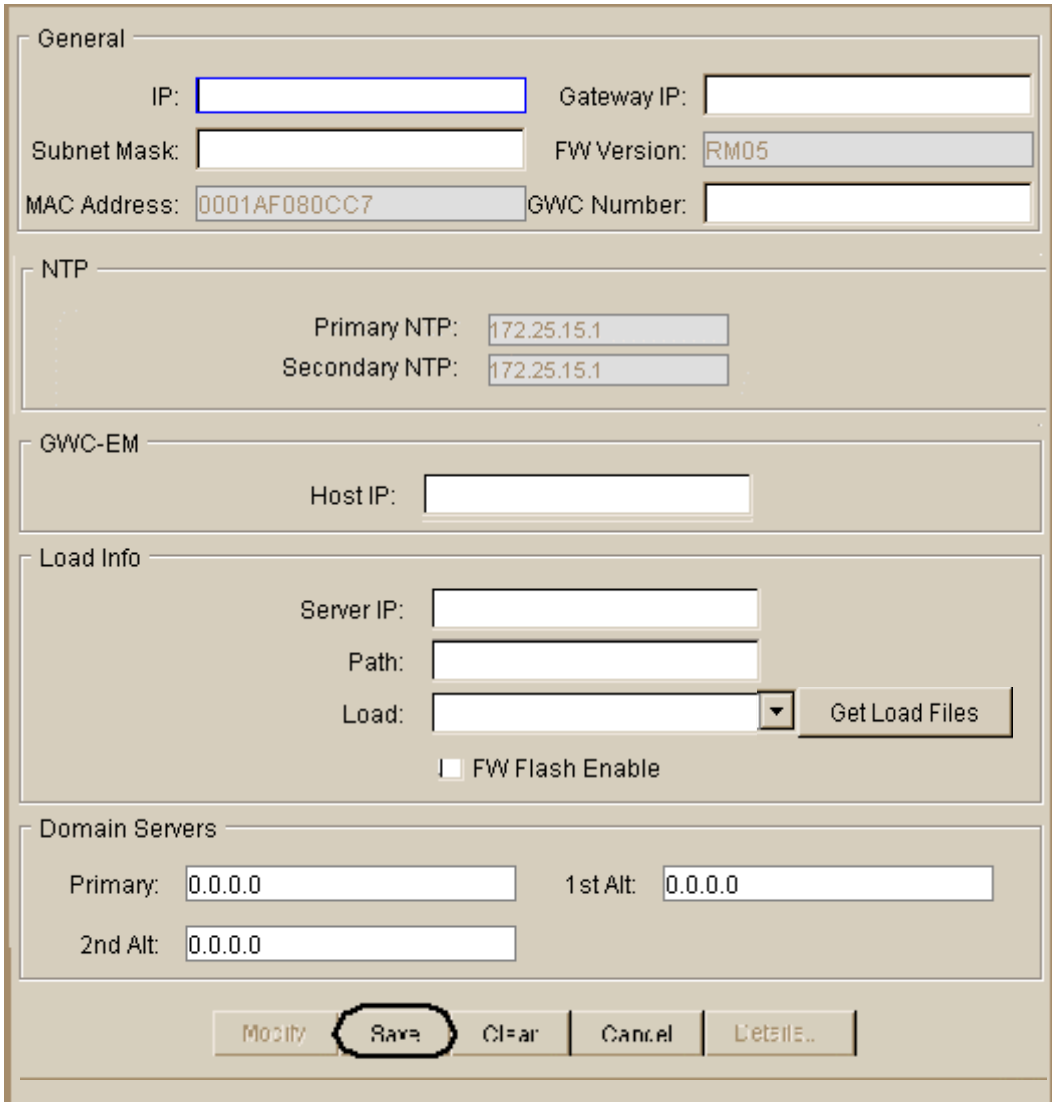
5 From the Service Assignment window, click the Gateway Controller (GWC) radio button, and then click the **Assign** button.



6

ATTENTION
You must configure at least one Domain Server IP address if this GWC will be hosting small line gateways configured for DNS use (gateways provisioned with IP address of 0.0.0.0). Otherwise, the associated lines will not recover after GWC cold switch of activity (SwAct).

Enter the configuration data in the GWC Provisioning window shown below, or use the default values (if applicable).



In most cases, when provisioning a GWC, use the default values indicated; otherwise, obtain and enter the following values:

- IP: <GWC_unit_0_IP_address> or IP:<GWC_unit_1_IP_address>

  Note 1: A contiguous block of four IP addresses is required.

  Note 2: If any of the four IP addresses for the new card is already used by another card, the following message appears. Contact your site system administrator to identify the IP addresses you should be using.

- Gateway IP: default_router or gateway_IP_address
- Subnet Mask: subnet mask
- GWC number: number given the GWC card, from 0 to 255

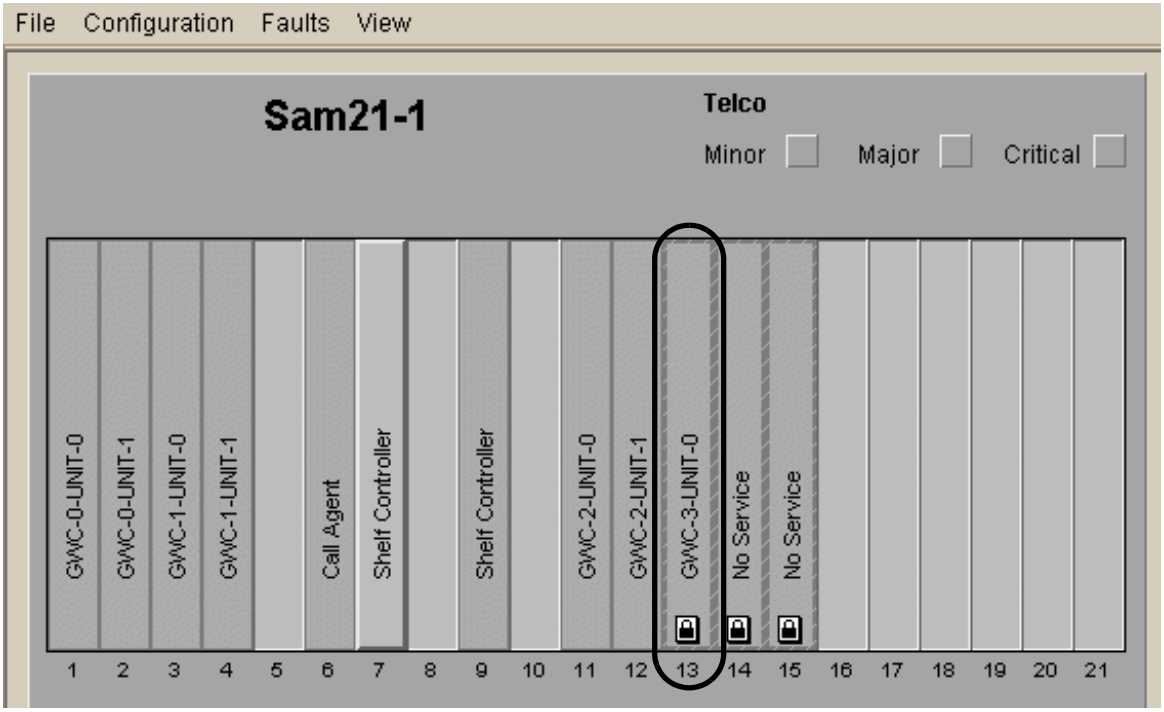
  Note: This field is used to label the GWC in the SAM21 shelf view pane. Refer to the CS 2000 GWC Manager provisioning panel to determine what this value should be by comparing and matching the IP address fields.

- Host IP: CS 2000 Management Tools server IP address
- Server IP: IP address of the CS 2000 Core Manager or Core and Billing Manager (CBM)
- Path: /swd/gwc/ - this is the path where the GWC load image is stored on the CS 2000 Core Manager or CBM disk drives
- Load: the name of the GWC load image file
  example: pgc8xx.imag
  Click the **Get Load Files** button and select the required load from the drop-down list.
- Check the **FW Flash Enable** box if you wish to flash the card firmware with a new firmware version, if available.

- Primary Domain Server: server_IP_address
- 1st Alternate Domain Server: server_IP_address
- 2nd Alternate Domain Server: server_IP_address

7 When you are finished entering data, click the **Save** button.

8 Observe that once the card has been provisioned, the label No Service is replaced by the GWC number and unit number in the shelf view. The same label also appears in the card view.



9 Return to step 2 and repeat the procedure for each GWC card you need to provision.

10 Unlock the card. Reprovisioning does not take effect until the card is unlocked and rebooted. Refer to procedure Unlock a GWC card on page 523 for instructions on unlocking GWC cards using the CS 2000 SAM21 Manager.

11 The procedure is complete.

Remove service from a GWC card

Purpose of this procedure

Use this procedure to remove all configuration information from the selected GWC card.

When to use this procedure

Use this procedure only when you wish to remove the card from service, or when a completely new service must be provisioned on the card.

Prerequisites and guidelines

Before removing the GWC card from service, you must first lock the card. Refer to procedure Lock a GWC card on page 519 in this NTP.

For additional information about GWC card states and diagnostics, refer to procedure “Interpret GWC card states” in the *Gateway Controller Fault Management* NTP, NN10202-911.

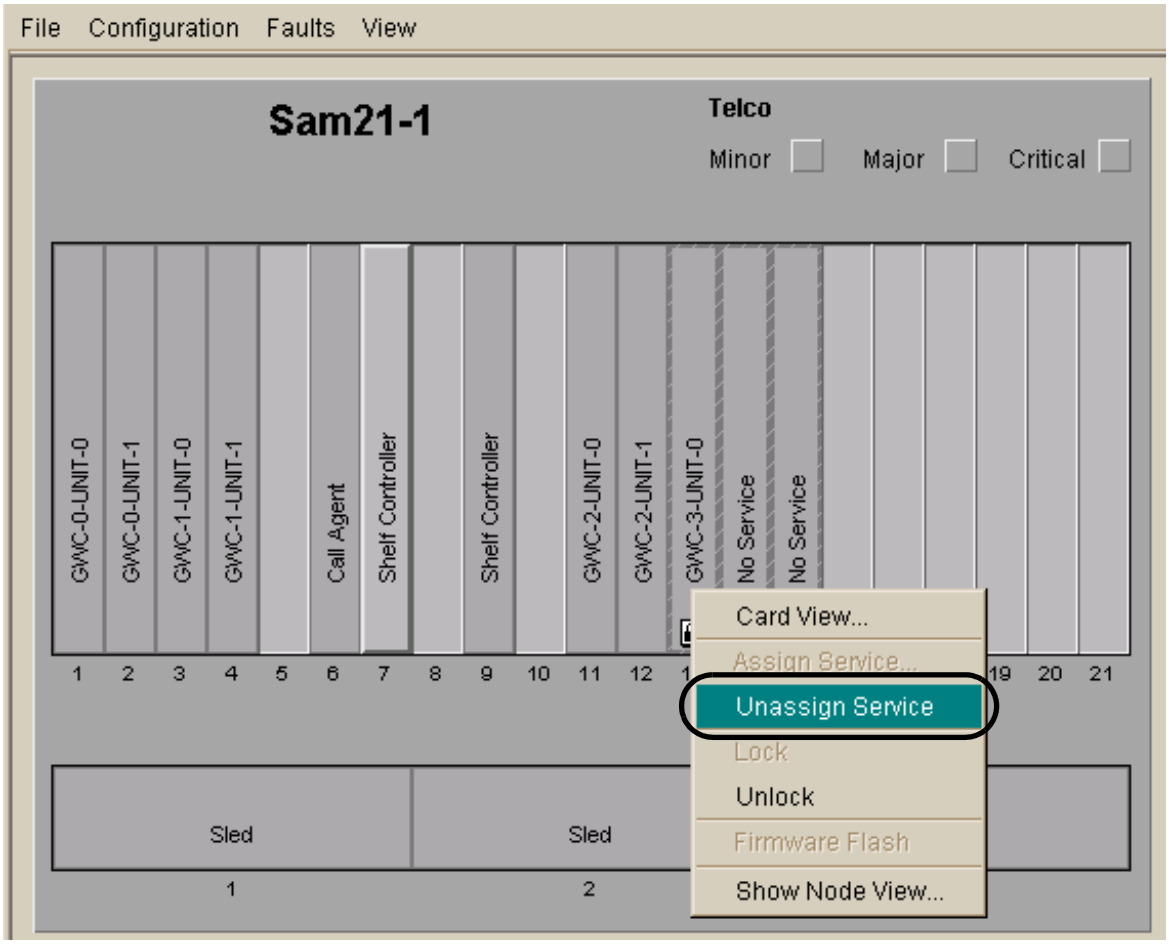
Action

At the CS 2000 SAM21 Manager client

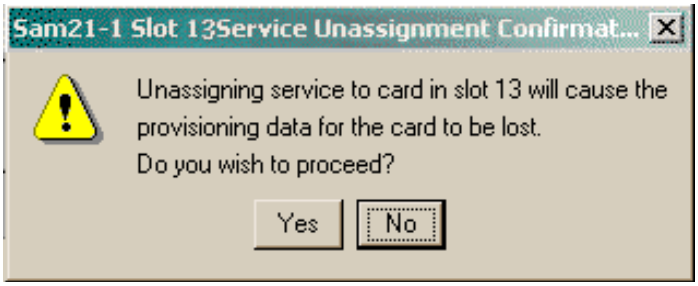
1 Ensure that the GWC card you are removing from service is locked.

Refer to procedure Lock a GWC card on page 519 in this NTP.

2 From the Shelf View window, right-click the GWC card you wish to remove from service and select **Unassign Service** from the pop-up menu.



3 The shelf controller responds with the following warning:



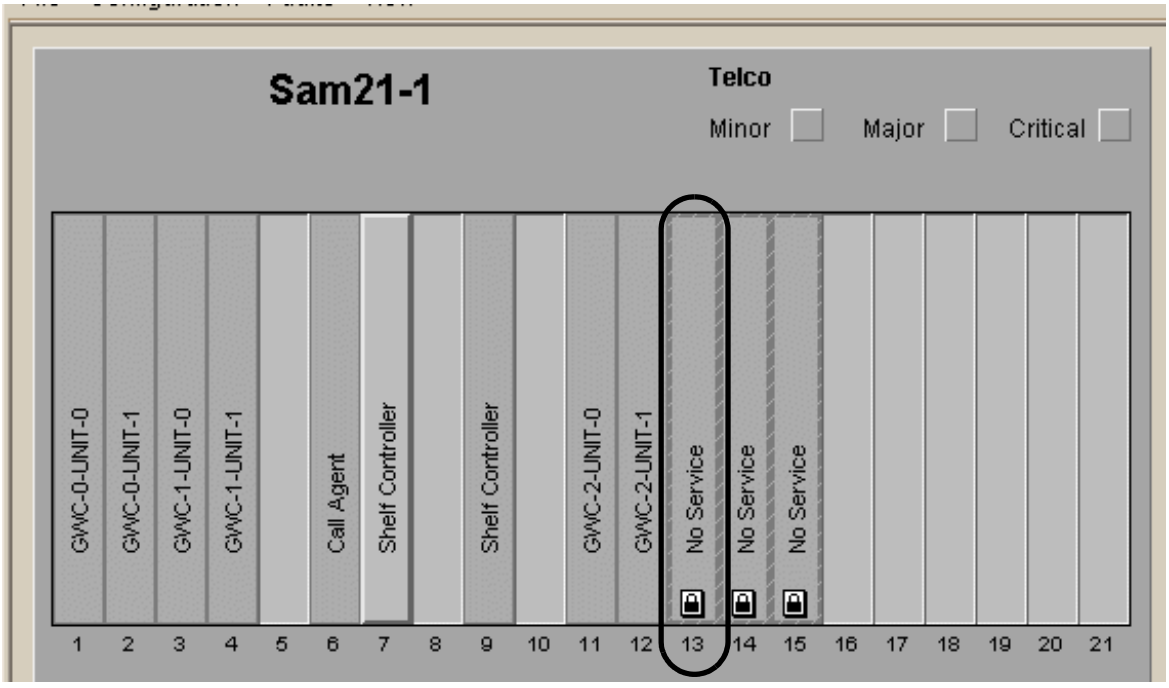
4

CAUTION

Confirming the unassign will remove all provisioning datafill from the selected GWC card. This operation cannot be reversed.

Click **Yes** to confirm that you wish to unassign service from the selected GWC card.

The selected GWC card status changes to *No Service* in the shelf view.



5 The procedure is complete.

Manually re-provision GWC cards

Purpose of this procedure

Use this procedure to manually change the basic provisioning information for a set of Gateway Controller (GWC) cards, including IP addresses, port addresses, gateway addresses, and load paths.

When to use this procedure

Use this procedure when it is necessary to change GWC card-related provisioning information in the CS 2000 SAM21 Manager database.

Prerequisites and guidelines

This procedure does not provide instructions on how to make provisioning changes to GWC services in the CS 2000 GWC Manager database (such as changing a service profile for a GWC node).

You must first busy the GWC node services using the CS 2000 GWC Manager before re-provisioning any cards in the node. Refer to the procedure Busy a GWC node on page 513 to accomplish this task.

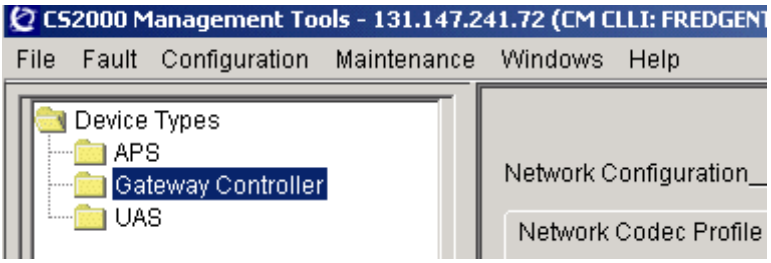
When re-provisioning IP addresses for GWC cards, you must use a block of four contiguous IP addresses for each card pair (node).

CAUTION
Partial service disruption
Changes to the IP addresses or other configuration values of a GWC card can cause inconsistencies with the CS 2000 GWC Manager database.

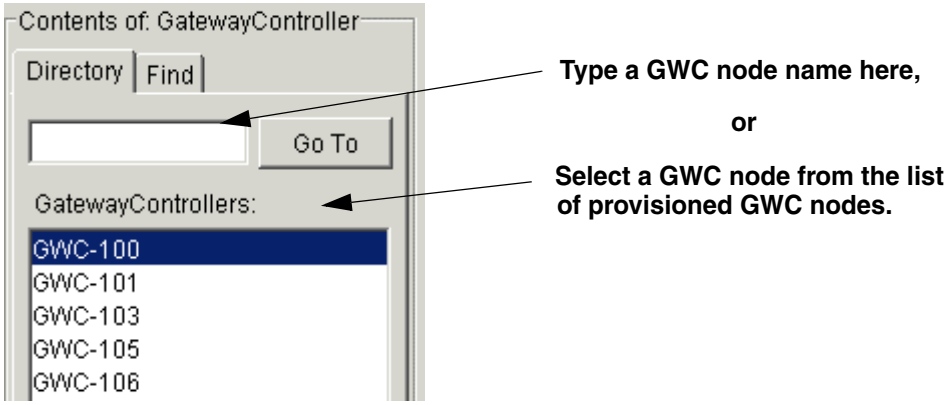
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 Select or type the name of the GWC node to re-provision.

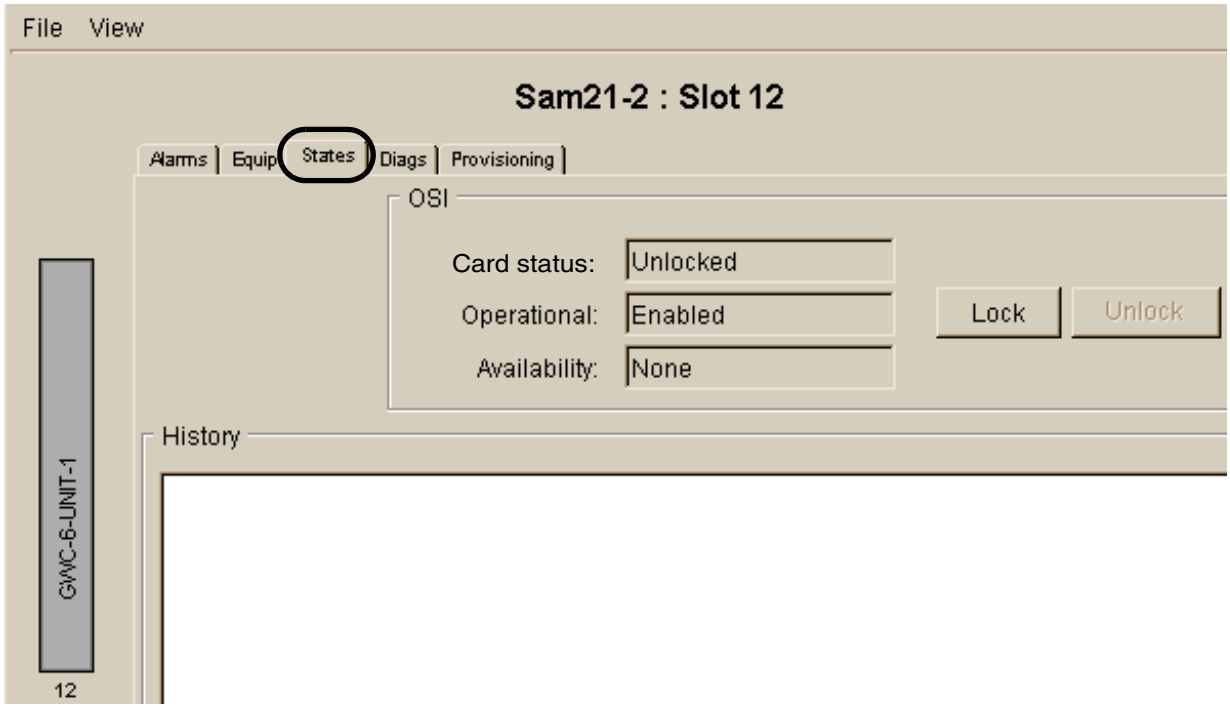


3 Complete the procedure Busy a GWC node on page 513 in this NTP to make the card resources unavailable for call processing activities.

4 Click the **Card View** button for the card you busied in step 3. This action opens the CS 2000 SAM21 Manager.

At the CS 2000 SAM21 Manager

5 Select the **States** tab to view the states window.

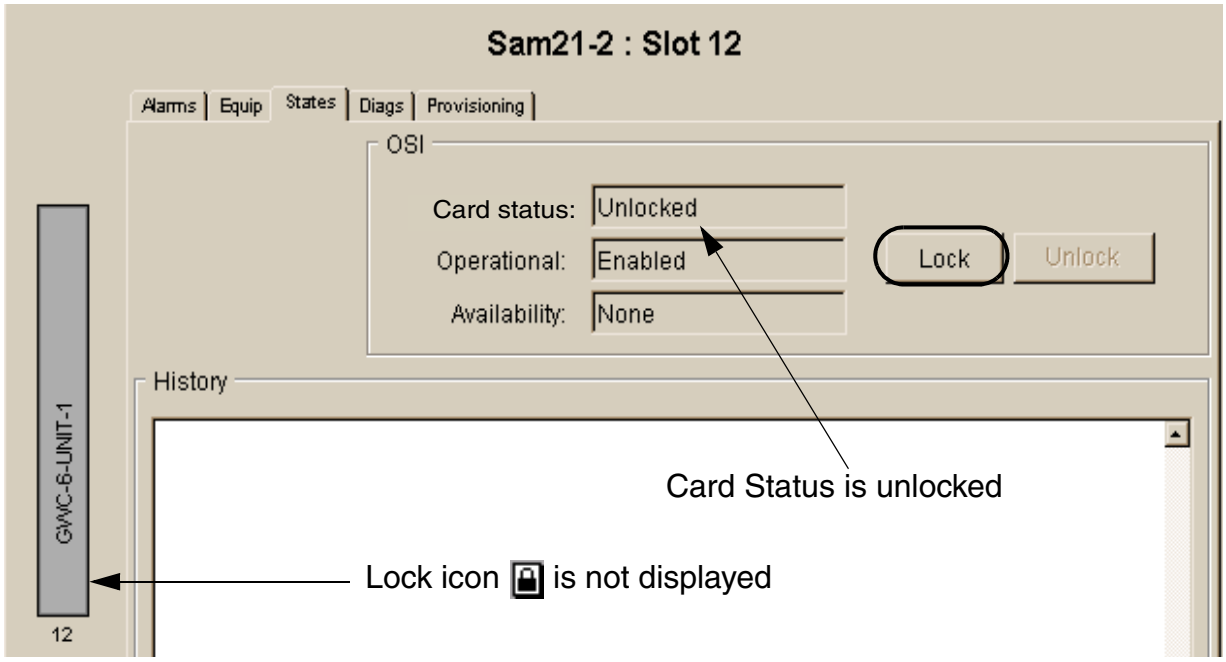


6 Click the **Lock** button to lock the card. For details on locking a card, refer to procedure Lock a GWC card on page 519 in this NTP.

Note: If the card is already locked, go to step 7.

Determine if the card is locked by looking at the card graphic at the left of the screen. If the lock icon

is present, the card is locked. If the lock icon is not present, the card is not locked. The Card Status also indicates whether the card is locked.



The system responds:

```
Application locked Successfully.
```

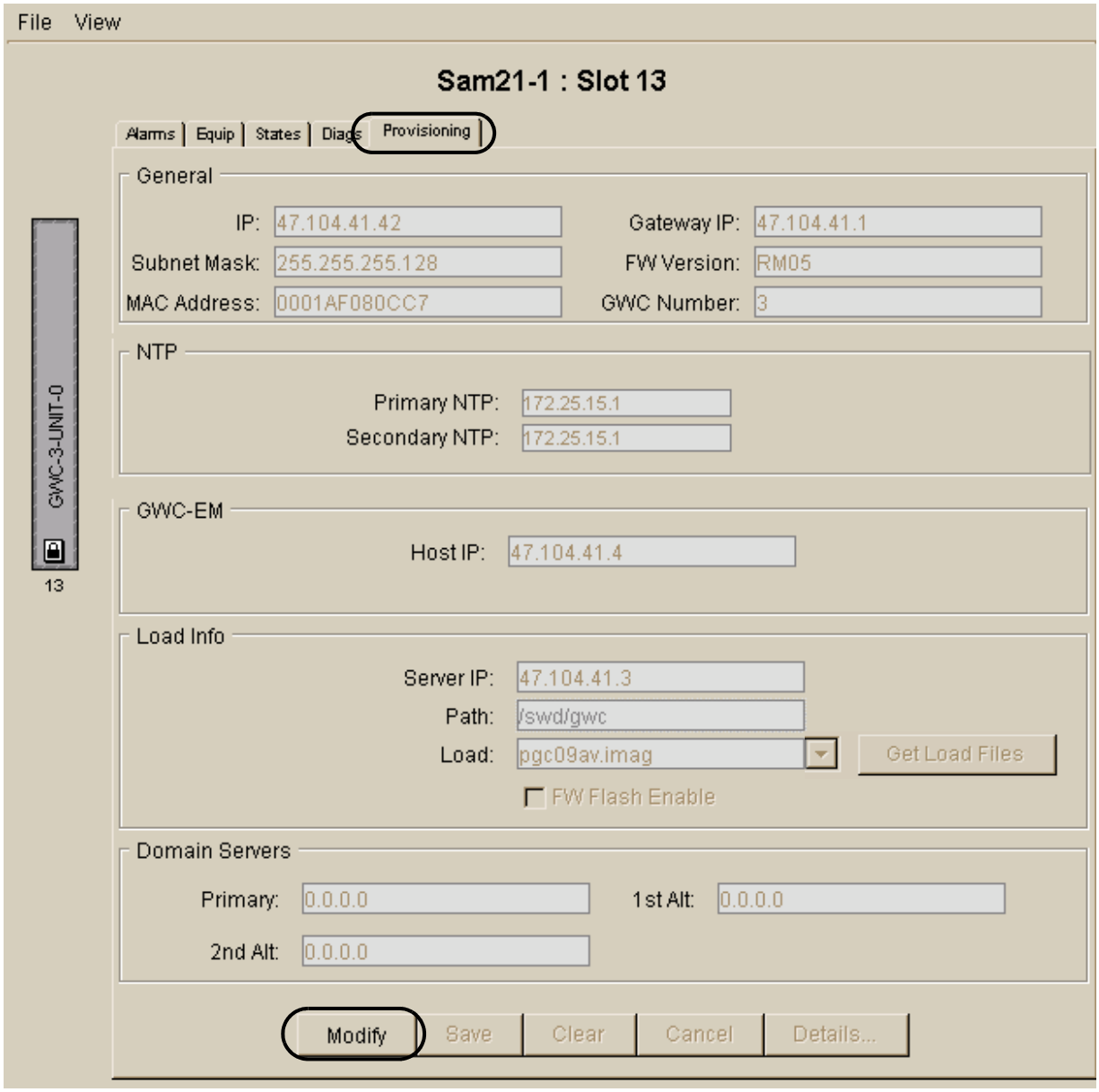
Note: If you are denied your first attempt to lock the card, you can override the lock request denial and force the card to lock. Refer to the procedure View and interpret the operational status of a GWC node on page 533 in this NTP to use the CS 2000 GWC Manager to interpret the various states of the card.

A card has accepted a lock request if it has the following states:

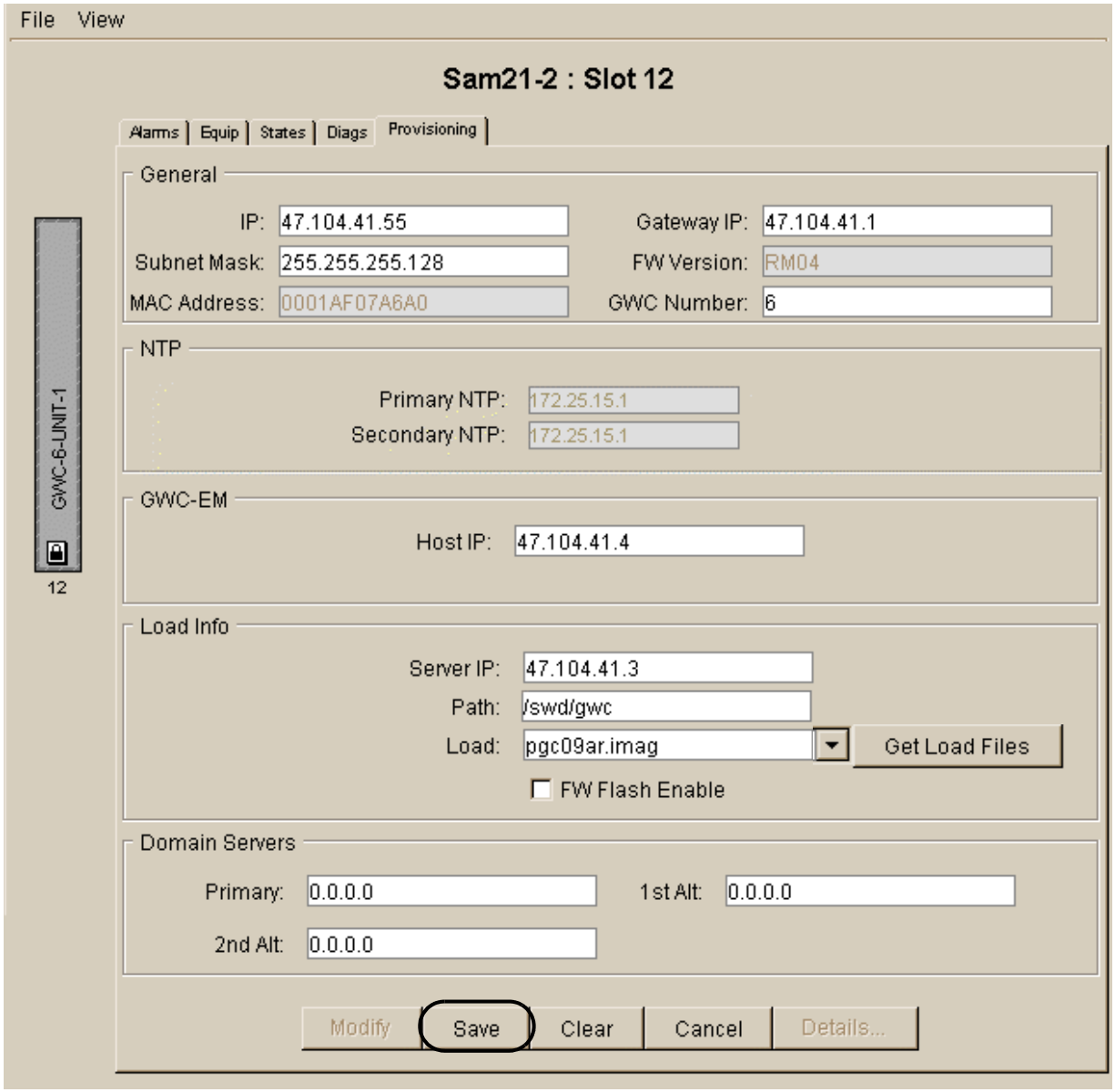
- Card Status: locked
- Operational state: disabled

7 Select the **Provisioning** tab.

8 Click the **Modify** button to make changes to the provisioning datafill.



9 Enter the new or changed provisioning data as described below.



In most cases, when pre-provisioning a GWC, use the default values indicated. Otherwise, obtain and enter the following values:

- IP: <GWC_unit_0_IP_address> or

  IP: <GWC_unit_1_IP_address>

  Note 1: A contiguous block of four IP addresses is required.

Note 2: If any of the four IP addresses for the new card is already used by another card, the following message appears. Contact your site system administrator to identify the IP addresses you must use.

- Gateway IP: default_router or gateway_IP_address
- Subnet Mask: subnet_mask
- FW Version: firmware version of the GWC load
- Host IP: CS 2000 Management Tools_Server_IP_Address
- Server IP: IP address of the CS 2000 Core Manager or Core and Billing Manager (CBM)
- Path: /swd/gwc/ - on the CS 2000 Core Manager or CBM
- Load: name of the GWC load image file;
  example: pgc08bg.imag
  Click the **Get Load Files** button and select the required load from the drop-down list.
- If available, select the **FW Flash Enable** check box if you wish to flash the card firmware with a new firmware version
- Primary Domain Server: server_IP_address
- 1st Alternate Domain Server: server_IP_address
- 2nd Alternate Domain Server: server_IP_address

10 When you are finished entering changes, click the **Save** button.

11 Return to step 2 and repeat the steps for each GWC node you are re-provisioning.

12 Re-provisioning does not take effect until the card is unlocked and rebooted. Refer to procedure Unlock a GWC card on page 523 in this NTP for instructions on how to unlock GWC cards.

13 The procedure is complete.

Add and configure a GWC node

Purpose of this procedure

Use this procedure to configure Gateway Controller (GWC) call processing services on a selected GWC node.

When to use this procedure

Use this procedure when configuring a GWC node for a specific Gateway Controller service profile.

Prerequisites and guidelines

Prerequisites

Determine the IP address of the active GWC card. Use the following steps:

1. At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2. From the Contents of: Gateway Controller frame, select the GWC node on which you are provisioning call processing services.
3. Click the **Maintenance** tab at the CS 2000 GWC Manager.
4. Determine the IP address of GWC unit 0 displayed at the top of the screen.
5. Subtract 2 from the last octet of the unit 0 IP address.

   For example, if the IP address of unit 0 is 216.25.2.42, the active IP address would be 216.25.2.40.

If you wish to add a GWC node and configure the node with a codec profile using a bearer network type that is new to your CS 2000, you must first modify table BEARNETS on the XA-Core. In the BEARNETS table, you must create a network instance of the new bearer network type before you can add a GWC node and configure the node to use the new codec profile.

To modify table BEARNETS on the XA-Core, refer to procedure “Specifying the bearer networks served by the CS 2000" in the CS 2000 Configuration Management NTP applicable to your solution.

General guidelines

To commission a GWC with an audio, SIP-T, or VRDN service profile, additional datafill on the XA-Core is required after provisioning of the GWC is completed using the CS 2000 GWC Manager.

If you are adding an audio controller with redirecting media gateway controller (RMGC) service profile, you must also complete procedure Add or change the RMGC default domain on page 63. Perform this procedure to ensure that a valid RMGC GWC default domain name is entered in the GWC Manager database for the CS 2000. This service profile would be either AUDCNTL_RMGC or AUDCNTL_RMGCINTL. This service profile combines the audio controller and RMGC capabilities. These capabilities are not inter-related. You may use a GWC node with this profile to perform the RMGC function, as well as an audio controller function.

Note: If you wish to change a GWC node from one service profile to another, you must remove the old GWC from the CS 2000 GWC Manager database and re-add it. It must then be unlocked to allow it to reboot.

Example

To change a trunk or line GWC to a SIP-T GWC, you must lock both GWC cards on the node, delete the trunk or line GWC from the CS 2000 GWC Manager database, and then re-add it as a SIP-T GWC. For more details about the procedures needed to perform this activity, along with the order in which to perform the applicable procedures, refer to the general procedure Modify the operating configuration of an installed GWC node on page 9.

Network codec profile guidelines

No matter which network bearer types (IP, AAL1 or AAL2) are configured for a CS 2000 using procedure Add a network codec profile on page 19, only one bearer network instance can be selected for any GWC node. You must modify table BEARNETS on the XA-Core to configure a network instance of a bearer network type.

You can change the network codec profile assigned to a GWC node, provided the profile supports the network bearer type already selected for the node.

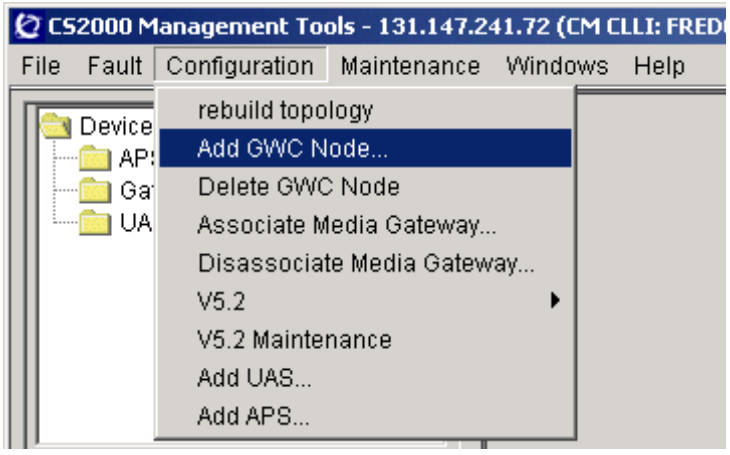
You cannot change the bearer network type assigned to a GWC node. You can change the specific network codec profile supported, but any new profile must use the same bearer network type as the codec you were using. If you wish to change the bearer network type assigned to a GWC node, refer to the general procedure Re-configure a GWC node in the network on page 10.

Action

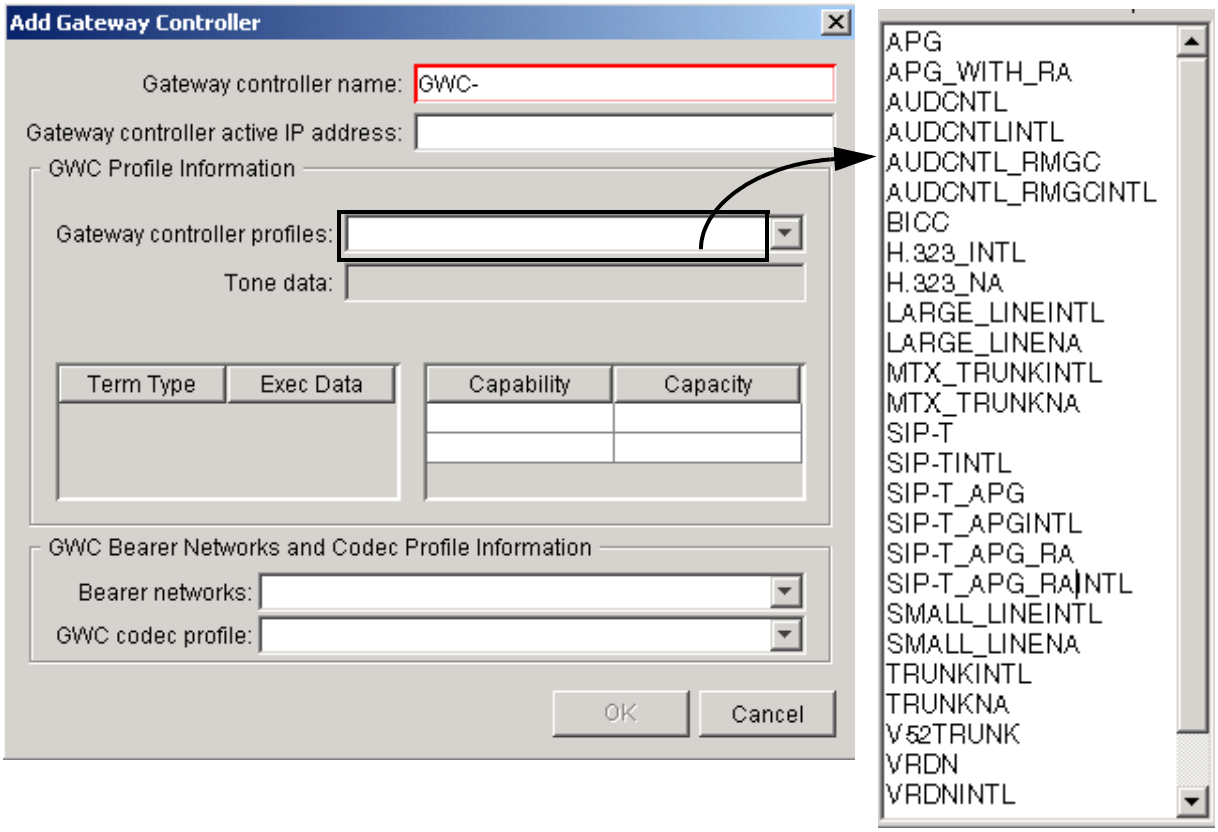
At the CS 2000 GWC Manager client

1 Lock the GWC cards using the procedure Lock a GWC card on page 519.

2 At the CS 2000 Management Tools main menu, click on the **Configuration** menu from the top menu bar and select **Add GWC Node...** to display the Add Gateway Controller dialog box.



3 At the Add Gateway Controller dialog box, enter or select the applicable node configuration information. Refer to table Add Gateway Controller configuration fields on page 127 for the description of each configuration field.



Note: Starting in SN08, you do not have to manually configure the message router IP address for each GWC. Instead, the Core IP address is automatically provisioned for all GWCs, and displayed under General Network Settings on the GWC network display panel.

The following table describes each configuration field of the Add Gateway Controller dialog box.

Add Gateway Controller configuration fields (Sheet 1 of 6)

Field	Description
Gateway controller name:	The node name of the GWC card in the format of: GWC-<n>; where n is a number from 0 to 255.
Gateway controller active IP address:	The IP address for the active GWC card.
Gateway controller profiles:	Select only one service profile. ***Note 1:*** Gateway Controller service profiles appended with *INTL* are international market place installations, while service profiles appended with *NA* are for North American market place installations. ***Note 2:*** Only one service profile (for example, line, trunk, or audio) is supported for each GWC node. ***Note 3:*** If you attempt to associate a media gateway of one service profile to a GWC of another service profile, the addition of the media gateway will be rejected. Select one of the following service profiles: ***Note:*** The APG functionality has been removed in the SN07 release. All GWC service profiles that were required to support the APG functionality (all profiles with "APG" in their names) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. The Packet Media Anchor device (supported by the audio controller GWCs) replaces the APG functionality in the IP network solutions. The RA server is now located and enabled by default on the audio controller GWC.
	APG - obsolete in the SN07 release. Do not use this service profile.
	APG_WITH_RA - obsolete in the SN07 release. Do not use this service profile.
	AUDCNTL or **AUDCNTLINTL** - to add an audio server gateway for your applicable market. Use these profiles to add the Packet Media Anchor functionality supplied by the Media Server 2010 gateways (IP market solutions).

Add Gateway Controller configuration fields (Sheet 2 of 6)

Field	Description
	AUDCNTL_RMGC or **AUDCNTL_RMGCINTL** - to add an audio controller with a redirecting media gateway controller (RMGC). This option combines the audio controller and RMGC capabilities in one profile. These capabilities are not inter-related. You may use a Gateway Controller with this profile to perform the RMGC function, as well as an audio controller function. An RMGC enables initializing gateways to obtain the IP address of their GWC from a registration agent in the network. This profile is applicable only to cable and wireline solutions for either NA or International markets. ***Note 1:*** RMGC capacity is limited to 115,000 gateways. ***Note 2:*** After adding either audio controller RMGC GWC services profile, complete the procedure Add or change the RMGC default domain on page 63 to ensure that a valid default domain name is datafilled in the GWC Manager database.
	BICC - to add a GWC that will host inter-office DPT trunk calls using Bearer Independent Call Control (BICC) on an ATM network for the bearer path. ***Note:*** If DPTs on a BICC GWC are used, then MG4000s are a required component in the solution.
	H.323_NA or **H.323_INTL -** to add an H.323 GWC for your applicable market. H.323 gateways provides VPN and PSTN connectivity for multiple enterprises and sites.
	LARGE_LINENA or **LARGE_LINEINTL -** to add a large line media gateway for your applicable market.
	MTX_TRUNKNA or **MTX_TRUNKINTL -** to add a GWC that supports the packet serving mobile switching center (MSC) solution for mobile telephone exchange (MTX). ***Note:*** In order to use either MTX profile, the CS 2000 XA-Core must be upgraded to the SN07 (or higher) MTX software load. ***Attention:*** For software release SN07 (P-MSC MTX13) in the international (INTL) market, do not use the MTX_TRUNKINTL profile when configuring MTX trunks. Instead, you must use the MTX_TRUNKNA profile. For more information on configuring MTX trunks, refer to the *MSC Server 1000 Configuration Management*, NN-20000-223.

Add Gateway Controller configuration fields (Sheet 3 of 6)

Field	Description
	SIP-T or **SIP-TINTL -** to add SIP-T based trunk services for your applicable market.
	SIP-T_APG or **SIP-T_APGINTL -** obsolete in the SN07 release. Do not use this profile.
	SIP-T_APG_RA or **SIP-T_APG_RAINTL** - obsolete in the SN07 release. Do not use this profile. **SMALL_LINENA** or **SMALL_LINEINTL -** to add a small line media gateway for your applicable market.
	TRUNKNA or **TRUNKINTL** - to add a local exchange carrier (LEC) trunk media gateway for your applicable market.
	V52TRUNK - to add a GWC that will host V5-based line services. (This service profile is used in international markets only.) ***Note:*** A PVG can be configured as a V5.2 gateway rather than a trunk gateway. A PVG V5.2 gateway supports V5.2 interfaces connected to V5.2 Access Networks (AN) serving V5.2 PSTN lines, such as analog subscriber lines.
	VRDN or **VRDNINTL** - to add a virtual router GWC for your applicable market. ***Note:*** Unless otherwise specified, use the default values indicated for Tone Data, Term Type, and Exec Data.

Add Gateway Controller configuration fields (Sheet 4 of 6)

Field	Description
Tone data:	Auto-datafilled when the appropriate profile is selected.
Term Type:	Auto-datafilled when the appropriate profile is selected.
Exec Data:	Auto-datafilled when the appropriate profile is selected.
Capability:	Auto-datafilled when the appropriate profile is selected.
Capacity:	Auto-datafilled when the appropriate profile is selected.

Note: Depending on the Gateway Controller profile selected, different options may be available in the Exec Data field for each Term Type. Click on the drop-down menu to view the options for each entry.

Attention - TGCP:

GWC nodes can operate with the gateway profile name TGCP (Trunk Gateway Control Protocol), assigned when performing procedure Associate a trunk media gateway on page 135. A GWC node that using TGCP that supports Per Trunk Signaling (PTS) endpoints requires the following settings:

- Term Type: set to “ABTRK”
- Exec_Data: set to “GWCEX”

Without these settings, maintenance and call processing will not work on the GWC.

Attention - TRUNKNA:

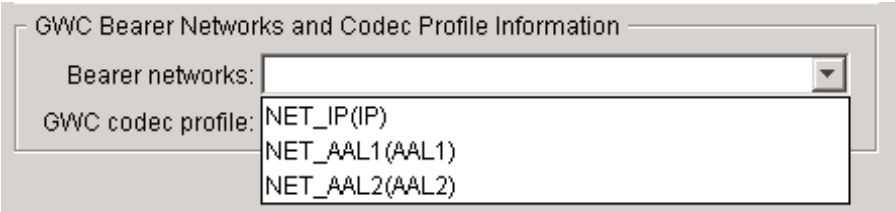
If you selected service profile TRUNKNA, the following configuration options exist for field Exec Data:

- for Term Type PRAB: DTCEX (default) or UTR250
- for Term Type ABTRK: GWCEX (default)
- for Term Type AB250: GWC250 (default) or GWCFX

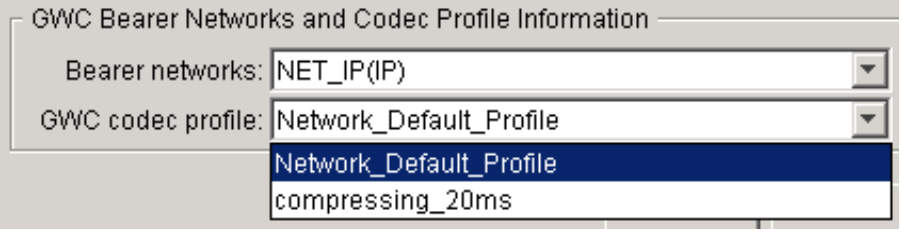
Use the following guidelines to configure field Exec Data:

- For DMS-100/200/250 *ISUP* trunks, use the default values.
- For DMS-100/200 *PRI* trunks, use the PRAB - DTCEX (default) setting.
- For DMS-250 *PRI* trunks, use the PRAB - UTR250 setting.
- For DMS-100/200/250 *PTS* (AB) trunks, use the default settings.
- For FX *PTS* (AB) trunks, use AB250 - GWCFX setting.

Add Gateway Controller configuration fields (Sheet 5 of 6)

Field	Description
Bearer networks:	Select the bearer network for this GWC node using the drop-down menu. Network codec profiles using different bearer network types are defined using procedure Add a network codec profile on page 19. Bearer network types must also be defined in the XA-Core table BEARNETS.  ***Note 1:*** You can select only one bearer network type for a GWC node. ***Note 2:*** You cannot change the bearer network type assigned to a GWC node. You can change the specific network codec profile supported, but any new profile must use the same bearer network type as the codec you were using. If you wish to change the bearer network type assigned to a GWC node, refer to the general procedure Re-configure a GWC node in the network on page 10. ***Note 3:*** If the GWC node will be hosting lines using NCS protocol, you must select a network codec profile with RFC 2833 disabled (RFC2833 check box de-selected).

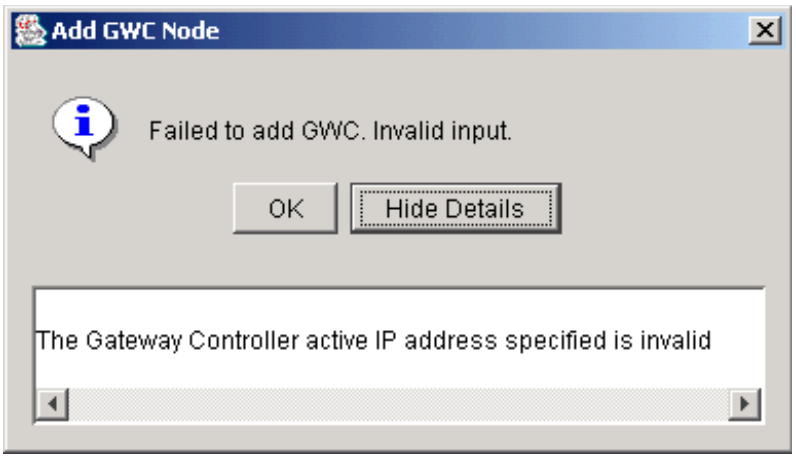
Add Gateway Controller configuration fields (Sheet 6 of 6)

Field	Description
GWC codec profile:	Select a codec profile for this GWC node using the drop-down menu. The profiles available are based on the bearer network selected in the previous field. Network codec profiles for each bearer network type are configured using procedure Add a network codec profile on page 19. The default codec is the first one listed for a bearer network type. The default codec is defined when adding or changing a profile using procedure Add a network codec profile on page 19.  ***Note 1:*** The default codec for the bearer network type is automatically selected if this step is skipped. ***Note 2:*** You can change the specific network codec profile supported, but any new profile must use the same bearer network type as the codec you were using. ***Note 3:*** If the GWC node will be hosting Media Server 2010 gateway configured with the Packet Media Anchor functionality, you must select a network codec profile that supports only G.711 a-Law or G.711-u Law codec. If not available, add a new profile using procedure Add a network codec profile on page 19.

4 After you have completed all required fields, click **OK**.

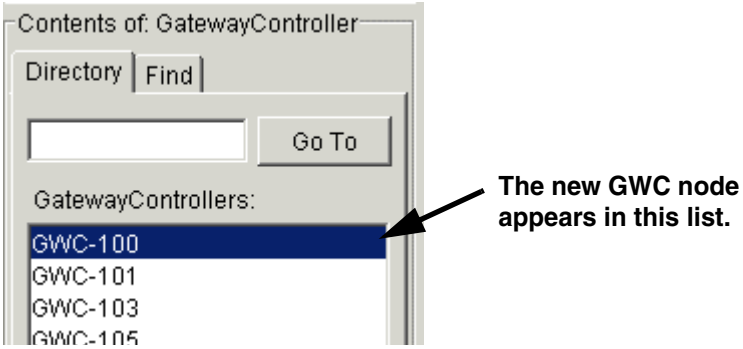
A “Processing...” window will be displayed for up to several minutes while the new GWC type is added to the system. A response dialog will be displayed when the operation is completed. If any error occurred during the transaction, click the **Show Details** button to show where the transaction failed. Refer to the CS 2000 Management Tools server logs for more details about the failure.

Note: If the active IP address for the new card is already used by another card, the following message appears. Contact your site network administrator to identify the IP address you must use.



When the new GWC node has been successfully added, its name will be displayed in the Contents of Gateway Controller view.

5 Observe that the new GWC node appears in the Contents of: Gateway Controller panel.



To verify that the Add GWC operation succeeded, click the GWC node you just added from the Contents of: Gateway Controller

panel and review the data displayed in the Provisioning and Maintenance panels.

6 Return to step 2 and repeat the procedure for each GWC node you are configuring.

7 Provisioning does not take effect until the card is unlocked and rebooted. Refer to procedure Unlock a GWC card on page 523 for instructions on how to unlock GWC cards.

8 The procedure is complete.

Associate a trunk media gateway

Purpose of this procedure

Use this procedure to associate a trunk media gateway with a Gateway Controller (GWC) node.

A gateway profile is a definition in the CS 2000 Management Tools database (CS 2000 GWC Manager database) that captures some of the characteristics and capabilities of a gateway device. A profile is chosen when the gateway is being associated to the GWC node. The information in the profile is then used to determine compatibility of the GWC node with which the gateway is being associated and to assess whether the node has the available endpoint capacity.

Note: Starting in SN08, you can change some gateway attributes defined by a profile (such as, the maximum endpoint capacity) by changing the profile for the selected gateway. For more information, refer to procedure Change gateway attributes on page 277.

When to use this procedure

Use this procedure when you wish to associate a trunk media gateway with a GWC node.

Prerequisites and guidelines

ATTENTION

The APG functionality has been removed in the SN07 release. The Packet Media Anchor is the replacement device. All GWC and gateway service profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, PVG_APG_ASPEN) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles.

The following guidelines apply when adding trunk media gateways:

- When you assign a media gateway name, the name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist, even if the media gateways are associated with different GWC nodes. Duplicate names will be rejected by the CS 2000 GWC Manager database.
- If you attempt to associate a large media gateway with a GWC that does not have adequate available capacity, the request will be rejected. While using this procedure to associate a large trunk

gateway to a GWC node, you can adjust the port capacity of the individual media gateway to fit within the available port capacity of the GWC node by changing the default value in the Reserved Terminations: field.

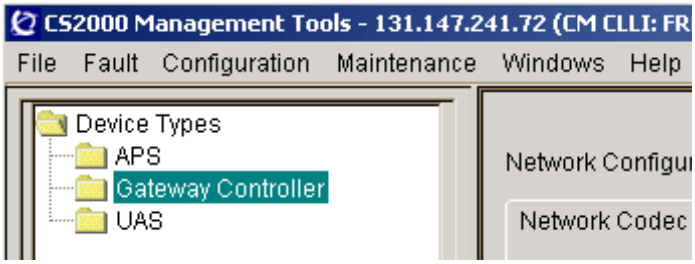
- If you attempt to associate a media gateway with a GWC that has a different service type, the request will be rejected. For example, you cannot associate a line media gateway with a trunk GWC node.
- You may associate up to 24 media gateways with 1 trunk GWC.

Note: If you wish to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC, click the **Statistics** button under the **Controller** tab of the **Provisioning** panel. If required, refer to procedure View characteristics of a GWC node on page 239.

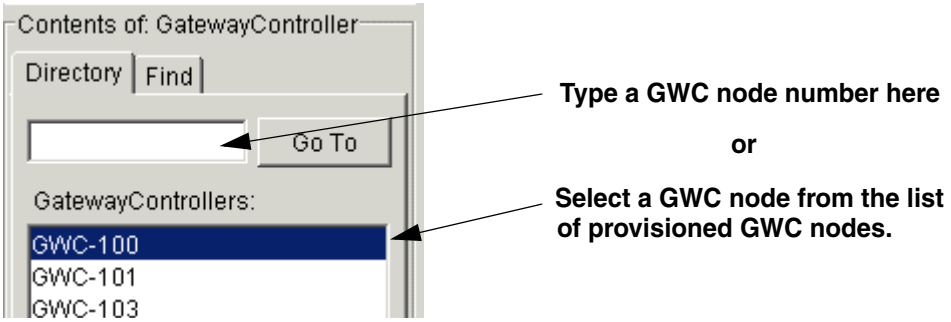
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

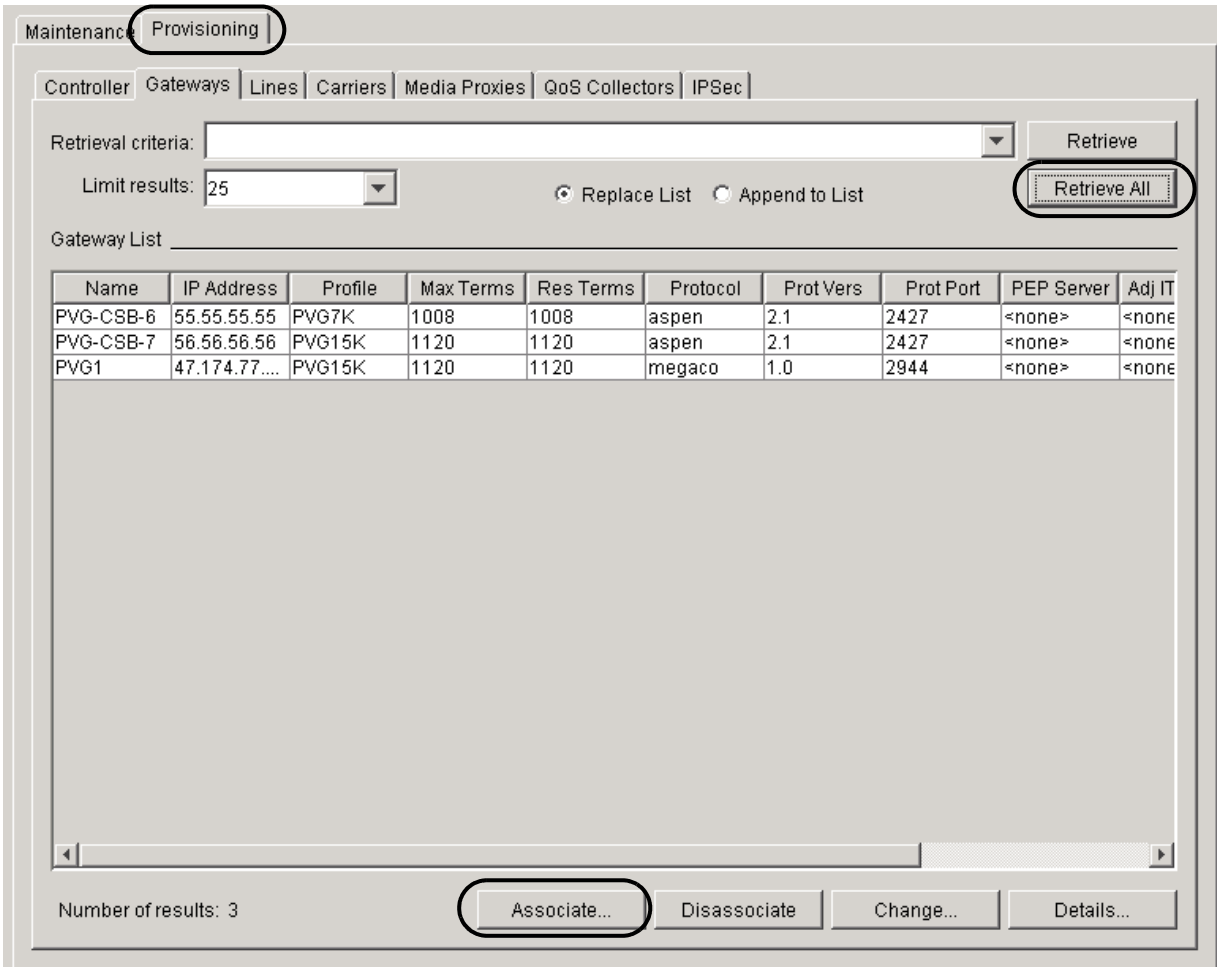


2 From the Contents of: Gateway Controller frame, select the GWC node to which you wish to associate a media gateway.



3 Click the **Provisioning** tab.

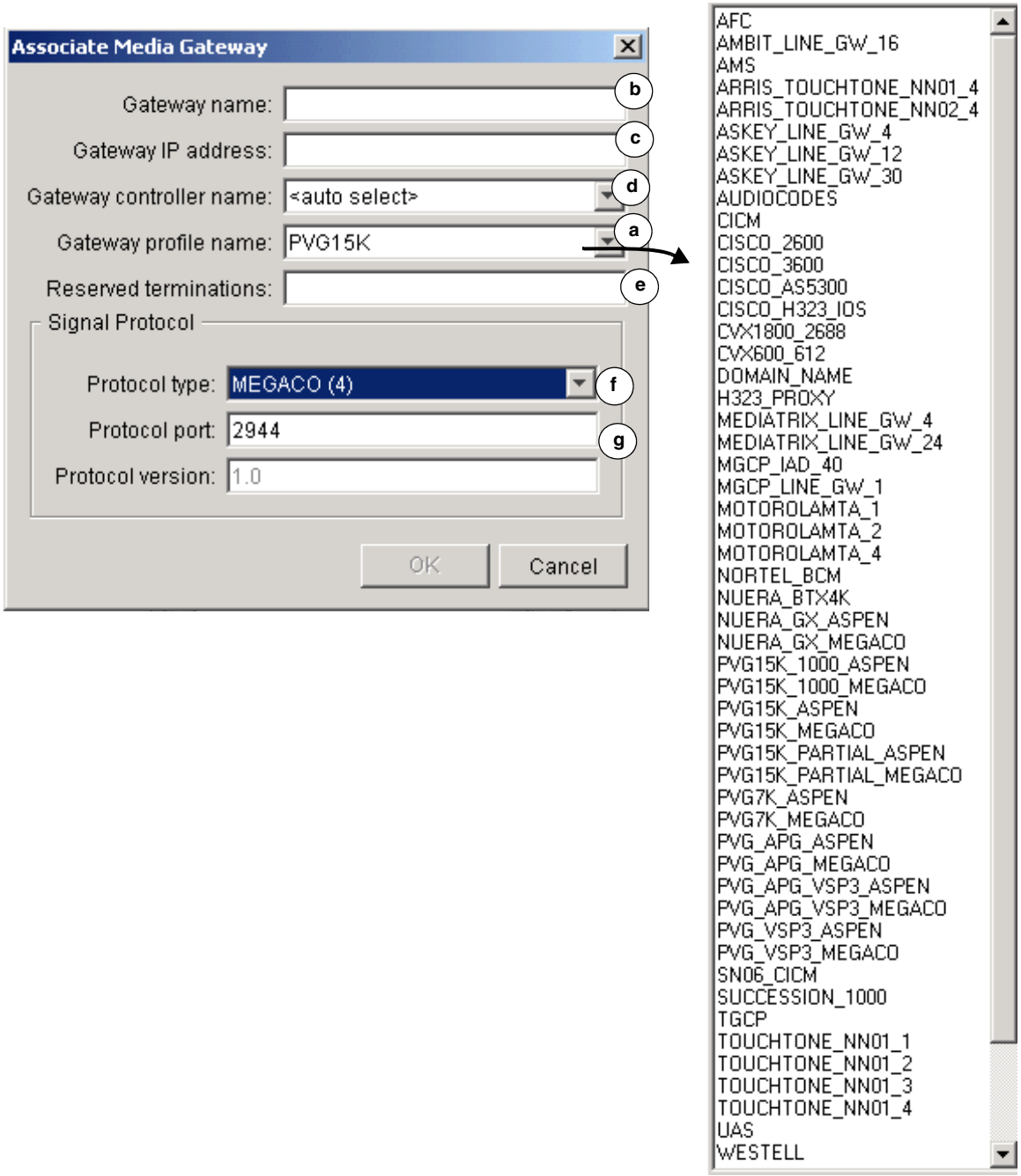
4 Click the **Gateways** tab, then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list will contain all gateways added using the CS 2000 GWC Manager and the XML interface of the OSSgate application.



5 Click the **Associate** button.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately 1 minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click this button during a client session while data is retrieved for the Gateway site name field. To configure DNS on the CS 2000 Management Tools server, refer to the *Configuration Management* NTP for your solution, NN10409-500.

6 Use the following set of steps to datafill all of the attributes for the desired trunk gateway.



a In the Gateway profile name: field, select the appropriate trunk gateway profile name from the list of profiles.

The following table lists the trunk media gateway profiles supported. Once a profile is selected, the data associated with the profile is listed for the user to view.

Note 1: Ensure that the gateway is being added to the correct GWC node.

Note 2: Newly supported gateways may be added to the list and they are not shown in this procedure. Not all gateways are supported for every solution and release

Note 3: If necessary, contact your Nortel Networks support for details on the gateways supported for each profile.

Trunk media gateway profiles (Sheet 1 of 2)

Gateway profile name	Gateway category	Signal protocol type	Protocol version	Default protocol port	Service type	Maximum port/ endpoint capacity
AUDIOCODES (Nortel Media Gateway 3200)	Large	MEGACO	1.0	2944	Trunk	280
CVX600_612	Large	DSM-CC	5.2	13818	Trunk	612
CVX1800_2688	Large	DSM-CC	5.2	13818	Trunk	2688
NUERA_BTX4K	Large	TGCP	1.0	2427	Trunk	4032
NUERA_GX_ASPEN	Large	ASPEN	2.1	2427	Trunk	2108
NUERA_GX_MEGACO	Large	MEGACO	1.0	2944	Trunk	2108
PVG7K_ASPEN	Large	ASPEN	2.1	2427	Trunk	1008
PVG7K_MEGACO	Large	MEGACO	1.0	2944	Trunk	1008
PVG15K_1000_ASPEN	Large	ASPEN	2.1	2427	Trunk	1000
PVG15K_1000_MEGACO	Large	MEGACO	1.0	2944	Trunk	1000
PVG15K_ASPEN	Large	ASPEN	2.1	2427	Trunk	1120
PVG15K_MEGACO	Large	MEGACO	1.0	2944	Trunk	1120
PVG15K_PARTIAL _ASPEN	Large	ASPEN	2.1	2427	Trunk	624

Trunk media gateway profiles (Sheet 2 of 2)

Gateway profile name	Gateway category	Signal protocol type	Protocol version	Default protocol port	Service type	Maximum port/ endpoint capacity
PVG15K_PARTIAL _MEGACO	Large	MEGACO	1.0	2944	Trunk	624
PVG_APG_ASPEN	APG	ASPEN	2.1	2427	APG	1120
PVG_APG_MEGACO	APG	MEGACO	1.0	2944	APG	1120
PVG_APG_VSP3 _ASPEN	APG	ASPEN	2.1	2427	APG	2016
PVG_APG_VSP3 _MEGACO	APG	MEGACO	1.0	2944	APG	2016
Note: The APG functionality has been removed in the SN07 release. All above APG-related profiles are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles.						
PVG_VSP3_ASPEN	Large	ASPEN	2.1	2427	Trunk	2016
PVG_VSP3_MEGACO	Large	MEGACO	1.0	2944	Trunk	2016
TGCP	Large	TGCP	1.0	2427	Trunk	4032

b In the Gateway name: field, type a gateway name according to the gateway profile. Use the suggested gateway naming conventions shown in the following table.

Note: The media gateway name must be unique within the CS 2000. Duplicate media gateway names cannot exist even if the media gateways are associated with different GWCs.

Trunk gateway naming conventions (Sheet 1 of 2)

Gateway profile	Suggested gateway naming conventions
AUDIOCODES (Nortel Media Gateway 3200)	Up to 8 alpha-numeric characters: 3 to 4 upper case characters followed by up to 4-5 numeric characters in the following format: NNNnnn Example: M2K003

Trunk gateway naming conventions (Sheet 2 of 2)

Gateway profile	Suggested gateway naming conventions
CVX600 CVX1800	Up to 8 upper case characters in the following format: CVX<nn> *where* <nn> is device number of the CVX gateway chassis
NUERA_BTX4K	Use a domain name of the media gateway in the form of an absolute domain name including the host_name of the device, suitable for lookup using Directory Name Service (DNS). The name must contain a "." and be no longer than 32 characters. Example: cust34671.rdu.cablevendor.net
NUERA_GX	Up to 8 alpha-numeric characters; 3-4 upper case characters followed by up to 4-5 numeric characters in the following format: NGXnnn Example: NGX003
PVG7K, PVG15K, PVG15K_1000 PVG15K_PARTIAL PVG_APG PVG_VSP3 PVG_APG_VSP3	Up to 8 upper case characters in the following format: PVG<nn><lp> *where* <nn> is device number of the PVG chassis <lp> is the slot number of the logical processor card for the VSP in the PVG (recommended slots 6-11)
TGCP	Do not use the underscore character (_) in gateway names. This rule applies to all TGCP gateways.

c In the Gateway IP address: field, type an address of the media gateway. Use the format:
<0-255>.<0-255>.<0-255>.<0-255>

d If necessary, in the Gateway controller name: field, use the drop-down menu to select a GWC node with which the gateway is being associated.

If a GWC is not specified, the node provisioning application will automatically discover a GWC node with which to

associate this gateway. The choice of GWC node is based on the service type of the media gateway (line, H.323, trunk, or audio) and the endpoint capacity of the gateway.

e In the Reserved terminations: field, type the number of reserved terminations (endpoints or ports) to be supported on the gateway.

Note: If you do not assign a value in this field, the system will use the default, which is the maximum number of reserved terminations for the gateway selected.

The different capacities for trunk gateway appear in the Trunk media gateway profiles on page 139. The total number required cannot exceed the capacity of a GWC node, which has a maximum capacity of 4094 ports.

To calculate the correct number of the reserved terminations or endpoints on your gateway to match the available endpoints on the selected GWC node, refer Changing reserved terminations - examples on page 143 for a worksheet along with some examples.

f In the Protocol type: field, use the drop-down menu to select the appropriate gateway protocol type. Refer to Trunk media gateway profiles on page 139 to determine the appropriate settings for the gateway type you wish to configure.

Note: The system restricts the protocol type options to those compatible with the gateway profile name selected previously.

g In the Protocol port: field, use the default value provided. Do not change this value.

Note: The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name and protocol type select previously.

7 Click the **OK** button to apply the data.

A response dialog box appears. The response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

8 Repeat this procedure as required for trunk gateways you wish to associate with this or other GWC nodes.

9 The procedure is complete.

Changing reserved terminations - examples

You must ensure that the total number of endpoint terminations required by all of the large media gateways associated to the same GWC node do not exceed 4094 ports. If they do, the last media gateway association activity will fail. Use the following method to allow multiple large media gateways to be associated with a single GWC node.

Calculating optimal reserved endpoint terminations

You can adjust the number of usable endpoints terminations (related to maximum port/endpoint capacity) required by the media gateway to a lower value. The formula used to calculate the value of the correct number of endpoint terminations varies according to the market in which your Carrier VoIP product is installed. Ports are allocated by trunk channel. In the North American market, trunks are based on increments of 24 channels or DS0s per endpoint group, while in the International market trunks are based on increments of 31 channels or DS0s per endpoint group. Only complete endpoint groups (24 or 31) can be provisioned against a trunk gateway. Refer to procedure Add carriers to a GWC on page 201 for more information about adding carrier endpoints.

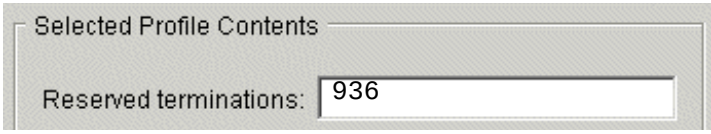
Calculating reserved terminations in the NA market - Example 1

You have a media gateway with a maximum reserved endpoints value of 1000 and the GWC node you want to associate with it has only 950 available endpoints. You must reduce the value in the Reserved Terminations: field so that it is less than or equal to the number of available ports on the GWC node, and so that it is also divisible by 24 (based on 24 ports per channel) with no remainder.

950 / 24 = 35 with a remainder of 14 (these are unused ports)

35 x 24 ports per channel = 936 used gateway ports

In this case, the closest you can get to using all 950 available ports on the GWC node is 936, based on allocating 24 ports per channel. This configuration will support 930 carrier endpoints managed by a single GWC node. You must change the endpoint value for that gateway to 936 in the Reserved Terminations: field.



Calculating reserved terminations in the NA market - Example 2

You want to associate four PVG15K media gateways on a single GWC by optimizing the reserved endpoints available for each PVG without exceeding the available endpoint capacity of the GWC node.

1 PVG w/1120 max. with reserved endpoints at 1056 (44 X 24)
3 PVGs w/1120 max. with reserved endpoints at 1008 (42 X 24)

This configuration uses 4080 ports with 14 unused gateway ports.

Calculating reserved terminations in the Intl. market - Example 1

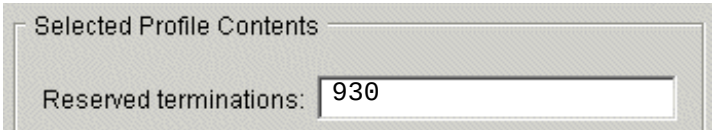
You have a media gateway with a maximum reserved endpoints value of 1000 and the GWC node you want to associate it with has only 950 available endpoints. You must reduce the value in the Reserved Terminations: field so that it is less than or equal to the number of available ports on the GWC node and so that it is also divisible by 31 (based on 31 ports per channel) with no remainder.

950 / 31 = 30 with a remainder of 20 (these are unused ports)

and

30 x 31 ports per channel = 930 used gateway ports

In this case, the closest you can get to using all 950 available ports on the GWC node is 930, based on allocating 31 ports per channel. This configuration will support 930 carrier endpoints managed by a single GWC node. You would change the endpoint value for that gateway to 930 in the Reserved Terminations: field.



Calculating reserved terminations in the Intl. market - Example 2

You want to associate four PVG15K media gateways on a single GWC by optimizing the reserved endpoints available for each PVG without exceeding the available endpoint capacity of the GWC node:

1 PVG w/1120 max. with reserved endpoints at 1116 (36 X 31)
3 PVGs w/1120 max. with reserved endpoints at 992 (32 X 31)

This configuration uses 4092 ports with 12 unused gateway ports.

Configure the domain name for MTA gateways (cable market)

Purpose of this procedure

Use this procedure to configure a common domain name for all multimedia terminal adapters (MTA) running network-based call signaling (NCS) protocol and associated with the specified Gateway Controller (GWC) node. To do that, associate a media gateway (configured with the DOMAIN_NAME profile and known as a "dummy" gateway) to the selected GWC.

The domain name capability allows a fully qualified domain name (FQDN) of an MTA gateway (in the cable market) to be broken into a <host_name> part and a <domain_name> part. This permits longer (maximum of 61 to 63 characters, depending on the GWC node number) FQDNs for MTA gateways. This longer FQDN consists of the following components:

- <host_name> portion: gateway-specific name; for example, my_mta_host_name
- <domain_name> portion: a gateway domain name common to all MTA gateways associated with a GWC; for example, 001.my_domain_name

> ***Note:*** When configuring the gateway name, you must add the GWC number in front of the <domain_name>. However, the FQDN will not include the GWC number. The system will combine only the <domain_name> (without the GWC number) with the MTA <host_name> name for both domain name service (DNS) lookups and NCS processing.

This procedure describes how to configure the gateway domain name, common to all MTAs associated with a GWC.

To configure the gateway-specific name for each MTA, refer to procedure Associate a small line media gateway (cable market) on page 153.

When to use this procedure

This procedure is optional. Use this procedure when the FQDN (combined host and domain name) of the MTA contains more than 32 characters.

Complete this procedure before associating MTAs to a GWC.

Prerequisites and guidelines

CAUTION
Possible partial service disruption
Use the DOMAIN_NAME media gateway profile only on a GWC node configured with the SMALL_LINEINTL or SMALL_LINENA service profile associated with MTAs running NCS protocol.

For example, if domain name capability is used on a GWC using media gateway control protocol (MGCP), it will affect DNS naming but not MGCP signaling. This will lead to inconsistencies and possible failures during a dead shelf recovery of a GWC when DNS is heavily used.

CAUTION
Possible loss of service
If there are MTAs configured on a GWC in the 32-character FQDN format, and you add the DOMAIN_NAME "dummy" gateway, all MTAs will be out of service until the <host_name> for each MTA is re-provision correctly.

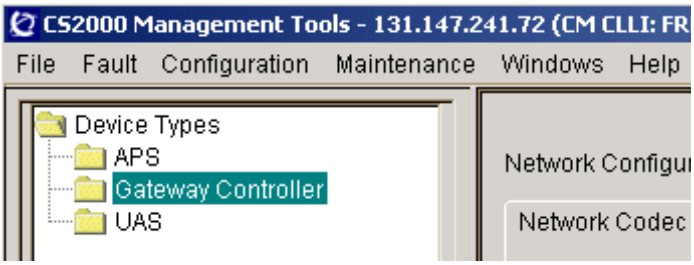
The following guidelines apply to this procedure:

- The domain name capability is available for MTA gateways running NCS protocol and associated with a GWC node. Other gateway types continue to have a restriction of 32 characters for their FQDN.
- Only one media gateway with the DOMAIN_NAME profile can be provisioned on a GWC node.
- Once configured, you cannot change the domain name of the MTA gateways associated with a GWC. You have to delete the existing DOMAIN_NAME gateway and add a new one. However, this action results in an outage since for a period of time, the GWC does not have a domain name.
- The DOMAIN_NAME gateway name can have up to 32 ASCII characters. For details, refer to step 7 in this procedure.
- The DOMAIN_NAME gateway name must always include a ".", which separates the GWC number from the <domain_name>.
- The DOMAIN_NAME gateway is a "dummy" gateway, which will always show as "out of service". Even though this gateway will have one endpoint, do not configure it with any lines.

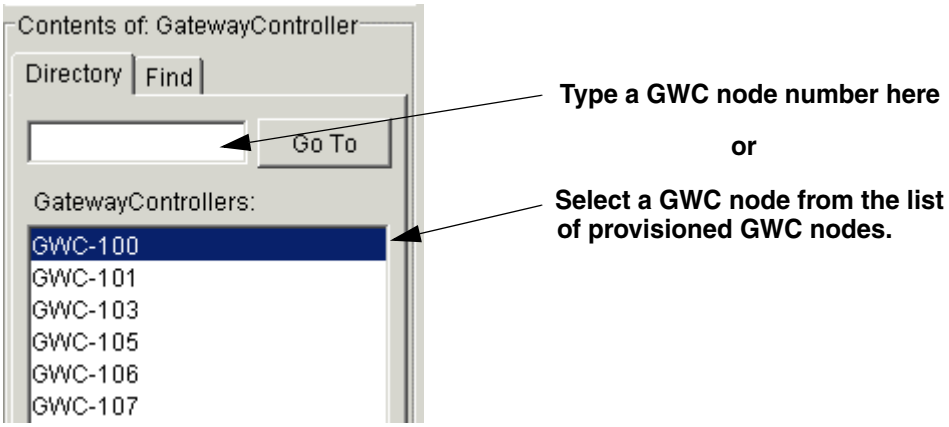
Action

At a CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

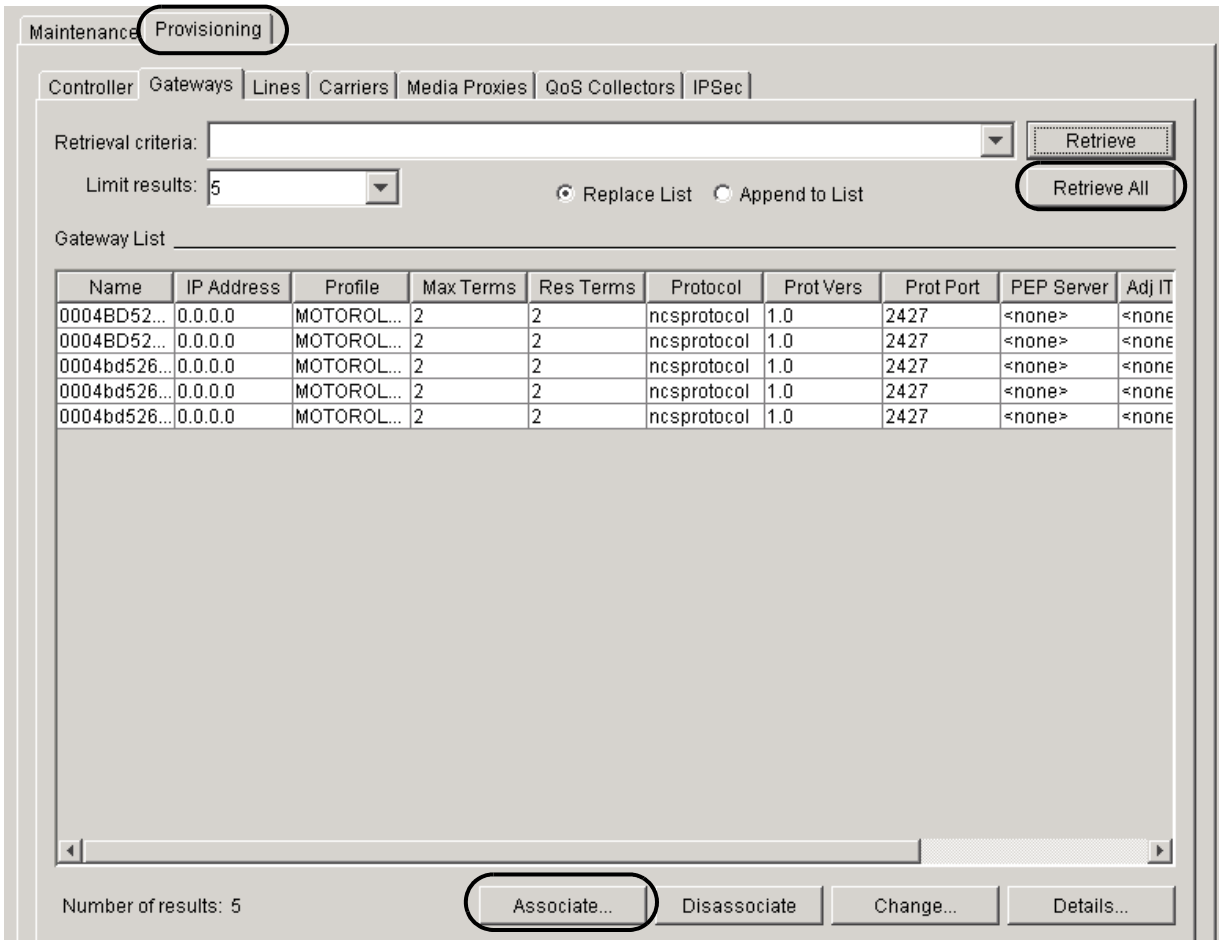


2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate a media gateway.



3 Click the **Provisioning** tab.

4 Click the **Gateways** tab. If you wish view information about gateways associated with the selected GWC node, click the **Retrieve All** button. Any newly-created gateways are added to the end of the list. The list will contain all gateways added using the CS 2000 GWC Manager and using the XML interface of the OSSgate application.



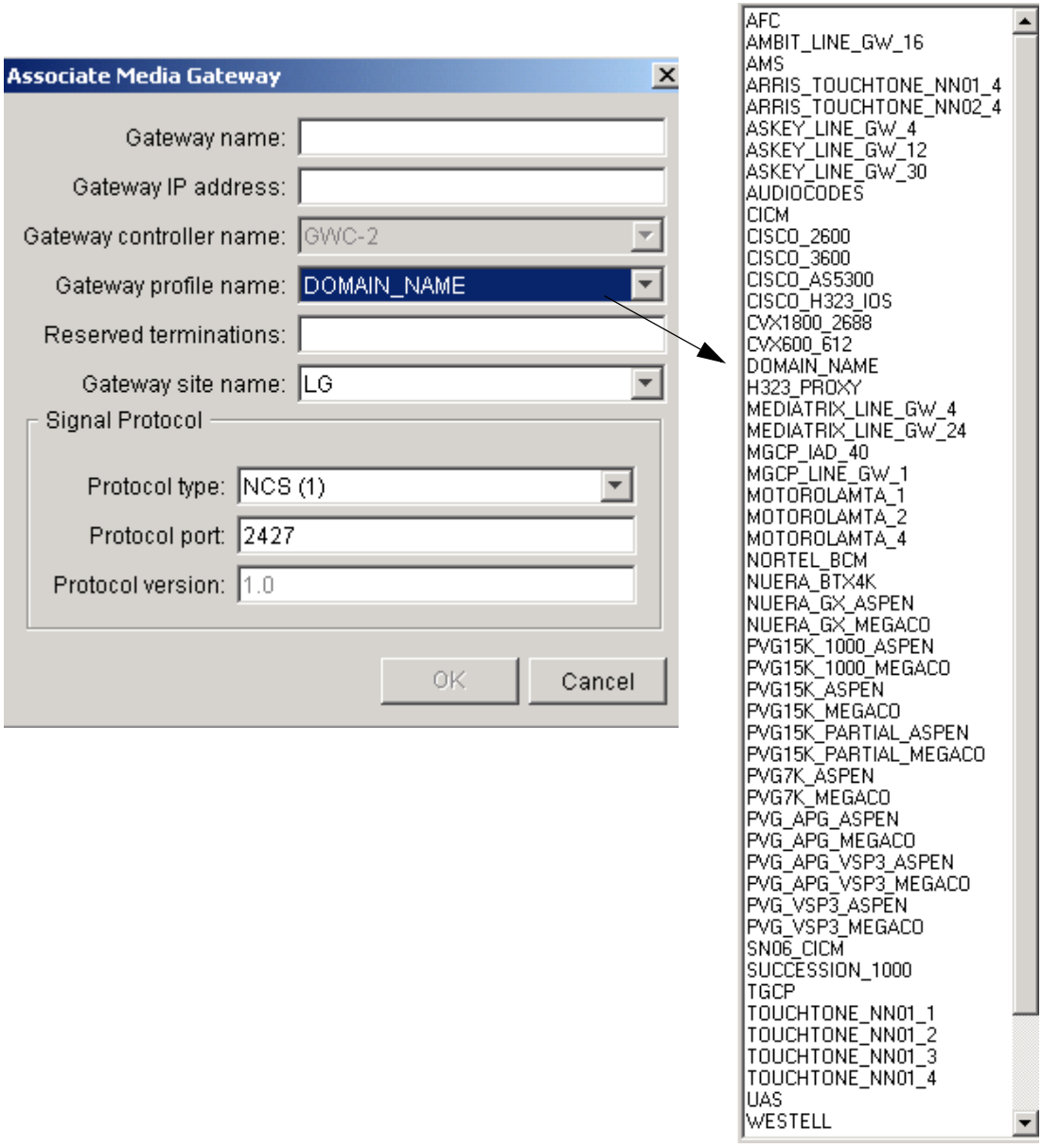
5 Click the **Associate** button to display the Associate Media Gateway dialog box.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately 1 minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click the Associate button during a client session while data is retrieved for the Gateway site name: field. To configure DNS on the CS 2000 Management Tools server, refer to the *Configuration Management* NTP for your solution, NN10409-500.

6 In the Gateway profile name: field, select the profile DOMAIN_NAME using the drop-down menu. Refer to table Attributes associated with the DOMAIN_NAME gateway profile on page 150 for details about the DOMAIN_NAME profile.

Note 1: Once a profile is selected, the applicable fields associated with this profile are displayed in the Associate Media Gateway dialog box.

Note 2: Ensure that you are adding the DOMAIN_NAME gateway to the correct GWC node (SMALL_LINENA or SMALL_LINEINTL).



The following table provides details about the DOMAIN_NAME gateway profile.

Attributes associated with the DOMAIN_NAME gateway profile

Attribute	Value
Gateway category	Small
Signaling protocol type	NCS
Protocol version	1.0
Default protocol port	2427
Service type	Line, DQos
Maximum port/endpoint capacity	1

7 In the Gateway name: field, type a name (up to 32 ASCII characters) for all MTA gateways associated with the selected GWC. You must follow naming conventions described in the following table.

Note: The media gateway name must be unique within the CS 2000. Duplicate media gateway names cannot exist even if the media gateways are associated with different GWCs.

DOMAIN_NAME gateway naming conventions

Gateway profile	Naming conventions
DOMAIN_NAME	The gateway name must be no longer than 32 ASCII characters (including a "." between the GWC number and the domain name). Use the following format: **<GWC_number>.<domain_name>** *where* <GWC_number> is the one- to three-digit number of the GWC node on which you are configuring the DOMAIN_NAME gateway. The number can be from 0 to 255; 0 (zero) padding is allowed but not required. This number must be followed by a "." (period). ***Note:*** This portion of the gateway name will not be included in the FQDN of an MTA. The system will combine only the <domain_name> portion with the MTA name for DNS lookups and NCS processing. <domain_name> is the domain name for all MTAs associated with this GWC. This part of the gateway name must follow the Directory Name Service (DNS) and RFC 1034 naming rules, and must consist of no more than 28 to 30 characters (depending on the length of the <GWC_number>). For example, if the GWC node number is 25 (two characters), followed by a "." (one character), you can enter up to 29 characters for the actual domain name. ***Note:*** You can use a "." (period) and "-" (dash) in the <domain_name>, but these characters are not mandatory. **Example** If you want to configure the domain name "mta.cablevendor.com" on the GWC 1, enter the following name in the Gateway name field: 1.mta.cablevendor.com

8 In the Gateway IP address: field, enter the IP address of the gateway. Use the following format:
<0-255>.<0-255>.<0-255>.<0-255>

Note: The IP address field is not used for the "dummy" DOMAIN_NAME gateway. You can type any valid IP address. The recommended value is "0.0.0.0".

9 The Gateway controller name: field specifies the GWC node to which the domain name applies, for example, GWC-1.

This field is pre-defined, you cannot change it.

10 In the Reserved terminations: field, type the number of reserved terminations (endpoints or ports) to be supported on the gateway. Enter the default value of 1.

Note: If you do not assign a value in this field, the system will use the default value.

11 In the Gateway site name: field, select a site name from the drop-down list provided. LG is the default.

Note: This list of site names comes from table SITE in XA-Core.

12 The Protocol type: field is pre-defined with the value of NCS(1), which is the only protocol compatible with the DOMAIN_NAME gateway profile.

13 The Protocol port: field is pre-defined with the default value of 2427. Do not change this value.

14 The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name and protocol type select previously. You cannot change this value.

15 Click the **OK** button to apply the input.

A response dialog box appears indicating that the system is processing the requested change. It can take up to 5 minutes for the change to be processed. During this time a “Timed Out” window may appear. This requires no action. When processing is complete, the response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

Note: Once configured, you cannot change the domain name of the MTA gateways associated with a GWC. You have to delete the existing DOMAIN_NAME gateway and add a new one. However, this action results in an outage since for a period of time, the GWC does not have a domain name.

16 The procedure is complete.

Associate a small line media gateway (cable market)

Purpose of this procedure

Use this procedure to associate a small line media gateway for the cable market with a specific Gateway Controller (GWC) node. In this case, a policy enforcement point (PEP) or an application layer gateway (ALG) may be included in the topology.

A gateway profile is a definition in the CS 2000 Management Tools database (CS 2000 GWC Manager database) that captures some of the characteristics and capabilities of a gateway device. A profile is chosen when the gateway is being provisioned. The information in the profile is then used to determine compatibility of the GWC node on which the gateway is being provisioned and to assess whether the node can support the added endpoint capacity.

Note: Starting in SN08, you can change some gateway attributes defined by a profile (such as, the maximum endpoint capacity) by changing the profile for the selected gateway. For more information, refer to procedure Change gateway attributes on page 277.

When to use this procedure

Use this procedure when you wish to associate a small line media gateway with a GWC node (in the cable market).

Prerequisites and guidelines

The following guidelines apply to this procedure:

- If you are associating a multimedia terminal adapter (MTA) gateway and you wish to take advantage of the DOMAIN_NAME capability, you must first complete procedure Configure the domain name for MTA gateways (cable market) on page 145, before proceeding with this procedure.
- When you assign a media gateway name, the name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist, even if the media gateways are associated with different GWCs. CS 2000 GWC Manager will reject duplicate media gateways.
- If you attempt to associate a media gateway with a GWC that has a different service type, the request is rejected. For example, you cannot associate a line media gateway with a trunk GWC.
- You must ensure that the total number of endpoint terminations required by all of the large media gateways associated to the same GWC node do not exceed 4094 ports. If you attempt to associate a

media gateway with a GWC that does not have adequate available capacity, the request is rejected.

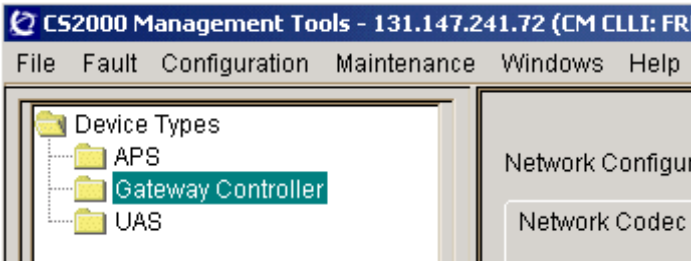
Example: You cannot associate a media gateway with a GWC if the gateway has a maximum-reserved-endpoints value of 4 and the GWC has only 3 available endpoints/TIDs.

Note: If you wish to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC, click the **Statistics** button under the **Controller** tab of the **Provisioning** panel. If required, refer to procedure View characteristics of a GWC node on page 239.

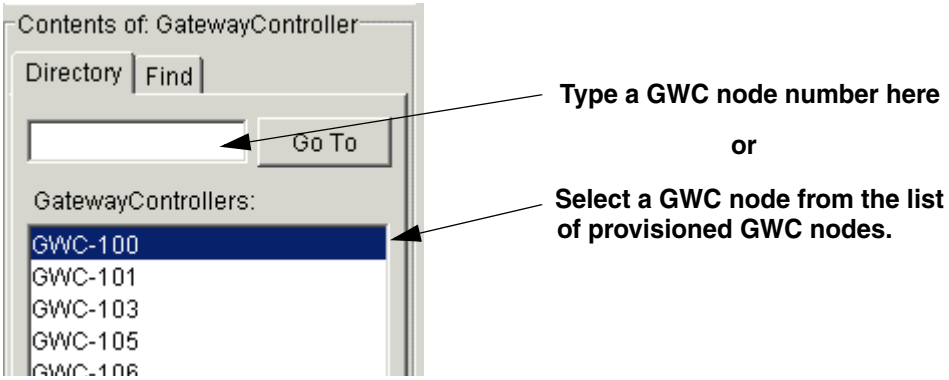
Action

At a CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

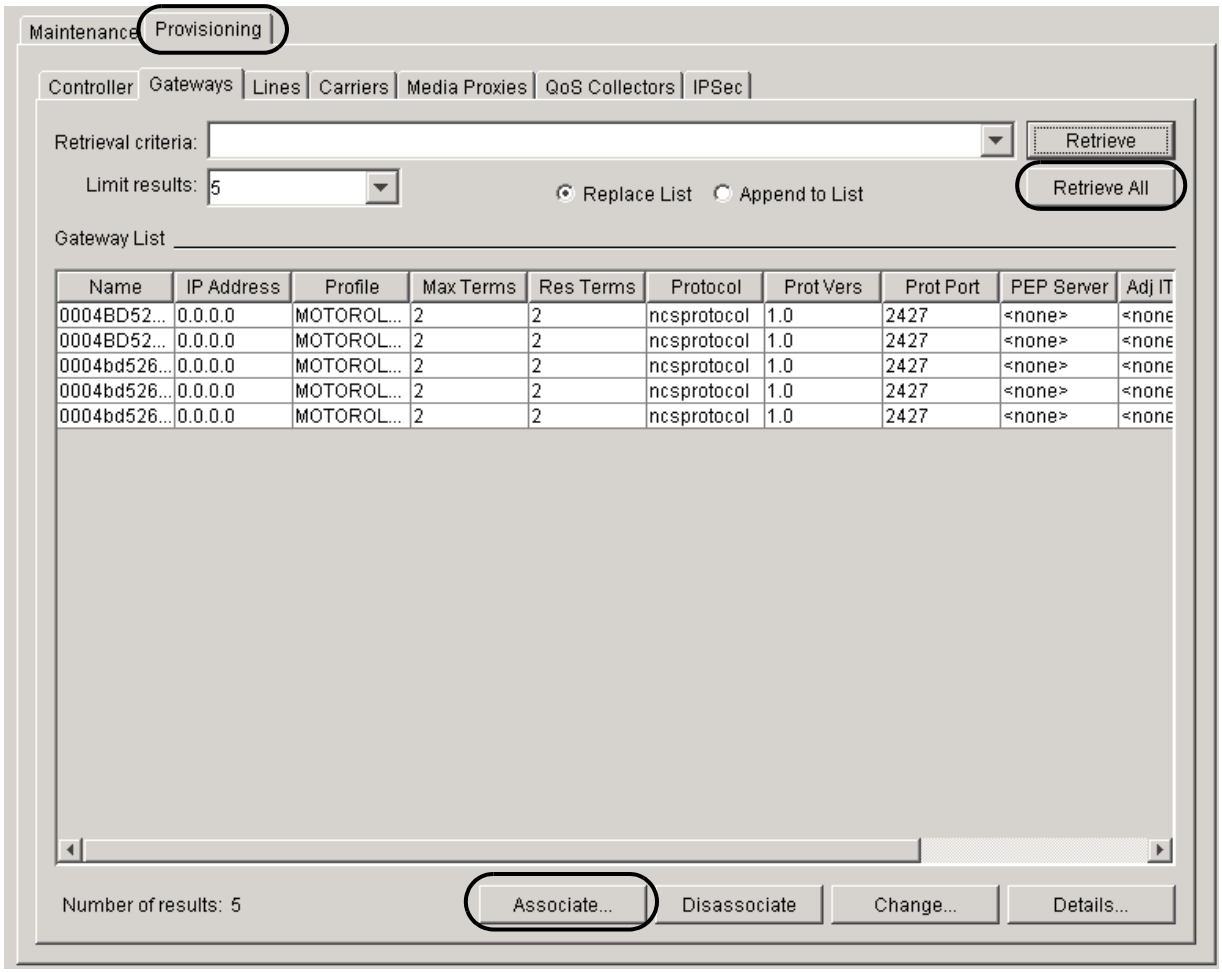


2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate a media gateway.



3 Click the **Provisioning** tab.

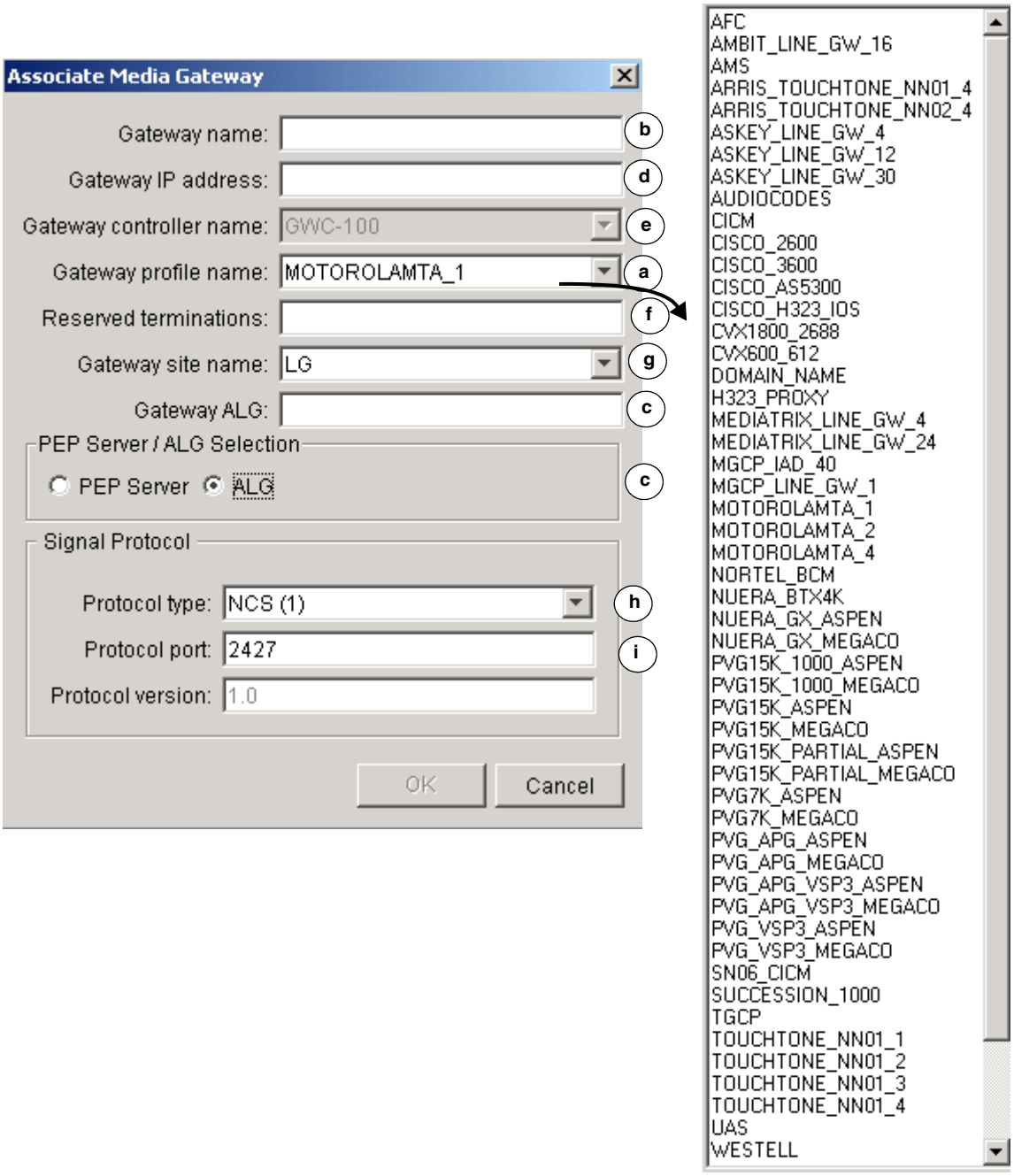
4 Click the **Gateways** tab, then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list will contain all gateways added using the CS 2000 GWC Manager and using the XML interface of the OSSgate application.



5 Click the **Associate** button.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately 1 minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click this button during a client session while data is retrieved for the Gateway site name: field. To configure DNS on the CS 2000 Management Tools server, refer to the *Configuration Management* NTP for your solution, NN10409-500.

6 Use the following set of steps to datafill all of the attributes for the desired gateway.



a In the Gateway profile name: field, select an appropriate line gateway profile name using the drop-down menu. See the following table for details about each small line media gateway profile.

Once a profile is selected, the configuration fields associated with the profile are listed for the user to view.

Note 1: Ensure that the line gateway is being added to the correct GWC node.

Note 2: Newly supported gateways may be added to the list and are not shown in this procedure. Not all gateways are supported for every solution and release.

Small line media gateway profiles and associated attributes (cable market)

Gateway profile name	Gateway category	Signal protocol type	Protocol version	Default protocol port	Service type	Max. port/ endpoint capacity
ARRIS_TOUCHTONE_ NN01_4	small	NCS	1.0	2427	Line, DQoS	4
ARRIS_TOUCHTONE_ NN02_4	small	NCS	1.0	2427	Line, DQoS	4
DOMAIN_NAME[1]	small	NCS	1.0	2427	Line, DQos	1
MOTOROLA MTA_1	small	NCS	1.0	2427	Line, DQoS	1
MOTOROLA MTA_2	small	NCS	1.0	2427	Line, DQoS	2
MOTOROLA MTA_4	small	NCS	1.0	2427	Line, DQoS	4
TOUCHTONE_NN01_1	small	NCS	1.0	2427	Line, DQoS	1
TOUCHTONE_NN01_2	small	NCS	1.0	2427	Line, DQoS	2
TOUCHTONE_NN01_3	small	NCS	1.0	2427	Line, DQoS	3
TOUCHTONE_NN01_4	small	NCS	1.0	2427	Line, DQoS	4

1.The DOMAIN_NAME profile provides the capability to configure a common domain name for all MTA gateways associated with the selected GWC. For more information, refer to procedure Configure the domain name for MTA gateways (cable market) on page 145.

b In the Gateway name: field, type a name for the line gateway according to the gateway profile. Use the suggested gateway naming conventions shown in the following table.

Note: The media gateway name must be unique within the CS 2000. Duplicate media gateway names cannot exist even if the media gateways are associated with different GWCs.

Line media gateway naming conventions

Gateway profile	Suggested gateway naming convention
All MOTOROLA MTA (when using the DOMAIN_NAME capability)	Provide a gateway-specific name, which will constitute the <host> part of the fully qualified domain name (FQDN) of the MTA gateway. Use a name suitable for lookup using Directory Name Service (DNS). This section of the FQDN (host name for the specific MTA gateway) must be no longer than 32 characters, and it *does not* have to include a "." or a "-". Examples: cust3467 cust1.3467 cust-1.3467 ***Note:*** The whole FQDN must consist of no more than 61 to 63 characters, depending on the GWC node number. For details and for information on the <domain_name> part of the FQDN, refer to procedure Configure the domain name for MTA gateways (cable market) on page 145.
All MOTOROLA MTA (when not using the DOMAIN_NAME capability) All TOUCHTONE_NN All ARRIS TOUCHTONE_NN	Use a domain name of the media gateway in the form of an absolute domain name including the host name of the device, suitable for lookup using Directory Name Service (DNS). The name must be no longer than 32 characters. A "." (period) can be included, but it is not required. Example: cust34671.rdu.cablevendor.net

c Select the middlebox that you want to assign to the gateway:

- If you wish to assign a policy enforcement point (PEP) server, click the PEP Server radio button. In the newly displayed Gateway PEP server: field, type the name of a PEP server, or type **none** if no PEP server is available.
- If you wish to assign an application layer gateway (ALG), click the ALG radio button. In the newly displayed Gateway ALG: field, type the name of an ALG, or type **none** if no ALG is available.

d

CAUTION
Possible loss of service
If you want to use an IP address of 0.0.0.0 for the small line gateway that you are associating with the selected GWC, make sure that a Domain Server is configured for that GWC. Otherwise, the line will not recover after the GWC cold switch of activity (SwAct).

If required, refer to procedure Manually re-provision GWC cards on page 115 for how to verify and change basic GWC node configuration values, including Domain Servers IP addresses.

In the Gateway IP address: field, enter the IP address of the gateway. Use the format:
<0-255>.<0-255>.<0-255>.<0-255>

Note 1: For gateways in the "small" category, you can type an IP address of "0.0.0.0" in this field. If you type this address, the GWC will attempt to discover the IP address for the gateway, but the line or lines will not recover after a network outage if no Domain Server is configured for the GWC.

Note 2: If you selected ALG in the previous step, leave this field blank. The system assigns the IP address of 0.0.0.0.

e If necessary, in the Gateway controller name: field, select a GWC node with which the gateway is being associated.

Note: If a GWC is not specified, the node provisioning applications will automatically discover a GWC node with which to associate this gateway. The choice of GWC node is based on the service type of the media gateway (line,

trunk, or audio) and the “maximum reserved endpoints” (the potential size of the media gateway).

f In the Reserved terminations: field, type the number of reserved terminations (endpoints or ports) to be supported on the gateway.

Note: If you do not assign a value in this field, the system will use the default, which is the maximum number of reserved terminations for the gateway selected.

The different capacities for line gateways appear in the Small line media gateway profiles and associated attributes (cable market) on page 157. The total number required cannot exceed the maximum capacity of a GWC node, which is 4094 ports.

g In the Gateway site name: field, select a site name from the drop-down list. LG is the default.

h In the Protocol type: field, select the appropriate gateway protocol type using the drop-down menu.

Note: The system restricts the protocol type options to those compatible with the gateway profile name selected previously.

i In the Protocol port: field, use the default value provided. Do not change this value.

Note: The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name and the protocol type selected previously.

7 Click the **OK** button to apply the input.

Once the **OK** button is clicked, a response dialog box appears indicating that the system is processing the requested change. It can take up to 5 minutes for the change to be processed. During this time a “Timed Out” window may appear. This requires no action. When processing is complete, the response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

8 Repeat this procedure as required for gateways you wish to associate to this or other GWC nodes.

9 The procedure is complete.

Associate a line media gateway (wireline market)

Purpose of this procedure

Use this procedure to associate a line media gateway for the wireline market with a specific Gateway Controller (GWC) node. In this case, a network service zone may be included in the topology.

A gateway profile is a definition in the CS 2000 Management Tools database (CS 2000 GWC Manager database) that captures some of the characteristics and capabilities of a gateway device. A profile is chosen when the gateway is being provisioned. The information in the profile is then used to determine compatibility of the GWC node on which the gateway is being provisioned and to assess whether the node can support the added endpoint capacity.

Note: Starting in SN08, you can change some gateway attributes defined by a profile (such as, the maximum endpoint capacity) by changing the profile for the selected gateway. For more information, refer to procedure Change gateway attributes on page 277.

When to use this procedure

Use this procedure when you wish to associate a line media gateway for the wireline market with a GWC node.

Prerequisites and guidelines

Network zones, including network address translator (NAT)-type and limited bandwidth links (LBL)-type service zones, must be configured before any media gateways that use the service zones can be associated with a GWC. Add a network zone to the GWC database using one of the following procedures:

- To add an IP-VPN (NAT) zone, refer to procedure Add an IP-VPN (NAT) zone on page 317.
- To add an LBL, refer to procedure Add a limited bandwidth link (LBL) zone on page 331.
- To add a composite IP-VPN (NAT) and LBL zone, refer to procedure Add a composite IP-VPN (NAT) and LBL zone on page 343.

Note 1: If your network configuration does not include the Policy Controller (Network VCAC status is OFF), all the gateways behind a given LBL must be controlled by the same GWC. This restriction does not apply, if the Network VCAC status is ON.

Note 2: A GWC card provisioned to support small line gateways can accommodate up to 2000 network zones. A GWC card provisioned

to support large line gateways can accommodate up to 150 network zones.

If you attempt to associate a media gateway with a GWC that has a different service type, the request is rejected. For example, you cannot associate a line media gateway with a trunk GWC.

When you assign a media gateway name, the name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist, even if the media gateways are associated with different GWC. CS 2000 GWC Manager will reject duplicate media gateways.

You must ensure that the total number of endpoint terminations required by all of the media gateways associated to the same GWC node do not exceed 4094 ports. If you attempt to associate a media gateway with a GWC that does not have adequate available capacity, the request is rejected.

Example: You cannot associate a media gateway with a GWC if the gateway has a maximum-reserved-endpoints value of 1000 and the GWC has only 950 available endpoints/TIDs.

Note: If you wish to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC, click the **Statistics** button under the **Controller** tab of the **Provisioning** panel. If required, refer to procedure View characteristics of a GWC node on page 239.

Centrex IP Client Manager gateways

Starting in SN07, to ensure that Centrex IP Client Manager (CICM) gateways support virtual call admission control (VCAC), the procedure to associate a CICM gateway differs from the procedure supporting small line gateways. The CICM procedure is different for the following reasons:

- CICM gateways reside in the telephony service provider (TSP) domain. As a result, a CICM gateway is not ordinarily used in an environment with adjacent network zone.
- CICM endpoints are not fixed lines. CICM users can move from one area of an enterprise to another, from behind one network zone to another.

Note: CICM gateways have a service type of ITRANS_ROAM.

The CICM procedure allows you to identify a set of root (top-level) network zones for CICM gateways. Once the root zones are identified, the CS 2000 GWC Manager will send data for all related zones in the

hierarchy to the GWC. This ensures that when a CICM user logs onto the network, all relevant network zones will be available on the GWC.

The CS 2000 GWC Manager notifies the GWC card about all zones from the top level zones identified, down through the children to the leaves of the zone tree. The single line of parent zones is also sent to the GWC.

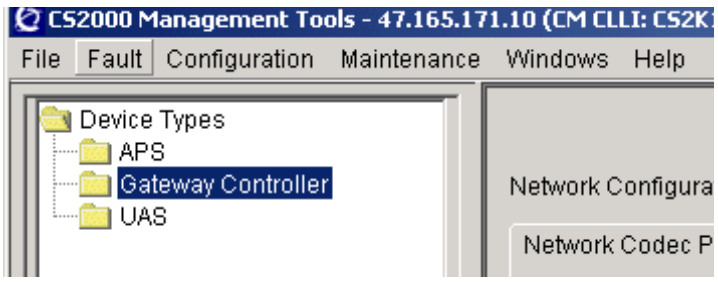
The following guidelines apply to GWCs associated with CICM gateways:

- A maximum of five root zones can be configured on a gateway.
- VCAC will not function if CICM telephony users roam outside the area provisioned with root zones.

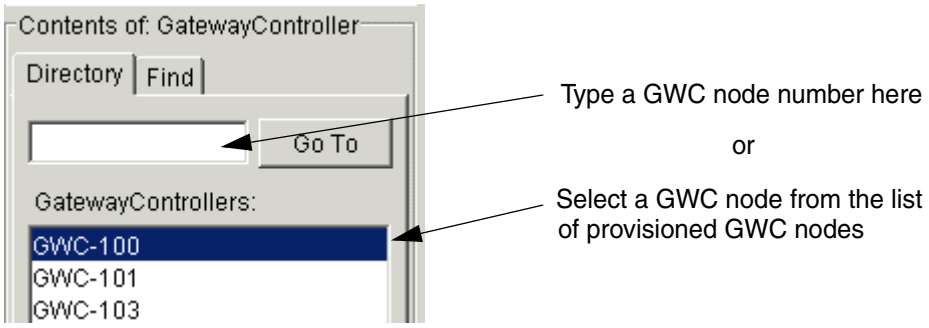
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate a media gateway.

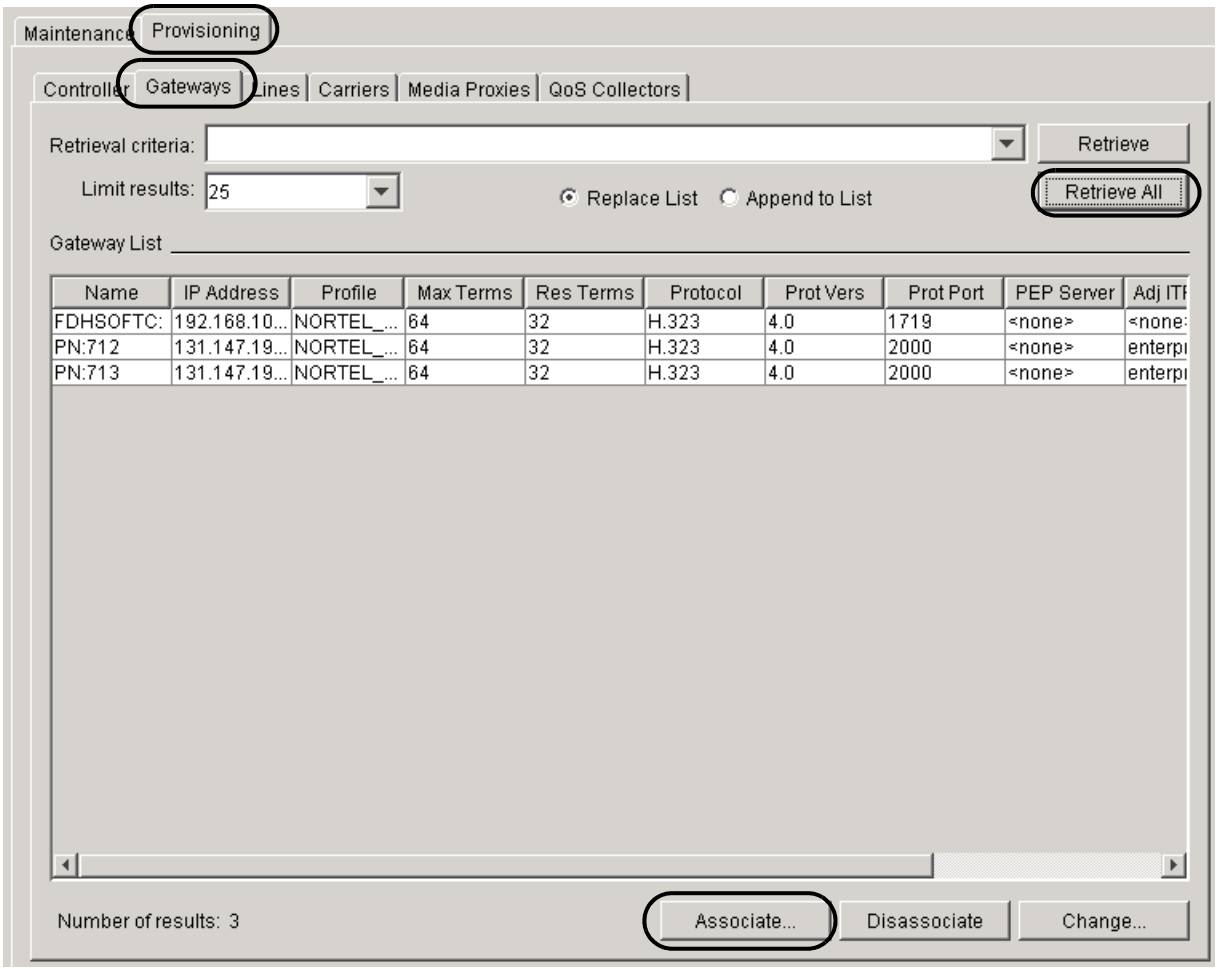


3 Click the **Provisioning** tab.

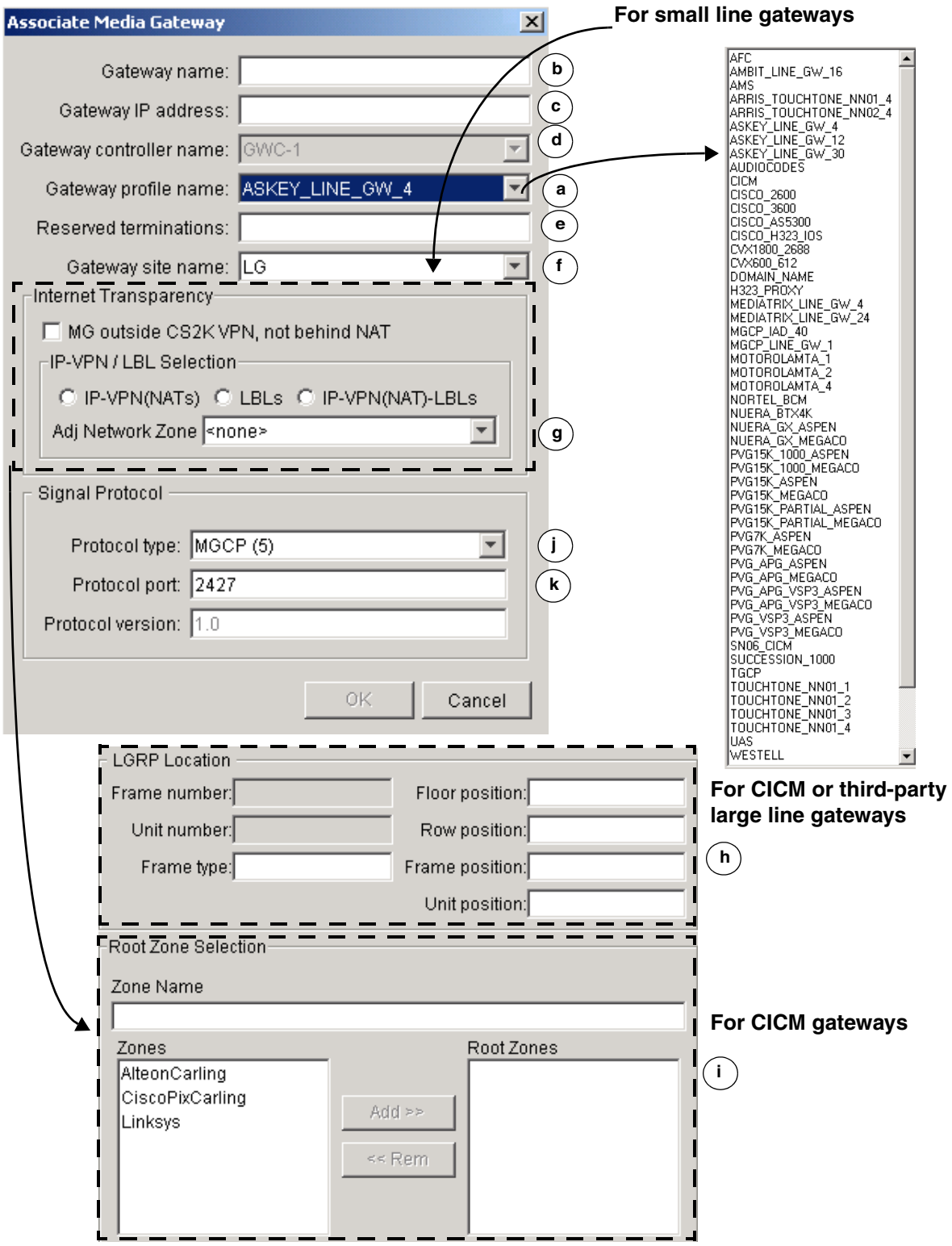
4 Click the **Gateways** tab, then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list will contain all gateways added using the CS 2000 GWC Manager and using the XML interface of the OSSgate application.

5 Click the **Associate** button.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately one minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click this button during a client session while data is retrieved for the Gateway site name: field. To configure DNS on the CS 2000 Management Tools server, refer to the *Configuration Management* NTP for your solution, NN10409-500.



6 Use the following set of sub-steps to datafill all of the attributes for the desired gateway.



a In the Gateway profile name: field, select the appropriate line gateway profile name using the drop-down menu.

Refer to the following table for details about line gateway profiles supported by this procedure. Once a profile is selected, the data associated with the profile is displayed.

Note 1: Ensure that the gateway is being added to the correct GWC node.

Note 2: Newly supported gateways may be added to the list and are not shown in this procedure. Not all gateways are supported for every solution and release.

Note 3: The SN06_CICM profile is present in the GWC Manager GUI, but it is not supported.

Line media gateway profiles (wireline market)

Gateway profile name	Gateway category	Signaling protocol	Protocol version	Default protocol port	Service type	Maximum port/ endpoint capacity
AFC	large	MEGACO	1.0	2944	Line	1023
AMBIT_LINE_GW_16	small	MGCP	1.0	2427	Line, ITRANS	16
ASKEY_LINE_GW_4	small	MGCP	1.0	2427	Line, ITRANS	4
ASKEY_LINE_GW_12	small	MGCP	1.0	2427	Line, ITRANS	12
ASKEY_LINE_GW_30	small	MGCP	1.0	2427	Line, ITRANS	30
CICM or CXIPCM	large	MEGACO	1.0	2944	Line, ITRANS_ROAM	1024
MEDIATRIX_GW_4	small	MGCP	1.0	2427	Line, ITRANS	4
MEDIATRIX_GW_24	small	MGCP	1.0	2427	Line, ITRANS	24
MGCP_IAD_40	small	MGCP	1.0	2427	Line, ITRANS	40
MGCP_LINE_GW_1	small	MGCP	1.0	2427	Line, ITRANS	1

b In the Gateway name: field, enter a gateway name according to the gateway profile. Use the suggested gateway naming conventions shown in the following table.

Note: The media gateway name must be unique within the CS 2000. Duplicate media gateway names cannot exist even if the media gateways are associated with different GWCs.

Line media gateway naming conventions

Gateway profile	Suggested gateway naming conventions
AFC All AMBIT line gateways All ASKEY line gateways All MEDIATRIX line gateways MGCP line gateways	Use a domain name of the media gateway in the form of an absolute domain name including the hostname of the device, suitable for lookup using Directory Name Service (DNS). The name must contain a "." and be no longer than 32 characters. Example: cust34671.rdu.cablevendor.net
CICM or CXIPCM	Use the recommended domain name of a Centrex IP Client Manger (CICM) gateway. Refer to the CICM customer documentation to perform this task.

c

CAUTION
Possible loss of service
For gateways in the "small" category, if you want to use an IP address of 0.0.0.0, make sure that a Domain Server is configured for the GWC. Otherwise, the line will not recover after the GWC cold switch of activity (SwAct).

If required, refer to procedure Manually re-provision GWC cards on page 115 for how to verify and change basic GWC node configuration values, including Domain Servers IP addresses.

In the Gateway IP address: field, enter the IP address of the gateway. Use the following format:
<0-255>.<0-255>.<0-255>.<0-255>

Note 1: If the gateway is behind an IP-VPN (NAT)-type network zone, specify the IP address on the CallServer side (customer VPN side) of the NAT device.

Note 2: For gateways in the “small” category, you can type an IP address of “0.0.0.0” in this field. If you type this address, the GWC will attempt to discover the IP address for the gateway, but the line or lines will not recover after a network outage if no Domain Server is configured for the GWC.

d If necessary, in the Gateway controller name: field, select a GWC node with which the gateway is being associated using the drop-down menu.

Note: If a GWC is not specified, the node provisioning applications will automatically discover a GWC node with which to associate this gateway. The choice of GWC node is based on the service type of the media gateway (line, trunk, or audio) and the endpoint capacity of the media gateway.

e In the Reserved terminations: field, type the number of reserved terminations (endpoints or ports) to be supported on the gateway.

Note: If you do not assign a value in this field, the system will use the default, which is the maximum number of reserved terminations for the gateway selected.

The different capacities for trunk gateway appear in the Line media gateway profiles (wireline market) on page 166. The total number required cannot exceed the maximum capacity of a GWC node, which is 4094 ports.

To calculate the correct number of the reserved terminations or endpoints on your gateway to match the available endpoints on the selected GWC node, refer Changing reserved terminations - examples on page 173 for a worksheet along with some examples.

f If applicable, in the Gateway site name: field, select a site name from the pull-down list (LG is the default). This list of site names is from table SITE in XA-Core. The site name can be from 1 to 4 alphanumeric characters, with the first character required to be an alpha character.

Use the following table to determine your next step.

If you are associating	Do
a small line gateway	go to step g
a CICM gateway or a large line gateway that supports displaying physical location of the gateway	go to step h
an AFC gateway	go to step j

g Configure internet transparency. Refer to section When a media proxy is used on page 174 for information on when a media proxy is inserted, depending on the location of the gateways involved in a call.

In the Internet Transparency section of the dialog box, complete *one* of the following tasks based on the following conditions:

- If the gateway is
  - — outside the CS 2000 carrier network
  - — outside the enterprise VPN
  - — not behind a network zone [IP-VPN (NAT), LBL, or composite NAT-LBL]

  select the checkbox “MG outside CS2K VPN, not behind NAT” and do not assign a zone.

  The gateway is in the public network. In this case, the gateway network zone name is set to a value of “outside the telecom service provider domain”. The Adj ITRANS MB column in the Gateway List appears as “outtsp” for any gateways in this category.
- If the gateway is
  - — outside the CS 2000 carrier network
  - — inside an enterprise VPN
  - — behind a network zone [IP-VPN (NAT), LBL, or composite NAT-LBL]

  do not select the checkbox “MG outside CS2K VPN, not behind NAT”.

Instead, select the name of an adjacent network zone in the Adj ITRANS Zone text field. Perform the following steps:

— Select the radio button for IP-VPN(NATs), LBLs, or IP-VPN(NAT)-LBLs to restrict your search.

— Click in the Adj Network Zone field.

— If desired, type text characters of a zone name in the field to fine tune your display. The system displays all network zones with a name that matches the characters you typed.

— Select adjacent network zone for the gateway from the list in the drop down menu.

Note: You can only select network zone names that are datafilled and appear in the Network Zones view in the CS 2000 GWC Manager. Refer to procedure Review available network devices on page 99.

The gateway is in the residential or enterprise VPN. In this case, the gateway network zone name is set to the NAT-type or LBL-type zone name. The Adj ITRANS MB column in the Gateway List appears as <zone name> for any gateways in this category.

- If the gateway is

  — inside the CS 2000 carrier network,

  do not select the checkbox “MG outside CS2K VPN, not behind NAT” and do not assign a network zone.

  The gateway is in the carrier VPN. In this case, the gateway network zone name is omitted (not used). The Adj ITRANS MB column in the Gateway List appears as “<none>” for any gateways in this category.

Continue with step j.

h If you selected a profile that supports displaying physical location of the gateway, the Associate Media Gateway dialog box includes the LGRP Location section.

Note 1: This option is only available for CICM and for the gateway profiles appropriately defined in their certificate files. Currently, only large line gateway profiles defined as third-party gateways support this option. For more information on creating gateway certificate files, refer to procedure Add a certificate file for a third-party gateway on page 265.

Note 2: For CICM gateways, fields Frame number: and Unit number: are not available.

Enter the physical location data for the selected gateway, as described in the following table.

Note: For all the fields described below as Optional, you must either not datafill any of them, or datafill all of them. You cannot datafill some and leave the others blank.

Field	Values	Description
Frame number	0 to 511	Does not apply to CICM profile. Enter the frame number.
Unit number	0 to 9	Does not apply to CICM profile. Enter the unit number.
Frame type	alphanumeric characters	Optional. Enter the unique frame type name. ***Note:*** For MG9K gateways, the only valid entry is MG9F.
Floor position	0 to 99	Optional. Enter a number to identify the unique floor within a unique Site (generally a building).
Row position	A...Z, AA...ZZ	Optional. Enter a value (from A...Z to AA...ZZ) to identify the unique row within a floor.
Frame position	0 to 99	Optional. Enter a number to identify the unique frame position within a row.
Unit position	0 to 77	Optional. Enter a number to identify the unique shelf position within a specific frame.

If you are associating a CICM gateway, continue with step i. Otherwise, go to step j

i Select root network zones. In the Root Zone Selection dialog box, complete the following steps:

- From the Zones list, select a root network zone that interacts with the gateway.

  If desired, type text characters in the Zone Name: field to display a specific group of zones. The system displays all zones with a name that matches the characters you type.

- Click the **Add >>** button to add your selection to the list of Root Zones.
- Repeat the two previous steps until you have a complete list of root zones.

  Note: A maximum of five root zones can be configured on a gateway.

- If desired, you can remove a zone from the Root Zones list. Select a zone and click the **<< Rem** button.

As a result of this configuration, the CS 2000 GWC Manager notifies the GWC card about all zones: from the top-level zones identified, down through the children to the leaves of the zone tree. The single line of parent zones is also sent to the GWC.

j In the Protocol type: field, select the appropriate gateway protocol type using the drop-down menu.

Note: The system restricts the protocol type options to those compatible with the gateway profile name selected previously.

k In the Protocol port: field, use the default value provided. Do not change this value.

Note: The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name and protocol type selected previously.

7 Click the **OK** button to apply the input.

A response dialog box appears indicating that the system is processing the requested change. It can take up to 5 minutes for the change to be processed. During this time a “Timed Out” window may appear. This requires no action. When processing is complete, the response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

8 Repeat this procedure as required for other line gateways you wish to associate to this or other GWC nodes.

9 Verify the addition of the gateway of the database by referring to procedure View gateway provisioning data for a GWC node on page 245.

10 The procedure is complete.

Changing reserved terminations - examples

You must ensure that the total number of endpoint terminations required by all of the small line media gateways associated to the same GWC node do not exceed 4094 ports. If they do, the last media gateway association activity will fail.

When a gateway profile is selected, the value specified in the Maximum Reserved Endpoints window will change to indicate the maximum number of endpoints allowed for that profile. This number can be lowered if all of the endpoints are not being used, Otherwise, do not change this number.

If you are attempting to use the maximum number of available ports on your GWC node, you must perform the following calculations:

- Calculate the total number of ports allocated used by all gateways currently associated to the GWC node, and subtract that number from 4094 (1024 for CICM). The remainder value represents the maximum number of endpoints that can be reserved for the gateway you are associating.
- When you associate the gateway, reduce the value in the Reserved Terminations: field to the value calculated previously.

When a media proxy is used

A call involves two GWCs, one controlling the originating part of the call, and the other the terminating part. Both parts may be on the same GWC, but they are separate logical entities. The gateways controlled by each GWC can be located in the carrier network (the VoIP VPN), in the public network, or in an enterprise or residential VPN.

When a call is set up, the system inserts a media proxy whenever the two gateways involved in the call are on different VPNs. The following matrix indicates when a media proxy is used.

Matrix for media proxy usage

GATEWAY LOCATION	In Carrier VPN	In Public Network	In Enterprise or Residential VPN
In Carrier VPN	No MP	MP added: 1 private and 1 public interface	MP added: 1 private and 1 public interface
In Public Network	MP added: 1 private and 1 public interface	No MP	MP added: 2 public interfaces
In Enterprise or Residential VPN	MP added: 1 private and 1 public interface	MP added: 2 public interfaces	No MP if both gateways in same VPN; Otherwise MP added: 2 public interfaces

Associate an H.323 media gateway

Purpose of this procedure

Use this procedure to associate an H.323 media gateway or gatekeeper with a selected Gateway Controller (GWC) node, with or without a network zone in the configuration. H.323 gateways provide connectivity to multiple enterprise VPNs as well as gatekeeper functionality between a Carrier VoIP network and an external network using H.323 signaling protocol.

A GWC gateway profile is a definition in the CS 2000 GWC Manager database that captures some of the characteristics and capabilities of a gateway device. A profile is selected when the gateway is configured on the GWC node. The information in the profile is then used to determine compatibility with the GWC node on which the gateway is being configured and to assess whether the node can support the added endpoint capacity.

Note: Starting in SN07, a CS 2000 H.323 gatekeeper in a carrier network is interoperable with H.323 gatekeepers in an external network. For more information, refer to Configuration details for H.323 gatekeeper functionality on page 188.

Note 3: Starting in SN08, you can change some gateway attributes defined by a profile (such as, the maximum endpoint capacity) by changing the profile for the selected gateway. For more information, refer to procedure Change gateway attributes on page 277.

When to use this procedure

Use this procedure when you wish to associate a specific H.323 type media gateway or gatekeeper with a GWC node.

Prerequisites and guidelines

Prerequisites

Network zones, including network address translator (NAT)-type, limited bandwidth links (LBL)-type, or composite NAT-LBL service zones, must be configured before any media gateways that use the service zone are associated to a GWC. (This includes enterprise-side zones.) Add a network zone to the GWC database using one of the following procedures:

- To add an IP-VPN (NAT) zone, refer to procedure Add an IP-VPN (NAT) zone on page 317.
- To add an LBL zone, refer to procedure Add a limited bandwidth link (LBL) zone on page 331.
- To add a composite NAT and LBL zone, refer to procedure Add a composite IP-VPN (NAT) and LBL zone on page 343.

Guidelines

If you attempt to associate a media gateway with a GWC that has a different service type, the request is rejected. For example, you cannot associate a line media gateway with a trunk GWC.

When you assign a media gateway name, the name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist, even if the media gateways are associated with different GWC. Duplicate media gateways will be rejected by the CS 2000 GWC Manager.

You must ensure that the total number of endpoint terminations required by all of the H.323 media gateways associated with the same GWC node does not exceed the following values:

- 1024 ports - International installations
- 1032 ports - North American installations

If you attempt to associate a media gateway with a GWC that does not have adequate available capacity, the request will be rejected. Refer to section Assigning reserved terminations on page 187 at the end of this procedure for more information about calculating available GWC node endpoint capacity.

Starting in SN07, carriers (endpoint groups) for H.323 gateways are added manually to permit greater flexibility in carrier provisioning. For

information on adding carriers to H.323 gateways, refer to procedure Add carriers to a GWC on page 201.

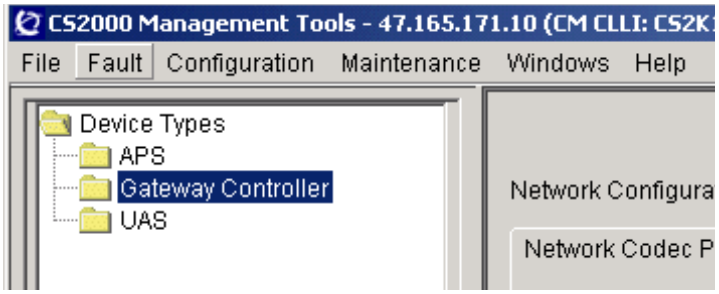
Note: If you wish to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC, click the **Statistics** button under the **Controller** tab of the **Provisioning** panel. If required, refer to procedure View characteristics of a GWC node on page 239.

After adding an H.323 gateway to the GWC database, you must also perform additional provisioning of endpoint groups in the XA-Core database. Refer to the *CS 2000 Configuration Management* NTP applicable to your solution to perform this task.

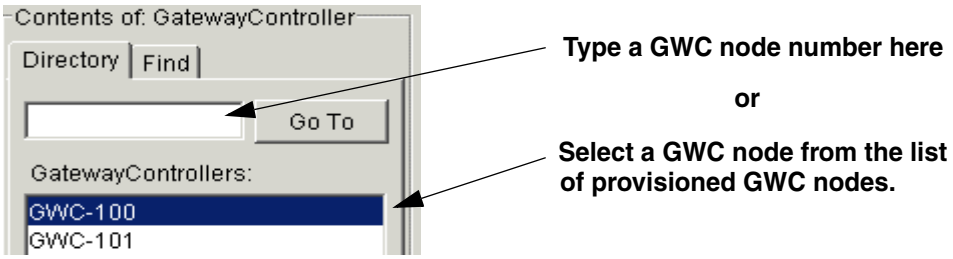
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree.



2 From the Contents of: Gateway Controller frame, select the GWC node to which you wish to associate a media gateway.

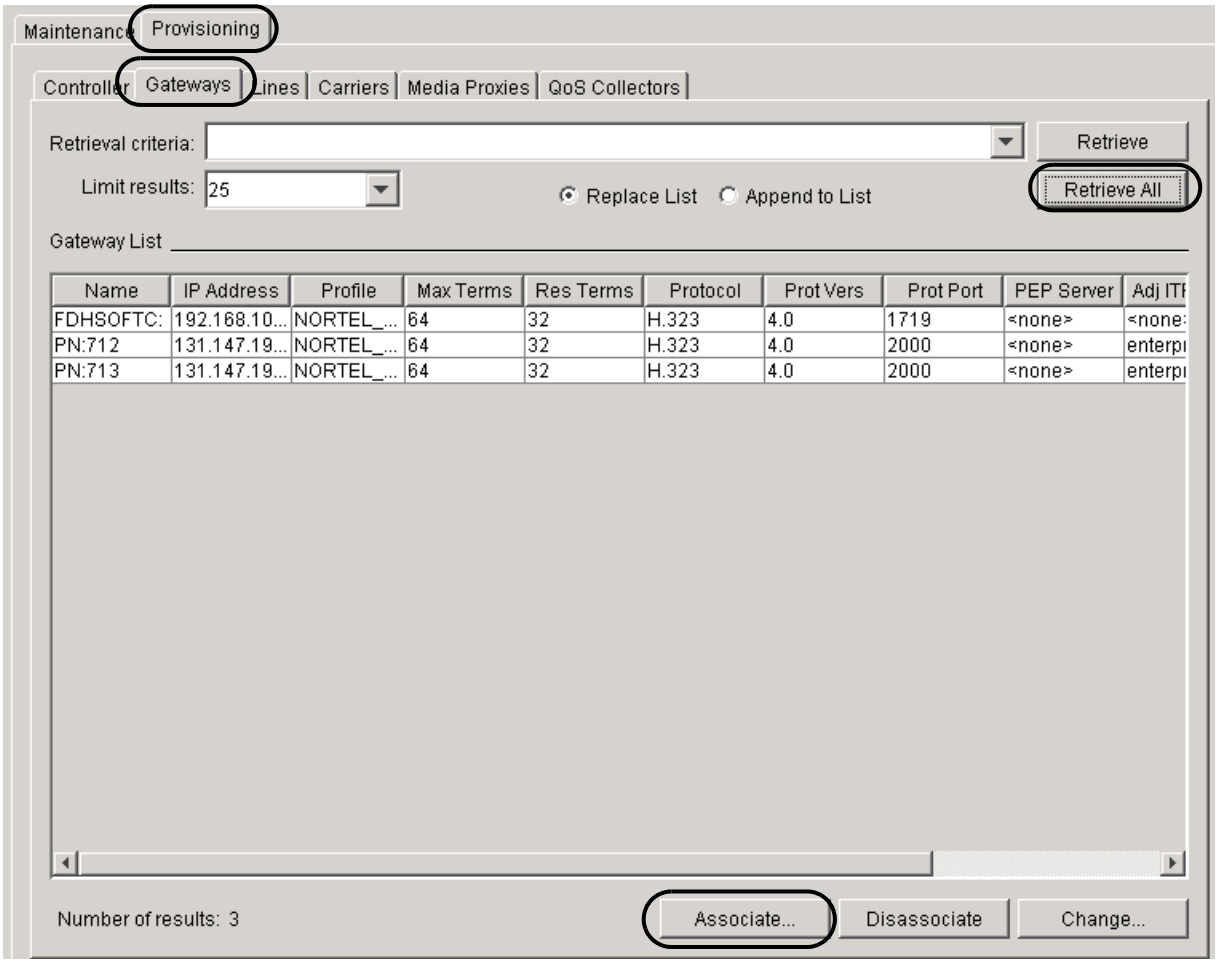


3 Click the **Provisioning** tab.

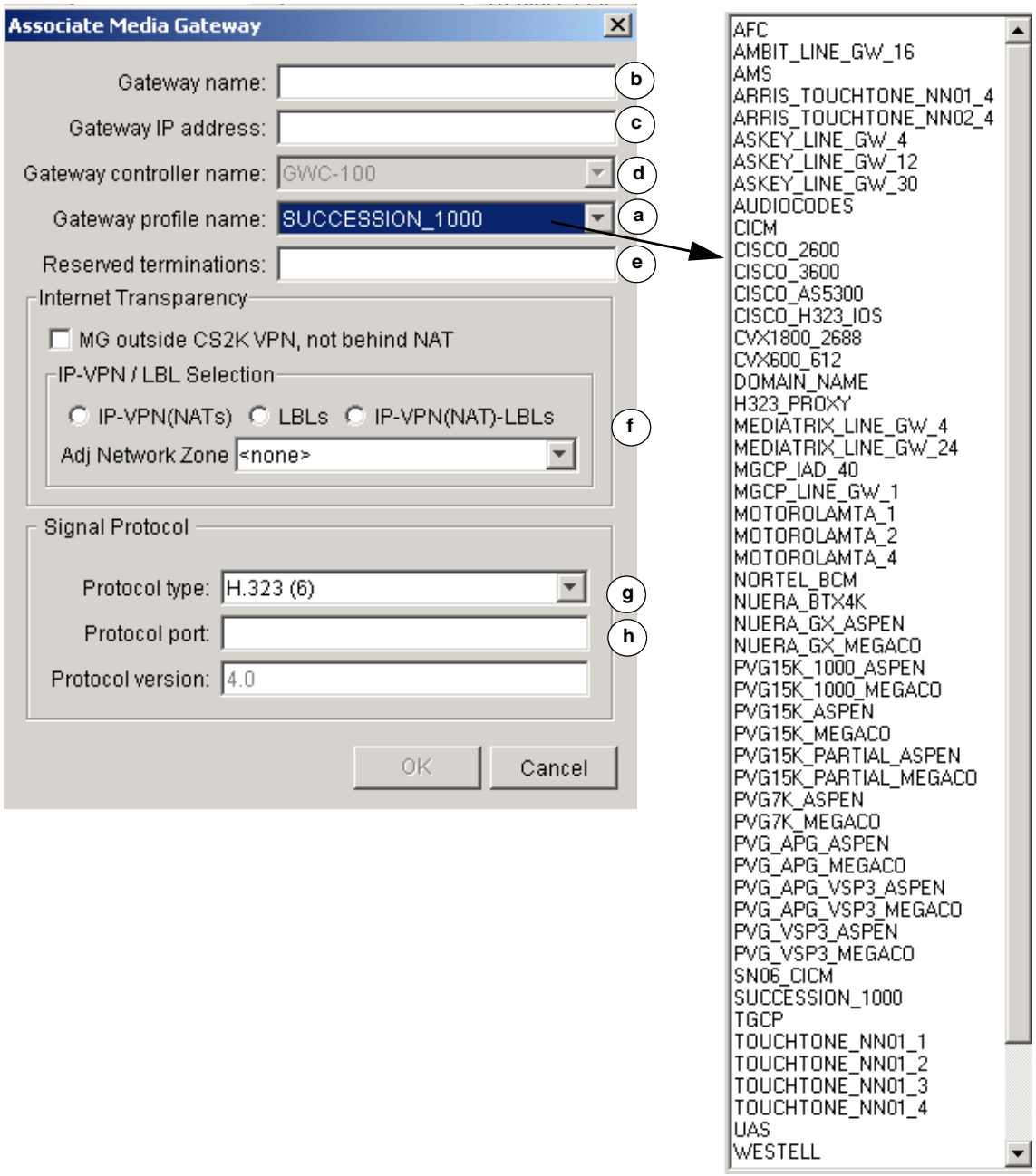
4 Click the **Gateways** tab, then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list contains all gateways added using the CS 2000 GWC Manager and the XML interface of the OSSgate application.

5 Click the **Associate** button.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately one minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click this button during a client session while data is retrieved for the Gateway site name: field. To configure DNS on the CS 2000 Management Tools server, refer to the *ATM/IP Solution-level Configuration Management* NTP, NN10409-500.



6 Use the following set of steps to datafill all of the attributes for the desired gateway.



a In the Gateway profile name: field, select the appropriate H.323 gateway profile name using the drop-down menu.

Refer to the following table for details about H.323 gateway profiles supported by this procedure. Once a profile is selected, the data associated with the profile is displayed.

Note 1: Ensure that the gateway is being added to the correct GWC node.

Note 2: Newly supported gateways may be added to the list and are not shown in this procedure. Not all gateways are supported for every solution and release.

Note 3: The gateway profile H323_PROXY is used only for CS 2000 H.323 gatekeeper scenarios. For details, refer to section Configuration details for H.323 gatekeeper functionality on page 188.

H.323 media gateway profiles (Sheet 1 of 2)

Gateway profile name (see Note 1)	Gateway category	Signaling protocol	Protocol version	Protocol port (see Note 2)	Service type	Maximum port/ endpoint capacity (see Note 3)
CISCO_2600	large	H.323	4.0	0	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_3600	large	H.323	4.0	0	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_AS5300	large	H.323	4.0	0	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_H323_IOS	large	H.323	4.0	0	H.323, ITRANS	1032 (NA) 1024 (Intl)
H323_PROXY	large	H.323	4.0	0	H.323, ITRANS	1032 (NA) 1024 (Intl)
NORTEL_BCM	large	H.323	4.0	1719	H.323, ITRANS	1032 (Intl) 1024 (Intl)
SUCCESSION_1000	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl)

H.323 media gateway profiles (Sheet 2 of 2)

Gateway profile name (see Note 1)	Gateway category	Signaling protocol	Protocol version	Protocol port (see Note 2)	Service type	Maximum port/ endpoint capacity (see Note 3)
WESTELL	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl)

Note 1: Contact your Nortel Networks account prime for details on the specific gateways supported for each profile.

Note 2: When associating an H.323 gateway with a GWC, the protocol port must be set as follows:

- Use a value of **0** for auto-discovery. This option enables the system to discover the protocol port when the gateway registers. Use this value for all CISCO profiles and for H.323_PROXY.

  or

- Use the specific port value of the static bind that has been configured on the NAT for the H.323 gateway. Do not use the port value of 1719.

  or

- Use a value of 1720 to enable an operation mode in which no registration, admission, and status (RAS) messages are exchanged between a gateway and a GWC (RAS-less mode). This functionality applies only to H.323 gateways without NAT or with a NAT configuration of 1:1, in Carrier Hosted Services (CHS) solutions only. A 1:1 (one to one) NAT configuration means that a NAT is configured to translate an IP address only and each gateway uses one and only one IP address.

Note 3: For H.323 gateways, the endpoint capacity indicated is a recommended value based on the GWC capacity. The actual endpoint capacity supported depends on the details of your specific installation. For all profiles listed above, refer to the corresponding product documentation to determine the recommended endpoint maximum supported on a specific gateway.

b In the Gateway name: field, type a text string that consists of up to 32 alpha-numeric characters; for example, custH323Gateway.

Note: The media gateway name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist even if the media gateways are associated with different GWCs.

c In the Gateway IP address: field, type the IP address of the gateway. Use the following format:
<0-255>.<0-255>.<0-255>.<0-255>

Note 1: If the gateway is behind a NAT-type network zone, specify the IP address on the CS 2000 side of the NAT device.

Note 2: The H.323 gateways can share the same IP address. For CS 2000 H.323 gatekeeper to H.323 gatekeeper configuration using the H323_PROXY gateway profile, the IP address is shared and both

gateways are configured with Protocol port 0. (Refer to step h in this procedure.)

d If necessary, in the Gateway controller name: field, select a GWC node with which the gateway is being associated.

Note: If a GWC is not specified, the node provisioning application will automatically discover a GWC node with which to associate this gateway. The choice of GWC node is based on the service type of the media gateway (line, H.323, trunk, or audio) and the endpoint capacity of the media gateway.

e In the Reserved terminations: field, enter a value for the reserved terminations, up to the maximum indicated in the specific gateway manufacturer's documentation.

Note 1: A value must be entered in this field for H.323 gateways.

Note 2: If you are configuring a GWC node as a CS 2000 H.323 gatekeeper, refer to section Configuration details for H.323 gatekeeper functionality on page 188 for details on how to configure reserved terminations for the following gateways:

- a carrier gateway
- an external gateway

Table Configuration required for H.323 gatekeeper functionality on page 189 contains configuring details for GWC H.323 gatekeeper scenarios.

The following guidelines apply to H.323 gateways:

- The range of valid reserved terminations for an H.323 gateway is (inclusive):
  - in North American market: 4 to 1032
  - in International market: 4 to 1024
- The value entered in the Reserved terminations: field must be equal to, or greater than, the total sum of values entered in the Number of ports: field of the Add Carrier dialog box for all carriers assigned to the gateway. Refer to procedure Add carriers to a GWC on page 201.
- Refer to H.323 media gateway profiles on page 180 for endpoint capacities of supported H.323 gateways. For H.323 gateways, the endpoint capacity indicated is a recommended value. The endpoint capacity supported depends on your specific installation

f In the Internet Transparency section of the dialog box, complete *one* of the following tasks based on the conditions indicated below.

Note 1: If you are configuring a GWC node as a CS 2000 H.323 gatekeeper, refer to section Configuration details for H.323 gatekeeper functionality on page 188. The table Configuration required for H.323 gatekeeper functionality on page 189 contains configuration details for GWC H.323 gatekeeper scenarios.

Note 2: Refer to section When a media proxy is used on page 191 for information on when a media proxy is inserted depending on the location of the gateways involved in a call.

- If the gateway is
  - — outside the CS 2000 carrier network
  - — outside the enterprise VPN
  - — not behind a network zone [IP-VPN (NAT), LBL, or composite NAT-LBL],

  select the checkbox “MG outside CS2K VPN, not behind a NAT” and do not assign a zone.

  The gateway is in the public network. In this case, the gateway network zone name is set to a value of “outside the telecom service provider domain”. The Adj ITRANS MB column in the Gateway List appears as “outtsp” for any gateways in this category.

  Note: In this scenario, the suggested port configuration values for the gateway are:
  - — for the registration, admission and status (RAS) port: 1719
  - — for the call signaling (CS) port: 1720

- If the gateway is
  - — outside the CS 2000 carrier network
  - — inside an enterprise VPN
  - — behind a network zone [IP-VPN (NAT), LBL, or composite NAT-LBL],

  do not select the checkbox “MG outside CS2K VPN, not behind a NAT”.

Instead, select the name of an adjacent network zone in the Adj Network Zone text field. Perform the following steps:

— Select the radio button for IP-VPN(NATs), LBLs, or IP-VPN(NAT)-LBLs to restrict your search.

— Click in the Adj Network Zone field.

— If desired, type text characters of a zone name in the field to fine tune your display. The system displays all zones with a name that matches the characters you typed.

— Select adjacent network zone for the gateway from the list in the drop-down menu.

Note: You can only select network zone names that are datafilled and appear in the Network Zones view in the CS 2000 GWC Manager. Refer to procedure Review available network devices on page 99.

The gateway is in the enterprise or residential VPN. In this case, the gateway network zone name is set to the NAT-type, LBL-type, or composite NAT-LBL zone name. The Adj ITRANS MB column in the Gateway List appears as <zone name> for any gateways in this category.

- If the gateway is

  — inside the CS 2000 carrier network

  do not select the checkbox “MG outside CS2K VPN, not behind a NAT” and do not assign a network zone.

  The gateway is in the carrier VPN. In this case, the gateway network zone name is omitted (not used). The Adj ITRANS MB column in the Gateway List appears as “<none>”.

  Note: In this scenario, the suggested port configuration values for the gateway are:

  — for the registration, admission and status (RAS) port: 1719

  — for the call signaling (CS) port: 1720

g In the Protocol type: field, select the appropriate gateway protocol type using the drop-down menu.

Note: The system restricts the protocol type options to those compatible with the gateway profile name selected previously.

h

ATTENTION

All gateways that use the following gateway profiles must be configured with signaling protocol port 0:

- H323_PROXY
- CISCO_2600
- CISCO_3600
- CISCO_AS5300
- CISCO_H323_IOS

A protocol port value of 0 enables the system to discover the protocol port when the gateway registers.

For more information on gatekeeper configuration, refer to table Configuration required for H.323 gatekeeper functionality on page 189

In the Protocol port: field, type the protocol port to be used by the gateway.

This field identifies the port number for the gateway's RAS protocol channel corresponding to the static bind at the enterprise NAT.

Note 1: Starting in release SN07, there is no default value for this field. You must type a value.

Note 2: If you enter a value of 1720, the GWC treats this gateway as operating in RAS-less mode (no RAS messages exchanged between the gateway and the GWC).

Assign a value in this field based on the following guidelines:

- Type a value of **0** for auto-discovery. This value enables the system to discover the protocol port when the gateway registers.

  or

- Type the specific port value of the static bind that has been configured on the NAT for the H.323 gateway. Do not use the port value of 1719.

  or

- Type the port value of 1719 for H.323 gateways that are set to the Adj ITRANS MB setting of "<none>".

  or

- Type a value of 1720 to enable an operation mode in which no registration, admission, and status (RAS) messages are exchanged between a gateway and a GWC.

  Note: This functionality applies only to H.323 gateways without NAT or with a NAT configuration of 1:1, in Carrier Hosted Services (CHS) solutions only.

The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name selected previously.

7 Click the **OK** button to apply the input.

A response dialog box appears indicating that the system is processing the requested change. It can take up to 5 minutes for the change to be processed. During this time a “Timed Out” window may appear. This requires no action. When processing is complete, the response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

8 Repeat this procedure as required for other H.323 gateways you wish to associate with this or other GWC nodes.

9 Verify the addition of the gateway to the database by referring to procedure View gateway provisioning data for a GWC node on page 245.

10 The procedure is complete.

Assigning reserved terminations

You must ensure that the total number of endpoint terminations required by all of the H.323 media gateways associated with the same GWC node does not exceed the following values:

- 1032 ports - North American market
- 1024 ports - International market

Any media gateway associations that exceed these limits will fail.

You must enter a value in the Reserved terminations: field when associating an H.323 media gateway with a GWC. The endpoint capacity indicated in H.323 media gateway profiles on page 180 is a recommended value. The endpoint capacity supported depends on your specific installation.

If you are attempting to use the maximum number of available ports on your GWC node, you must perform the following calculations:

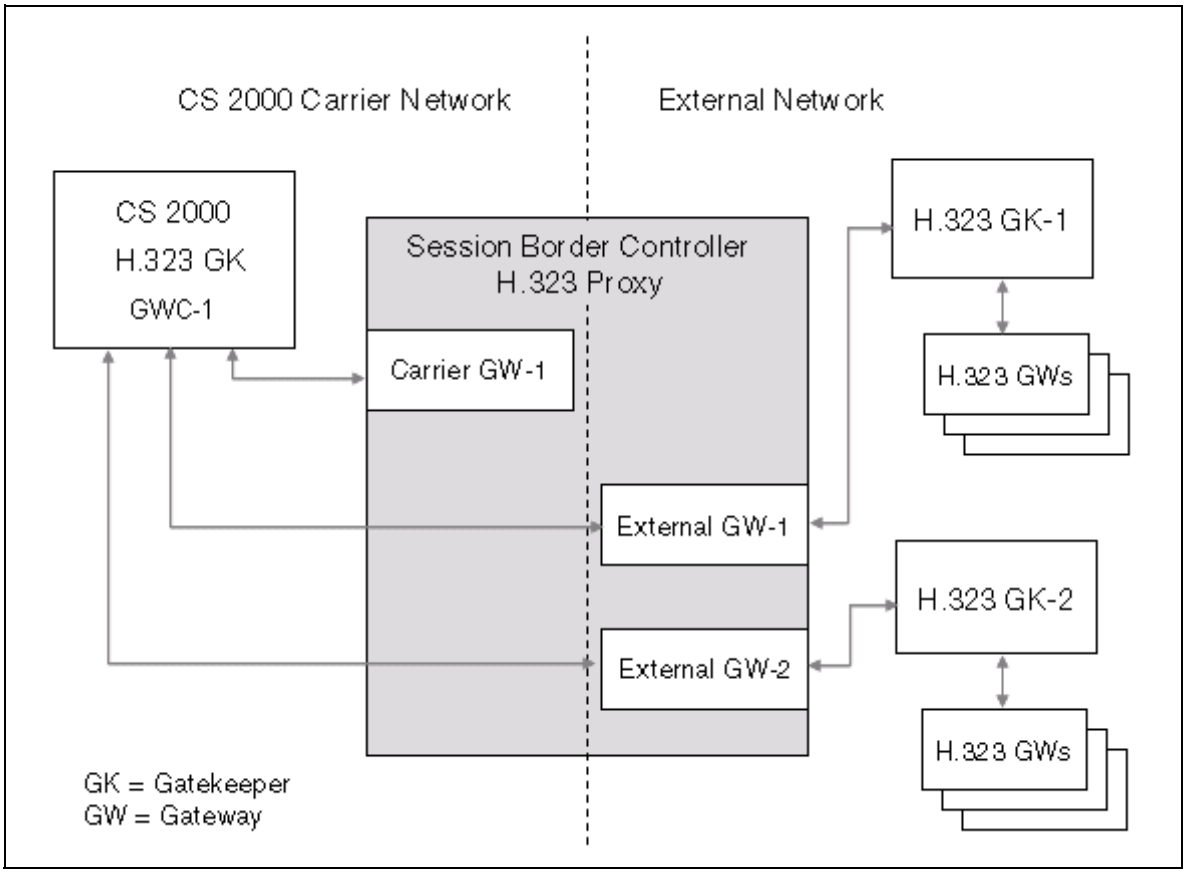
1. Calculate the total number of ports used by all H.323 gateways currently associated with the GWC node. Then, subtract that number from 1032 (NA) or 1024 (Intl). The remainder represents the maximum number of endpoints that can be allocated to an additional gateway.
2. When you associate an additional gateway with the GWC node, provision the Reserved Terminations: field with the maximum number of endpoints calculated in the previous step.

Note: If you wish to assign the full capacity of a GWC to a single H.323 gateway, create only two H.323 carriers for the gateway.

Configuration details for H.323 gatekeeper functionality

Starting in SN07, a CS 2000 H.323 gatekeeper in a carrier network is interoperable with H.323 gatekeepers in an external (private, enterprise, or another carrier) network. A third party session border controller device acts as an H.323 signaling proxy between the two networks by registering virtual gateways in each network.

The following figure illustrates one example of H.323 gatekeeper functionality between a CS 2000 carrier network and an external network.



In this example

- Three virtual gateways reside within the session border controller, each representing a protocol stack on the device.
- Carrier GW-1 is associated with GWC -1 to provide an interface for H.323 maintenance and call signaling messages between external

gateways and the GWC. The carrier gateway does not originate or terminate any calls and therefore requires no bearer channels.

- External GW-1 and External GW-2 are each associated with an external gatekeeper, as well as with GWC-1. Each external gateway represents an external gatekeeper to the CS 2000. For example, External GW-1 proxies all calls from gateways associated with H.323 GK-1 and the CS 2000.

In the above scenario, the available endpoints (reserved terminations) on GWC-1 could be provisioned as described in the following table.

Example of GWC endpoint distribution in H.323 gatekeeper scenario

	Endpoint provisioning	
Gateway	**North America market**	**International market**
Carrier GW-1	4 (minimum)	4 (minimum)
External GW-1	514	510
External GW-2	514	510
Total on GWC-1	1032 (capacity)	1024 (capacity)

Starting in SN07, the CS 2000 GWC Manager supports the following gateway profile for H.323 gatekeeper functionality: H323_PROXY.

The Carrier GW-1 and the two External GWs must be configured with H323_PROXY to permit the gatekeeper scenario using the CS 2000. For details on the values required to support H.323 gatekeeper functionality, refer to the following table.

Configuration required for H.323 gatekeeper functionality (Sheet 1 of 2)

	Associate Media Gateway dialog	
Field	**Carrier gateway**	**External gateway**
Gateway name	Name of carrier gateway Example: Carrier GW-1	Name of external gateway Example: External GW-1
Gateway IP address	IP address of carrier gateway	IP address of external gateway
Gateway profile name	H323_PROXY	H323_PROXY

Configuration required for H.323 gatekeeper functionality (Continued) (Sheet 2

Associate Media Gateway dialog		
Field	**Carrier gateway**	**External gateway**
Reserved terminations	4 - See Note 1	Assign a value based on network requirements - See Note 2
Internet transparency (Adj Network Zone)	No NAT required	Add a NAT for the external network - where the gatekeeper resides
Protocol type	H.323	H.323
Protocol port	0 - See Note 3	0 - See Note 3
Protocol version	4.0	4.0

Note 1: Since the carrier gateway is used only for signaling between the CS 2000 GWC gatekeeper and the external gateways, provision the minimum reserved terminations (4) on this gateway.

Note 2: Refer to section Assigning reserved terminations on page 187.

Note 3: You must configure all gateways using the profile H323_PROXY with signaling *Protocol port 0*. This value enables the system to discover the protocol port when the gateway registers.

When a media proxy is used

A call involves two GWCs, one controlling the originating part of the call, and the other the terminating part. Both parts may be on the same GWC, but they are separate logical entities. The gateways controlled by each GWC can be located in the carrier network (the VoIP VPN), in the public network, or in an enterprise or residential VPN.

When a call is set up, the system inserts a media proxy whenever the two gateways involved in the call are on different VPNs. The following matrix indicates when a media proxy is used.

Matrix for media proxy usage

GATEWAY LOCATION	In Carrier VPN	In Public Network	In Enterprise or Residential VPN
In Carrier VPN	No MP	MP added: 1 private and 1 public interface	MP added: 1 private and 1 public interface
In Public Network	MP added: 1 private and 1 public interface	No MP	MP added: 2 public interfaces
In Enterprise or Residential VPN	MP added: 1 private and 1 public interface	MP added: 2 public interfaces	No MP if both gateways in same VPN; Otherwise MP added: 2 public interfaces

Associate an audio server media gateway

Purpose of this procedure

This procedure describes how to associate an audio server gateways (including any Media Server 2000 Series gateways) with the selected Gateway Controller (GWC) node, using the UAS or AMS media gateway profile.

A gateway profile is a definition in the CS 2000 Management Tools database (CS 2000 GWC Manager database) that captures some of the characteristics and capabilities of a gateway device. A profile is chosen when the gateway is being configured. The information in the profile is then used to determine compatibility with the GWC node on which the gateway is being configured and to assess whether the node can support the added endpoint capacity.

Note: Starting in SN08, you can change some gateway attributes defined by a profile (such as, the maximum endpoint capacity) by changing the profile for the selected gateway. For more information, refer to procedure Change gateway attributes on page 277.

Media Server 2010 gateways supply the Packet Media Anchor functionality, which replaces the APG device. Use the AMS gateway profile to associate a Media Server 2010 gateway configured with the Packet Media Anchor functionality.

Note 1: For an overview of the Packet Media Anchor functionality, refer to the *Gateway Controller Basics* NTP, NN10189-111.

Note 2: For instructions on how to enable the Packet Media Anchor functionality on a GWC node, refer to procedure Configure the Packet Media Anchor functionality on an audio controller GWC node on page 16 in this NTP.

For an overall Packet Media Anchor configuration procedure, refer to the solution-level *Configuration Management* NTP applicable to your solution.

When to use this procedure

Use this procedure when you wish to associate an audio server (including any Media Server 2000 Series) media gateway with a GWC node.

Prerequisites and guidelines

ATTENTION

Do not associate UAS-based and AMS-based gateways with the same GWC node.

The following additional prerequisites and guidelines apply to this procedure:

- For the Packet Media Anchor functionality,
  - Use the AMS (audiocodes media server) gateway profile to associate a Media Server 2010 gateway configured with the Packet Media Anchor functionality.
  - If the Media Server 2010 gateway that you want to use for this functionality has the UAS profile currently assigned to it, you must complete the following steps:
    - Disassociate the gateway from the GWC using procedure Disassociate a media gateway on page 305.
    - Complete this procedure to re-associate the gateway using the AMS profile.
  - You must first configure table SERVSINV to specify the maximum number of simulations calls to support.
  - On the Media Server 2010 gateway, configure three BCT and one audio resource for each anchored call.

    Note: For more information, refer to the solution-level *Configuration Management* NTP applicable to your solution.

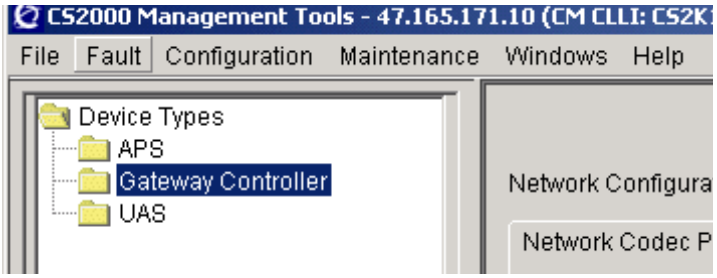
- The assigned media gateway name must be unique within the CS 2000 domain. Duplicate media gateway names cannot exist, even if the media gateways are associated with different GWCs. The CS 2000 GWC Manager will reject duplicate media gateways.
- An attempt to associate a media gateway with a GWC that has a different service type will be rejected.

Note: If you wish to verify the total number of endpoints currently reserved for the gateways associated with the selected GWC, click the **Statistics** button under the **Controller** tab of the **Provisioning** panel. If required, refer to procedure View characteristics of a GWC node on page 239.

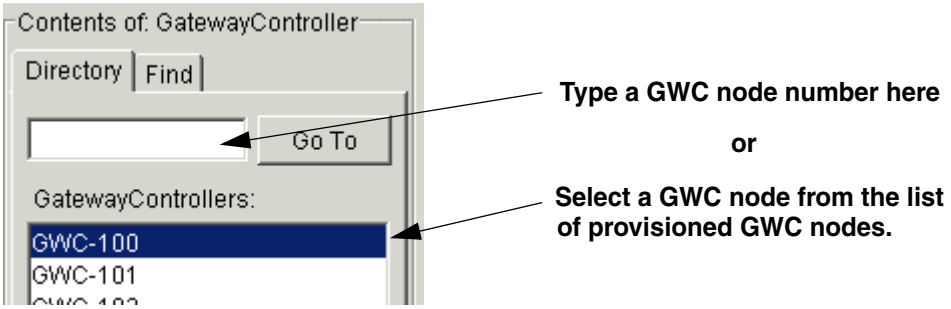
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate a media gateway.

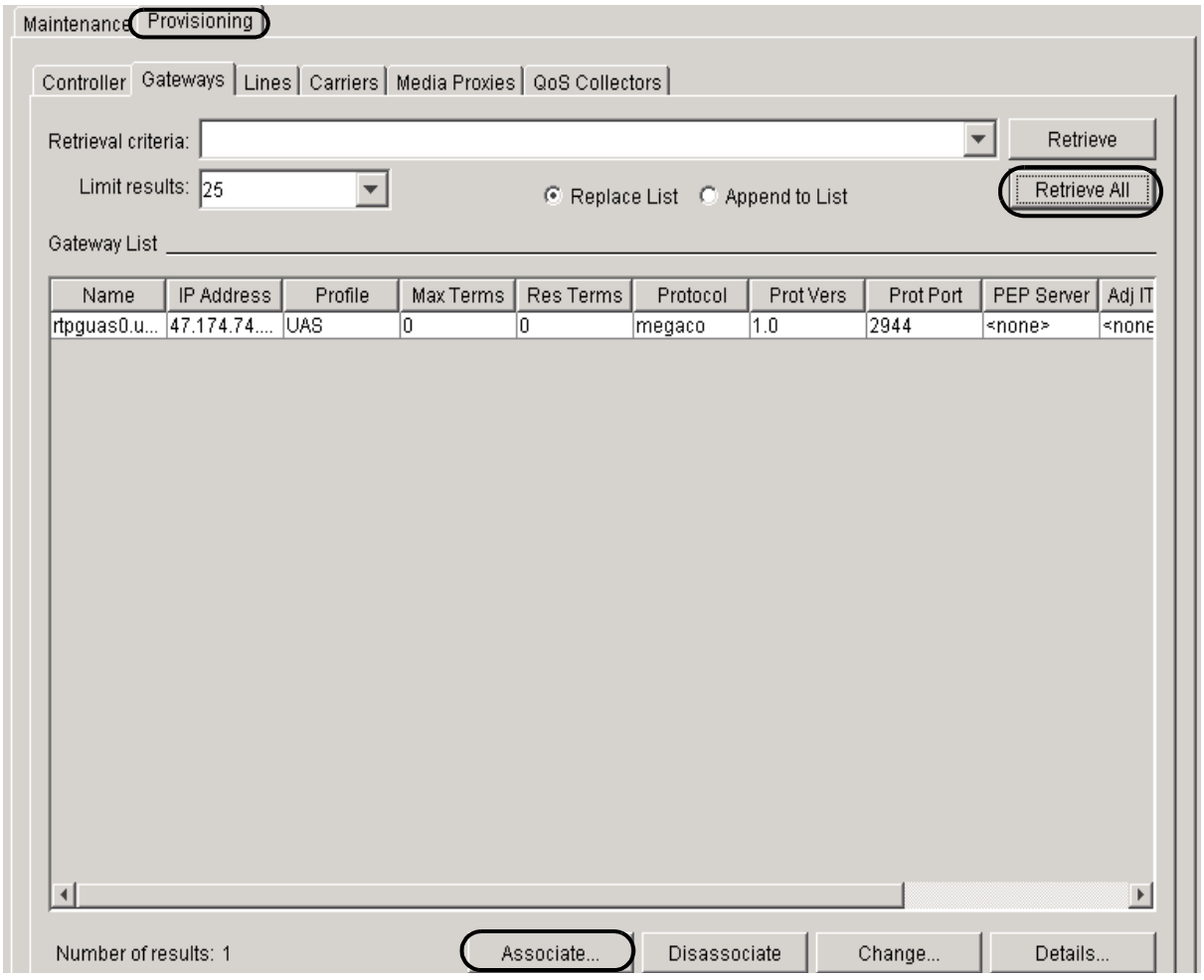


3 Click the **Provisioning** tab.

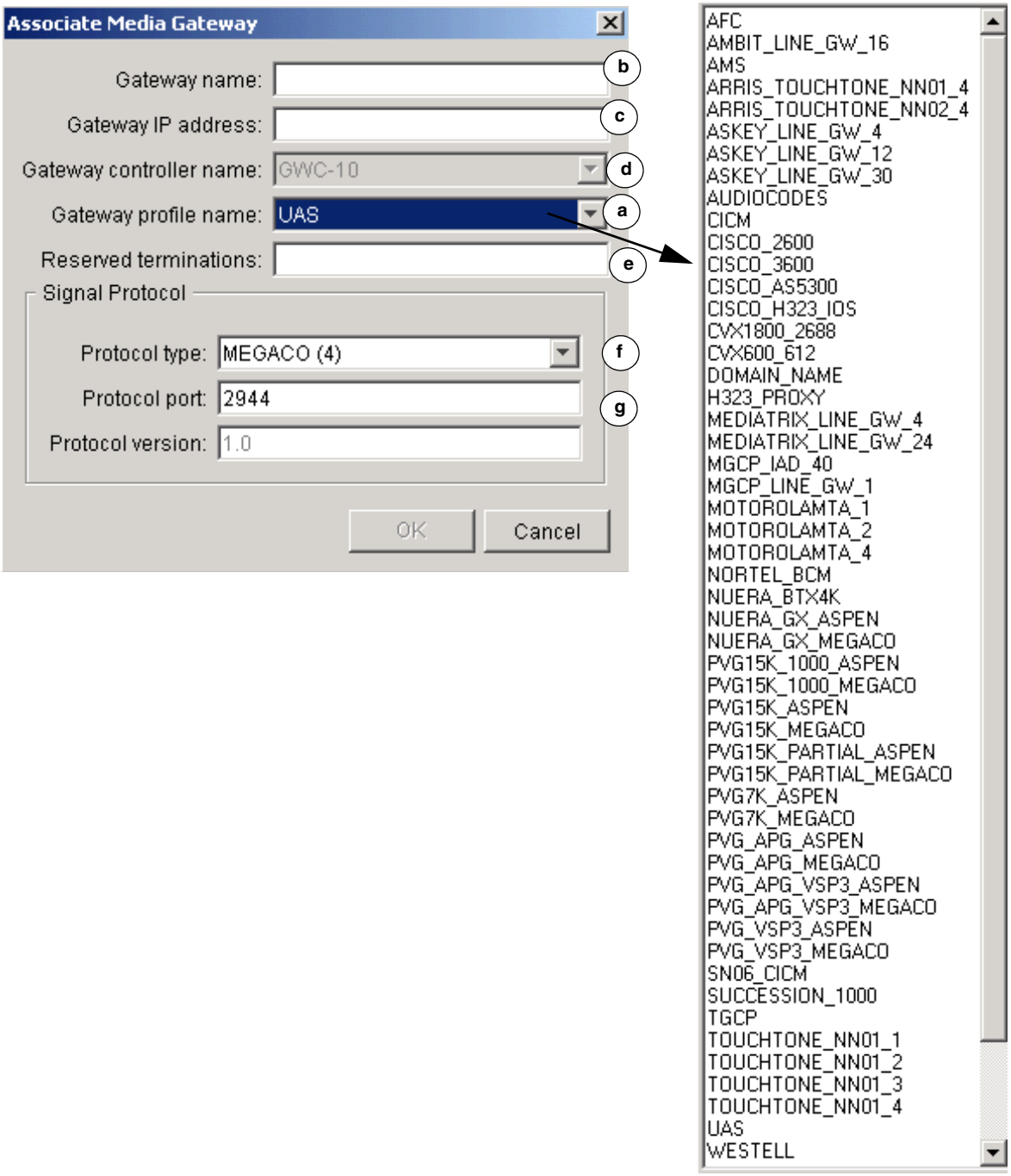
4 Click the **Gateways** tab, then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list contains all gateways added using the CS 2000 GWC Manager and the XML interface of the OSSgate application.

5 Click the **Associate** button.

Note: If Domain Name Service (DNS) is not activated on the CS 2000 Management Tools server, or if it is not working properly, you will experience a delay of approximately one minute before the Associate Media Gateway dialog box is fully displayed. The delay occurs the first time you click this button during a client session while data is retrieved for the Gateway site name: field. To configure DNS on the CS 2000 Management Tools server, refer to the *ATM/IP Solution-level Configuration Management* NTP, NN10409-500.



6 Use the following set of steps to datafill all of the attributes for the audio server gateways.



a In the Gateway profile name: field, select the appropriate audio server profile name using the drop-down menu.

Refer to the following table for details about audio server profiles supported by this procedure. Once a profile is selected, the data associated with the profile is displayed.

Note 1: Ensure that the gateway is being added to the correct GWC node.

Note 2: Newly supported gateways may be added to the list and are not shown in this procedure. Not all gateways are supported for every solution and release.

Audio server media gateway profiles

Gateway profile name	Gateway category	Signaling protocol	Protocol version	Default protocol port	Service type	Maximum port/ endpoint capacity
UAS	audio	MEGACO	1.0	2944	Audio	n/a
AMS	audio	MEGACO	1.0	2944	Audio	120

Note 1: These profiles support Media Server 2000 Series audio servers.

Note 2: Use the AMS profile to associate a Media Server 2010 gateway configured with the Packet Media Anchor functionality.

b In the Gateway name: field, enter a gateway name according to the gateway profile. Use the suggested gateway naming conventions shown in the following table.

Note: The media gateway name must be unique within the CS 2000. Duplicate media gateway names cannot exist even if the media gateways are associated with different Gateway Controllers.

Audio server media gateway naming conventions

Audio gateway profile	Suggested gateway naming conventions
UAS AMS	Use a domain name of the media gateway in the form of an absolute domain name including the hostname of the device, suitable for lookup using Directory Name Service (DNS). The name must contain a "." and be no longer than 32 characters. Example: uas1.ral5.vendor.net

Note: This naming convention supports Media Server 2000 Series audio servers.

c In the Gateway IP address: field, enter the IP address of the gateway. Use the following format:
<0-255>.<0-255>.<0-255>.<0-255>

d If necessary, in the Gateway controller name: field, use the drop-down menu to select a GWC node with which the gateway is being associated.

If a GWC is not specified, the node provisioning application will automatically discover a GWC node with which to associate this gateway. The choice of GWC node is based on the service type of the media gateway (line, H.323, trunk, or audio) and the endpoint capacity of the gateway.

e In the Reserved terminations: field, type a value of 0 for audio servers.

Note: If you do not assign a value in this field, the system will use the default, which is the maximum number of reserved terminations for the gateway selected.

f In the Protocol type: field, use the default value provided (MEGACO).

Note: The system restricts the protocol type options to those compatible with the gateway profile name selected previously.

g In the Protocol port: field, use the default value provided. Do not change this value.

Note: The Protocol version: field displays the version of the protocol that is applicable to the gateway profile name and protocol type select previously.

7 Click the **OK** button to apply the input.

A response dialog box appears indicating that the system is processing the requested change. It can take up to 5 minutes for the change to be processed. During this time a “Timed Out” window may appear. This requires no action. When processing is complete, the response dialog indicates whether the gateway association succeeded or failed. If the association failed, the response dialog indicates the reason why it failed.

8 Repeat this procedure as required for other audio server gateways you wish to associate with this or other GWC nodes.

9 The procedure is complete.

Add carriers to a GWC

Purpose of this procedure

Use this procedure to add carriers (endpoint groups) and their endpoints to a gateway associated with a GWC node.

Carrier endpoints are usually provisioned in groups representing E1 and DS1 levels allowing access to all timeslots for service provisioning. Services supported include ISUP trunking, and PRI trunking.

The section Carrier and endpoint naming on page 209 contains a table of carrier formats to be used for different media gateway profiles.

Note: The APG functionality has been removed in the SN07 release. All GWC service profiles and gateway profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, PVG_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. It is recommended that the existing DPT GWCs that still use these profiles migrate to SIP-T or SIP_TINTL profile to optimize resource utilization (resources previously reserved for APG will be released for other tasks).

Line carriers

Line endpoints are added automatically when you provision lines to a GWC. For instructions on how to provision lines, refer to procedures in the *CS 2000 Configuration Management* NTP for your solution.

In a Carrier VoIP environment, the allocation of line equipment numbers (LEN) for new lines is done by the system. This is because the LEN is no longer directly associated with physical hardware and its location as it was in legacy networks. In Carrier VoIP networks, LENs act as an internal map to a gateway endpoint pair. Use of LEN has been replaced with the implementation of the gateway endpoint to designate actual termination points in the network. This mapping is done by the system and is not intended to be determined manually at provisioning time. Since the data needs to reside in multiple locations and retain synchronization in the network, the line provisioning system acts as a single point of entry for this data to ensure it is named and assigned consistently across all network elements.

H.323 carriers

Starting in release SN07, to permit greater flexibility in carrier provisioning, H.323 carriers are added manually using this procedure. The existing auto-generated carrier names from release SN06.2 appear in SN08. Any new H.323 carriers assigned in SN08 are added manually based on the naming convention for H.323 carriers.

Also, new features have been added to enhance H.323 support in Carrier VoIP networks. For examples of how to take advantage of the added flexibility and new features, refer to H.323 carrier provisioning on page 225.

After an H.323 gateway is added to the CS 2000 GWC Manager database, additional provisioning of terminal identifiers (TID) that are mapped to endpoints must be manually added to the XA-Core. Refer to the *CS 2000 Configuration Management* NTP applicable to your solution to perform this task.

When to use this procedure

Use this procedure after you have associated specific media gateways with a GWC node.

Prerequisites and guidelines

You must first associate a media gateway with a GWC node before you can add carriers (endpoint groups) to the gateway.

You need to be familiar with the names of the media gateways associated with the GWC node. If necessary, refer to procedure View gateway provisioning data for a GWC node on page 245.

You may plan your approach to carrier naming prior to starting this procedure. Refer to Carrier and endpoint names on page 209 to determine the naming convention for your gateway profile type.

Note: Do not add V5.2 carriers using this procedure. Refer to the procedure Add V5.2 interfaces on page 445 in this NTP.

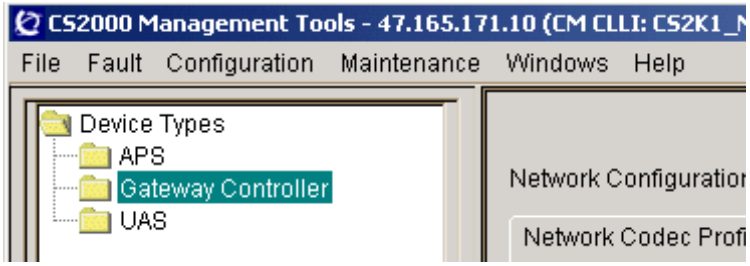
After you have completed this procedure, refer to the *CS 2000 Configuration Management* NTP for your solution to specify the trunks to provision by adding tuple datafill to table TRKMEM.

CAUTION
Possible partial service disruption
If you are adding carrier endpoints after having previously removed them from the same gateway, you will have terminal identifier (TID) mismatches. Contact your next level of support for instructions on how to avoid TID mismatches.

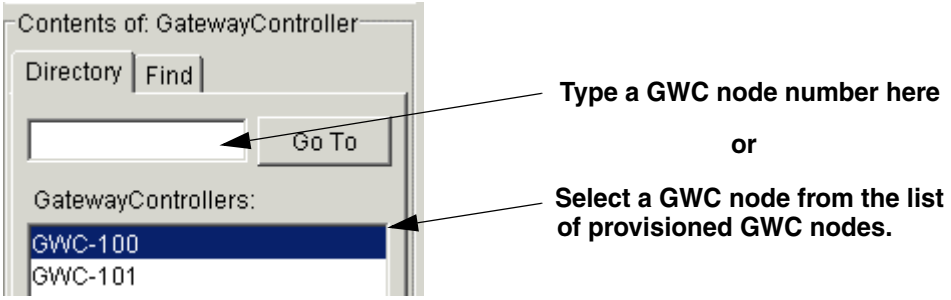
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

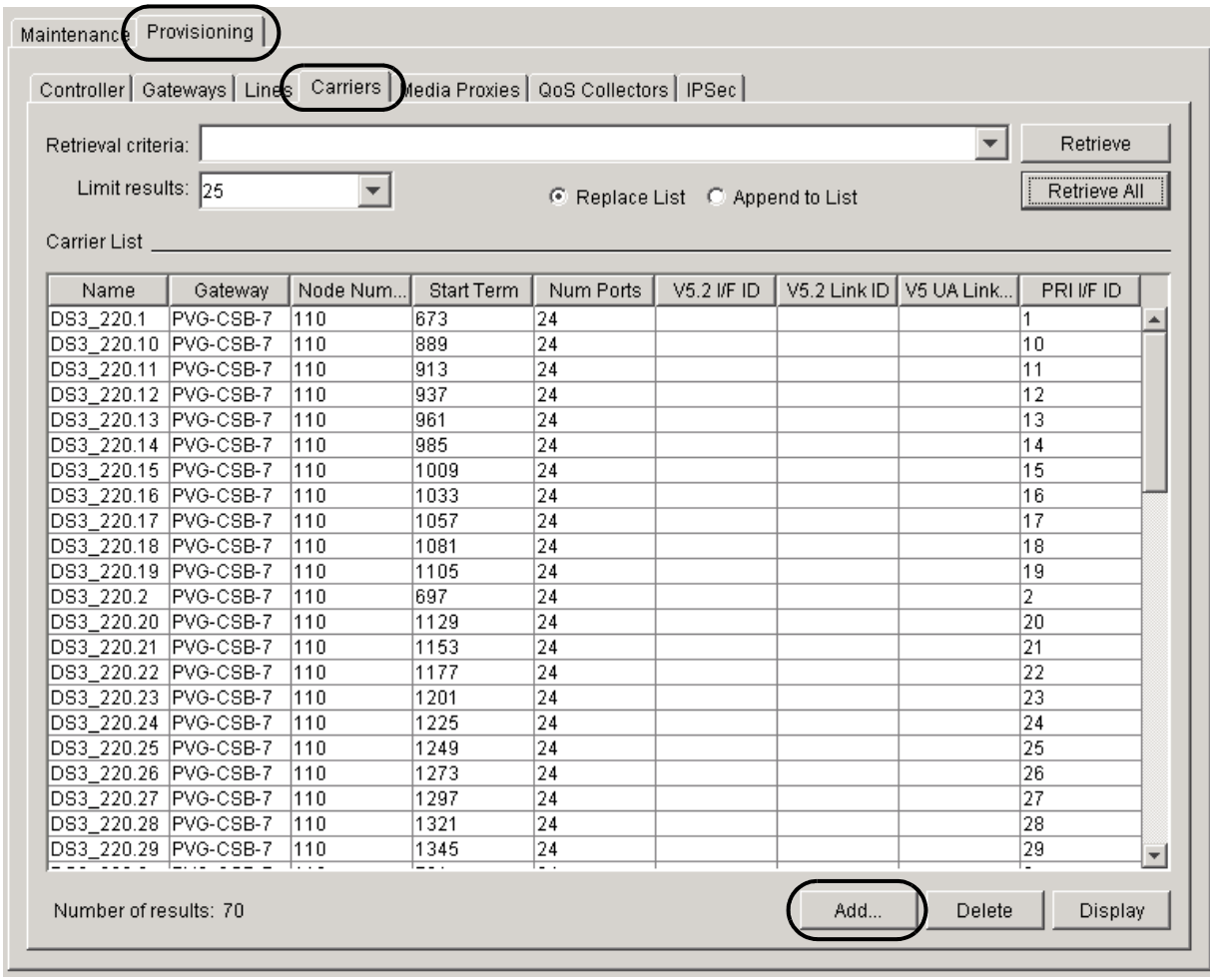


2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.

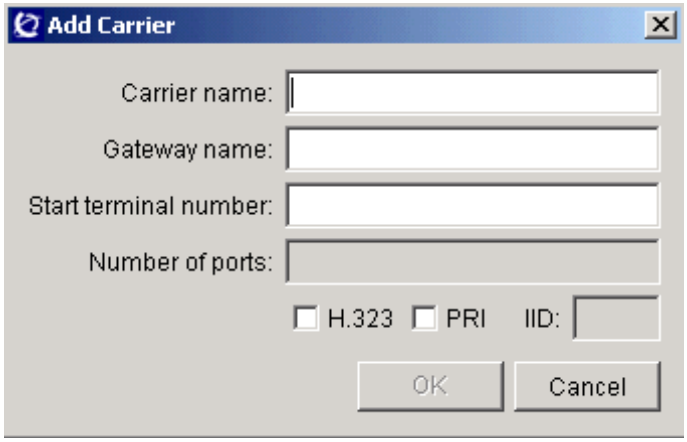


3 Click the **Provisioning** tab.

4 Click the **Carriers** tab.



5 Click the **Add** button at the bottom of the screen to display the Add Carrier dialog box.



a In the Carrier name: field, type the name (an alphanumeric character string) of the carrier that you want to add.

Note: Determine whether your system uses strict naming conventions for assigning some types of gateway endpoints.

The carrier name is based on the media gateway type (the gateway profile name). Refer to the Carrier and endpoint names on page 209 for naming conventions applicable to specific media gateways.

b In the Gateway name: field, type the name (an alphanumeric character string) of the gateway to which you are adding carriers.

Note: The name of the gateway is selected when associating a media gateway with a GWC node.

c If desired, in the Start terminal number: field, type a number representing the starting point of a contiguous block of endpoints or terminal identifiers (TID).

Note: This field is optional. If you do not type a number in this field, the system will automatically define which TIDs are used and how they map to the carrier.

For any gateway other than an H.323 gateway, the contiguous block of endpoints will be either 24 (North American market) or 32 (International market). Note that 31 endpoints will be added for International PRI. The system automatically identifies the number of endpoints included in the block based on the configuration of the CS 2000 Management Tools server.

For gateways supporting H.323, the number of endpoints in the contiguous block is defined by the value in the Number of ports: field (see step f below). If no value is entered in the Number of ports: field, then the default of 24 (NA market) or 32 (International market) endpoint will be used.

Note: Ensure that a contiguous range of endpoints are available on your gateway to fulfill your requirements when you perform the following tasks:

- assign a value in the Start terminal number: field
- change the size of your carrier block

d Determine your next step using the following table.

If you are adding carriers to	Do
an H.323 gateway	go to step e
a non-H.323 gateway and PRI trunks *are* provisioned in the carrier group	go to step h
a non-H.323 gateway and PRI trunks *are not* provisioned in the carrier group	go to step i

e If you are adding carriers to an H.323 gateway, select the H.323 check box.

The Number of ports: field is activated.

Note: You must select the H.323 check box to add carriers to an H.323 gateway.

f If desired, in the Number of ports: field, type a number defining the size of the H.323 virtual carrier block you are adding.

A range of 4 to 672 endpoints (inclusive) is supported.

For examples of how to take advantage of carrier block flexibility when provisioning H.323 gateways, refer to H.323 carrier provisioning on page 225.

Note 1: The Number of ports: field is optional for H.323 gateways. If you do not type a number in this field, the system allocates the default block of endpoints for your system, either 24 (NA) or 32 (International).

Note 2: The Number of ports: field is not used for any gateways other than those supporting H.323.

Note 3: The total sum of values entered in the Number of ports: field for all carriers assigned to an H.323 gateway must be less than, or equal to, the value entered in the

Reserved terminations: field of the Associate Media Gateway dialog box. Refer to procedure Associate an H.323 media gateway on page 175.

g Go to step i.

h Select the PRI check box, if applicable, and enter a PRI Interface ID (IID) value within the range of 0 to 31 (inclusive).

Note 1: The IID value is not used in international PRI. Therefore, for offices using international PRI, select the PRI check box and set the value to 0.

Note 2: For PRI in the North American market, the IID value is used in the non-facility associated signaling (NFAS) configuration in which multiple DS1 trunks are controlled by one D-channel. In this case, the IID value must match the IID value provisioned at the far-end switch.

Note 3: Do not select this check box if

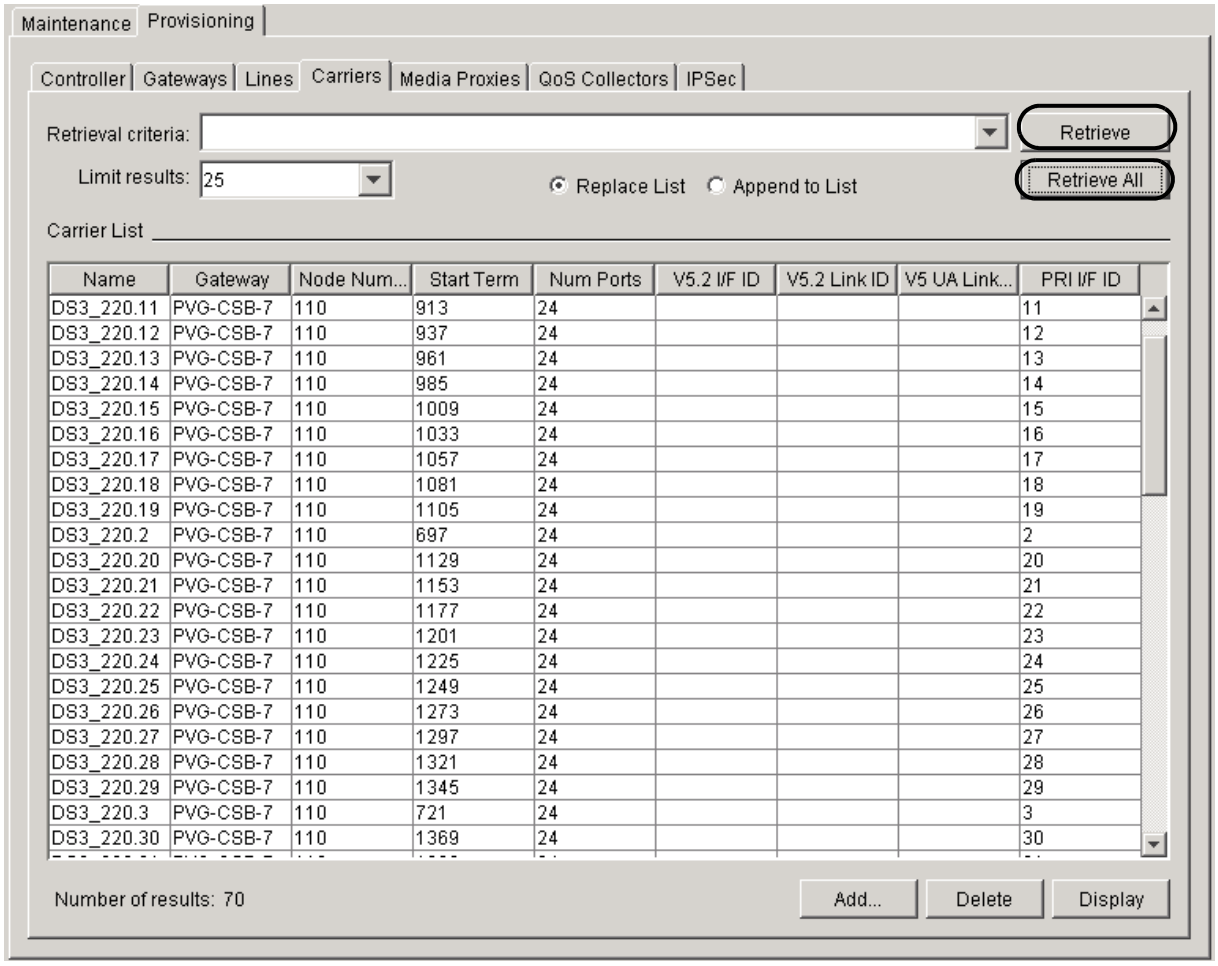
- PRI trunks are not provisioned in the carrier group;
- you are adding carriers to a gateway supporting H.323.

i Click the **OK** button to accept the input to the Add Carrier dialog box.

If the add carrier operation is successful, a dialog box is displayed. Click **OK** to continue.

If the add carrier operation fails, an error message will be displayed. Click the Show Details button for more information. An error message will also appear in the status bar at the bottom of the screen.

6 To verify your changes, click the **Retrieve All** or the **Retrieve** button to update the Carrier List.



7 Repeat this procedure as required for other carriers you wish to add to a media gateway.

8 Refer to the *CS 2000 Configuration Management* NTP applicable to your solution to provision the trunks that correspond to the carriers.

9 The procedure is complete.

Carrier and endpoint naming

This section provides a table containing the naming conventions for carriers (endpoint groups) and endpoints. This table is organized based on the gateway profile name selected when associating a media gateway with a GWC node.

This table references the following signaling protocols:

- Aspen
- H.248/Megaco
- Media Gateway Control Protocol (MGCP)
- Trunk Gateway Control Protocol (TGCP)
- H.323

Carrier and endpoint names (Sheet 1 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
AFC	**tp/<TT><tt>** where tp is lower case <TT> is a number: 00-10 <tt> is a number: 00-99 (except where <TT> is 10, in which case <tt> is limited to the range: 00-22); for a maximum of 1022 terminations allowed for each gateway **Example:** tp/1013
AMBIT line gateways	**aaln/<n>** where <n> is a number: 1-16 depending on the model and market (specified when choosing the media gateway profile)
ARRIS_TOUCHTONE line gateways	**aaln/<n>** where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile)

Carrier and endpoint names (Sheet 2 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
ASKEY_LINE Integrated Access Devices (IAD) gateways	**aaln/<n>** where <n> is a number: 1-30 depending on the model and market (specified when choosing the media gateway profile)
AUDIOCODES (Nortel Media Gateway 3200)	Carrier or gateway endpoints are provisioned in groups representing E1 and DS1 levels. Provisioning at this level gives access to all timeslots for service provisioning. Carrier names are case sensitive and must be entered in upper case. Descriptions below include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS1/E1 timeslot level. **DS1** **DS1/<h2>/<g>** (H.248/Megaco) where <h2> is the DS1 (two digit) port or span number: 01-04 <g> is the channel number: 1-24 (no leading 0), assigned by the system **Example:** Carrier name: DS1/03 Carrier Endpoint name (timeslot): DS1/03/1
CICM	tp/<TT><tt> where tp is lower case <TT> is a number: 00-10 <tt> is a number: 00-99 (except where <TT> is 10, in which case <tt> is limited to the range: 00-23); for a maximum of 1023 terminations allowed for each gateway **Example:** tp/1013 ***Note:*** Each endpoint appears as a virtual media gateway (VMG). Refer to the *CICM Series 2.5 Product and Technology Fundamentals*, NN10027-111.

Carrier and endpoint names (Sheet 3 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
CISCO_2600 CISCO_3600 CISCO_AS5300 CISCO_H323_IOS Supporting H.323 signaling protocol	**EPG_<n>** where <n> is a number: 000 - 999 ***Note 1:*** The underscore character "_" is required and the number must include three digits (it must be zero-padded). ***Note 2:*** Duplicate carrier names on different media gateways are permitted. **Example**: EPG_001
CVX-600 CVX-1800	**<gateway Name>.<E1 carrier>_<W0>.<Y1>.<Z1>** where <W0> is the slot number on the CVX chassis: 1-18 <Y1> is the E1 port number on the Digital Access Card: 0-99 <Z1> is the E1 timeslot/channel number: 0-31 **Example:** CVX1.E1_17.2.19 ***Note:*** Provisioning of the endpoints is same for both RAS and VOIP setup.
H323_PROXY	**EPG_<n>** where <n> is a number: 000 - 999 ***Note 1:*** The underscore character "_" is required and the number must include three digits (it must be zero-padded). ***Note 2:*** Duplicate carrier names on different media gateways are permitted. **Example**: EPG_001

Carrier and endpoint names (Sheet 4 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
MEDIATRIX Integrated Access Device (IAD) gateways	**aaln/<n>** where <n> is a number: 1-4 or 1-24 depending on the model and market (specified when choosing the media gateway profile).
MGCP line gateway MGCP_IAD_40 line gateway	**aaln/<n>** where <n> is a number: 1-40 depending on the configuration of the gateway.
MOTOROLA MTA line gateways	**aaln/<n>** where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile)
NORTEL_BCM Supporting H.323 signaling protocol	**EPG_<n>** where <n> is a number: 000 - 999 ***Note 1:*** The underscore character "_" is required and the number must include three digits (it must be zero-padded). ***Note 2:*** Duplicate carrier names on different media gateways are permitted. **Example**: EPG_001

Carrier and endpoint names (Sheet 5 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
NUERA_BTX4K	The gateway profile name NUERA_BTX4K supports the Nuera BTX4K gateway, which allows provisioning of six DS3s. **DS3** (with channelized DS1 levels) **ds/ds3-<u1>/ds1-<u2>/<c>** where <u1> is a decimal value referring to the particular instance of ds3: 1-6 <u2> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy:1-24 **Example:** Carrier name: ds/ds3-2/ds1-3 Carrier Endpoint name (timeslot): ds/ds3-2/ds1-3/1

Carrier and endpoint names (Sheet 6 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
NUERA_GX	Carrier or gateway endpoints are provisioned in groups representing E1 and DS3 levels. Provisioning at this level gives access to all timeslots for service provisioning. Supported services include ISUP trunking and PRI trunking. Carrier names are case sensitive and must be entered in upper case. Descriptions below include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS1/E3 timeslot level. **E1** **E1_<h1><h2>.<g>** (Aspen) or **E1/<h1>/<h2>/<g>** (H.248/Megaco) where <h1> is the two-digit LP (logical processor) number (or slot) of the E1: 1-15 <h2> is the E1 (two digit) port number: 01-32 <g> is the channel number: 1-31 (no leading 0), assigned by the system **Aspen example:** Carrier name: E1_305 Carrier Endpoint name (timeslot): E1_305.1 **H.248/Megaco example:** Carrier name: E1/03/05 Carrier Endpoint name (timeslot): E1/05/05/1

Carrier and endpoint names (Sheet 7 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
NUERA_GX (continued)	**DS3/DS1** ***Note:*** DS1 carriers are provisioned using the same endpoint naming as DS3. **DS3_<b1><b2>.<c>.<d>** (Aspen) or **DS3/<h1>/<h2>/<g>** (H.248/Megaco) where <b1> is the LP (logical processor) number or slot of the DS3: 1-15 (2-5 recommended) <b2> is the DS3 (single digit) port number: 0-1 <c> is the DS3 number: 1-28 <d> is the channel number in the DS3: 1-24, assigned by the system **Aspen example:** Carrier name: DS3_20.3 Carrier Endpoint name (timeslot): DS3_20.3.1 **H.248/Megaco example:** Carrier name: DS3/03/05 Carrier Endpoint name (timeslot): DS3/05/05/1
PVG7K, PVG15K PVG15K_1000 PVG15K_PARTIAL PVG_APG	Carrier or gateway endpoints are provisioned in groups representing E1 and DS3 levels. Provisioning at this level gives access to all timeslots for service provisioning. Supported services include ISUP trunking and PRI trunking. Carrier names are case sensitive on the Passport Packet Voice Gateway (PVG) and must be entered in upper case. Descriptions below include both endpoint groups and individual endpoint descriptions. Services can be applied at the DS3/E1 timeslot level.

Carrier and endpoint names (Sheet 8 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
PVG7K PVG15K PVG15K_1000 PVG15K_PARTIAL PVG_APG (continued)	**E1** **e1_<h1><h2>.<g>** (Aspen) or **e1/<h1>/<h2>/<g>** (H.248/Megaco) where <h1> is the two-digit LP (logical processor) number or slot of the E1: 1-15 (no leading 0) <h2> is the E1 (two digit) port number: 01-32 <g> is the channel number: 1-31 (no leading 0), assigned by the system **Aspen example:** Carrier name: e1_305 Carrier Endpoint name (timeslot): e1_305.1 **H.248/Megaco example:** Carrier name: e1/03/05 Carrier Endpoint name (timeslot): e1/03/05/1
	DS3 **DS3_<b1><b2>.<c>.<d>** (Aspen) or **DS3/<h1>/<h2>/<g>** (H.248/Megaco) where <b1> is the LP (logical processor) number or slot of the DS3: 1-15 (2-5 recommended) <b2> is the DS3 (single digit) port number: 0-1 <c> is the DS3 number: 1-28 <d> is the channel number in the DS3: 1-24, assigned by the system **Aspen example:** Carrier name: DS3_20.3 Carrier Endpoint name (timeslot): DS3_20.3.1 **H.248/Megaco example:** Carrier name: DS3/03/05 Carrier Endpoint name (timeslot): DS3/05/05/1

Carrier and endpoint names (Sheet 9 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
PVG7K PVG15K PVG15K_1000 PVG15K_PARTIAL PVG_APG (continued)	**STM-1** **SM_<lp><pp>01_412_01<k><l><m>.<e>** (Aspen) or **STM/<lp>/<p>/1/VC4VC12/1/<k>/<l>/<m>/<e>** (H.248/Megaco) where <lp> is the LP (logical processor) number or slot of the STM-1 interface: 2-15 (slots 2-5 are recommended) <pp> is the two-digit port number: 00-03 <p> is the one-digit port number: 0-3 <k> is the one-digit TUG-3 number within a VC4: 1-3 <l> is the one-digit TUG-2 number within a TUG-3: 1-7 <m> is the one-digit TU number within a TU: 1-3 <e> is the VS-12 channel/timeslot: 1-31 (no leading 0) ***Note:*** Hard-coded values 01_412_01 (Aspen) and 1/VC4VC12/1 (H.248) indicate the STM carrier type, multiplexing within the STM-1 frame, and the AUG within the STM-1 frame. **Aspen example:** Carrier name: SM_020101_412_01361 Carrier Endpoint name (timeslot): SM_020101_412_01361.1 **H.248/Megaco example:** Carrier name: STM/2/1/1/VC4VC12/1/3/6/1 Carrier Endpoint name (timeslot): STM/2/1/1/VC4VC12/1/3/6/1/1

Carrier and endpoint names (Sheet 10 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
PVG7K PVG15K PVG15K_1000 PVG15K_PARTIAL PVG_APG (continued)	**OC-3** **SS_<lp><pp>03_VT15_<jj><l><m>.<e>** (Aspen) or **STS/<lp>/<p>/3/VT15/<t>/<l>/<m>/<e>** (H.248/Megaco) where <lp> is the LP (logical processor) number or slot of the OC-3 interface: 1-15 (recommended slots 2-5) <pp> is the (two digit) port number: 00-03 <p> is the (one digit) port number: 0-3 <jj> is the (two digit) STS-1 number within the STS-3: 01-03 <l> is the (one digit) VT group number within STS-1: 1-7 <m> is the (one digit) VT number within a VT: 1-4 <t> is the (one digit) STS-1 number within the STS-3: 0-3 <e> is the VT1.5 channel/timeslot: 1-24 (no leading 0) ***Note:*** Hardcoded values 03_VT15_ (Aspen) and /3/VT15/ (H.248) indicate the STS carrier type and the multiplexing within the OC-3 carrier. **Aspen example:** Carrier name: SS_20103_VT15_0131 Carrier Endpoint name (timeslot): SS_20103_VT15_0131.1 **H.248/Megaco example:** Carrier name: STS/2/1/3/VT15/1/6/1 Carrier Endpoint name (timeslot): STS/2/1/3/VT15/1/6/1/1

Carrier and endpoint names (Sheet 11 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
SUCCESSION_1000 Supporting H.323 signaling protocol	**EPG_<n>** where <n> is a three-digit number: 000 - 999 ***Note 1:*** The underscore character "_" is required and the number must include three digits (it must be zero-padded). ***Note 2:*** Duplicate carrier names on different media gateways are permitted. **Example**: EPG_001
TGCP	GWCs support TGCP media gateways with • DS1 interfaces • DS1 interfaces within a logical processor or slot • OC3 interfaces with channelized DS3 and DS1 levels • OC3 interfaces with channelized DS3 and DS1 levels within a logical processor or slot • DS3 interfaces with a channelized DS1 level within a logical processor or slot • DS3 interfaces without DS1 framing • DS3 interfaces with a channelized DS1 level • E1 interfaces ***Note 1:*** The following abbreviations are used in TGCP carrier and endpoint formats: • u = unit number • c = channel number ***Note 2:*** The gateway profile name TGCP supports third party media gateways using TGCP signaling protocol.

Carrier and endpoint names (Sheet 12 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	**DS1** **ds/ds1-<u>/<c>** where <u> is a decimal value referring to the particular instance of ds1: 1-68 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 **Example:** Carrier name: ds/ds1-1 Carrier Endpoint name (timeslot): ds/ds1-1/1
	DS1 (within a logical processor or slot) **ds/s-<u1>/ds1-<u2>/<c>** where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 **Example:** Carrier name: ds/s-2/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/ds1-1/1

Carrier and endpoint names (Sheet 13 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	**OC3** (with DS3 and DS1 levels) **ds/oc3-<u1>/ds3-<u2>/ds1-<u3>/<c>** where <u1> is a decimal value referring to the particular instance of oc3: 1-28 <u2> is a decimal value referring to the particular instance of ds3: 1-28 <u3> is a decimal value referring to the particular instance of ds1: 1-28 <channel #> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 **Example:** Carrier name: ds/oc3-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/oc3-2/ds3-3/ds1-1/1
	OC3 (with DS3 and DS1 levels within a logical processor or slot) **ds/s-<u1>/oc3-<u2>/ds3-<u3>/ds1-<u4>/<c>** where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of oc3: 1-28 <u3> is a decimal value referring to the particular instance of ds3: 1-28 <u4> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-24 **Example:** Carrier name: ds/s-2/oc3-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/oc3-2/ds3-3/ds1-1/1

Carrier and endpoint names (Sheet 14 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	**DS3** (with a DS1 level within a logical processor or slot) **ds/s-<u1>/ds3-<u2>/ds1-<u3>/<c>** where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of ds3: 1-28 <u3> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy:1-24 **Example:** Carrier name: ds/s-2/ds3-3/ds1-1 Carrier Endpoint name (timeslot): ds/s-2/ds3-3/ds1-1/1
	DS3 (without DS1 framing) **ds/s-<u1>/ds3-<u2>/<c>** where <u1> is a decimal value referring to the particular instance of s (slot): 1-28 <u2> is a decimal value referring to the particular instance of ds3: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy.: 1-24 **Example:** Carrier name: ds/s-2/ds3-3/ Carrier Endpoint name (timeslot): ds/s-2/ds3-3/1

Carrier and endpoint names (Sheet 15 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
TGCP (continued)	**DS3** (with channelized DS1 levels) **ds/ds3-<u1>/ds1-<u2>/<c>** where <u1> is a decimal value referring to the particular instance of ds3: 1-28 <u2> is a decimal value referring to the particular instance of ds1: 1-28 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy:1-24 **Example:** Carrier name: ds/ds3-2/ds1-3 Carrier Endpoint name (timeslot): ds/ds3-2/ds1-3/1
	E1 **ds/e1-<u1> /<c>** where <u1> is a decimal value referring to the particular instance of e1: 1-68 <c> is a decimal value indicating the channel number at the lowest level in the hierarchy: 1-31 **Example:** Carrier name: ds/e1-1 Carrier Endpoint name (timeslot): ds/e1-1/1
TOUCHTONE_NN line gateways	**aaln/<n>** where <n> is a number: 1-4 depending on the MTA model and market (specified when choosing the media gateway profile).
UAS Audio servers (including Nortel Media Server 2000 Series)	Endpoints are not specified during provisioning of audio servers.

Carrier and endpoint names (Sheet 16 of 16)

Media gateway type (based on profile)	Carrier name and endpoint names or identifiers
UE9000MG (Media Gateway 9000)	**tp/<slot>/<circuit>** where tp is lower case <slot> is a number: 1-21 <circuit> is a number: 0-31 **Example:** tp/1/13 **Note:** Each endpoint appears as a virtual media gateway (VMG).
WESTELL Supporting H.323 signaling protocol	**EPG_<n>** where <n> is a three-digit number: 000 - 999 ***Note 1:*** The underscore character "_" is required and the number must include three digits (it must be zero-padded). ***Note 2:*** Duplicate carrier names on different media gateways are permitted. **Example**: EPG_001

H.323 carrier provisioning

This section compares the various limits associated with carrier provisioning of GWCs supporting H.323 signaling protocol between Carrier VoIP releases. This section also provides two examples of carrier provisioning on a GWC node supporting H.323. One example uses many small gateways, and the other uses one large gateway.

Note: The information in this section applies only to H.323 GWCs.

The following table describes the rules that apply to provisioning carriers on GWCs supporting H.323.

H.323 carrier provisioning limits and ranges

Parameter	Pre-SN07 maximum	SN08 maximum
Number of endpoints supported on a GWC node	**1032** - NA **1024** - Intl	**1032** - NA **1024** - Intl
Number of endpoints supported on a media gateway	**480** (Succession_1000)	**1032** - NA **1024** - Intl (all supported gateways)
Number of media gateways supported on a GWC node	**43** - NA **32** - Intl (Succession_1000)	**254**
Number of endpoints in a carrier (size of a carrier block)	**24** - NA **32** - Intl	**4 - 672** (virtual carrier - user provisionable within this range)

Note: Starting in SN07, more than one carrier (D-channel) can be supported on a single media gateway. Therefore, more than one trunk group on the XA-Core can be mapped to the endpoints (TID) provisioned on the GWC.

For a provisioning example of this feature, refer to Example 2: One large gateway provisioned on a GWC node on page 226

Example 1: Many gateways provisioned on a GWC node

This example demonstrates how to take advantage of the flexible carrier size for small gateways with relatively few endpoints on each gateway.

In this example, a GWC node supporting H.323 protocol is provisioned as follows:

- 254 NORTEL_BCM media gateways are associated with 1 GWC node.
- 253 of the gateways are provisioned with 1 carrier containing 4 endpoints each.
- One gateway is provisioned with 1 carrier containing 20 endpoints.

In this example, the total number of endpoints used on the GWC node is 1032.

Example 2: One large gateway provisioned on a GWC node

This example demonstrates how to take advantage of the fact that more than one carrier (or D-channel) can be mapped to a single gateway starting release SN07.

In this example, a GWC node supporting H.323 protocol is provisioned as follows:

- One SUCCESSION_1000 media gateway is associated with one GWC node.
- The gateway is provisioned with two carriers containing 515 endpoints each.

In this example, the total number of endpoints used on the GWC node is 1032. Each carrier group maps to a trunk group on the XA-Core.

Delete carriers from a GWC

Purpose of this procedure

Use this procedure to delete (remove) carriers from a Gateway Controller (GWC) node.

When to use this procedure

Use this procedure when carriers must be removed or changed.

Note 1: Line endpoints are removed automatically when lines are removed (de-provisioned) from a GWC. To de-provision lines, refer to the *CS 2000 Configuration Management* NTP supporting your solution.

Note 2: Starting in SN07, H.323 gateway carriers (endpoint groups) must be removed manually.

Carriers for all other gateway types must also be removed manually.

Prerequisites and guidelines

All carriers on a gateway must be in one of the following states before they can be removed:

- INB (Installation Busy)
- UNKNOWN (core datafill is missing)

To place trunk groups on the XA-Core in a state of INB refer to procedure “Performing trunk maintenance using the Trunk Maintenance Manager” in the *ATM/IP Solution-level Fault Management* NTP, NN10408-900.

Additional XA-Core table datafill may need to be removed in order to remove all trunk and line endpoint data from all databases.

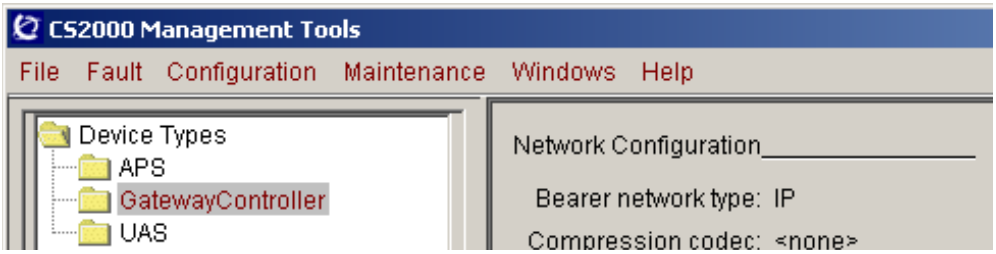
You must delete one carrier at a time.

Do not remove V5.2 carriers using this procedure. Refer to procedure Delete V5.2 interfaces on page 503 in this NTP.

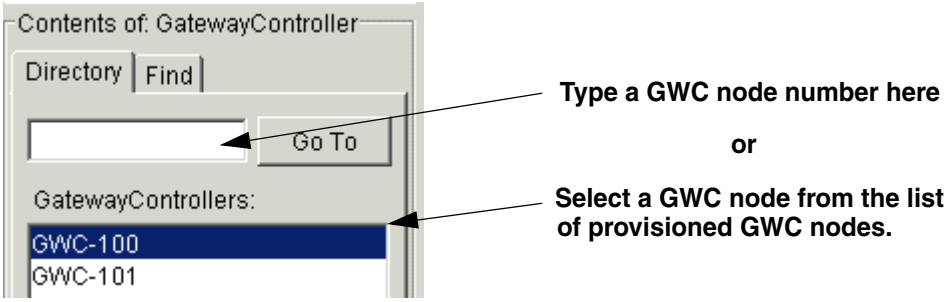
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.

4 Click the **Carriers** tab.

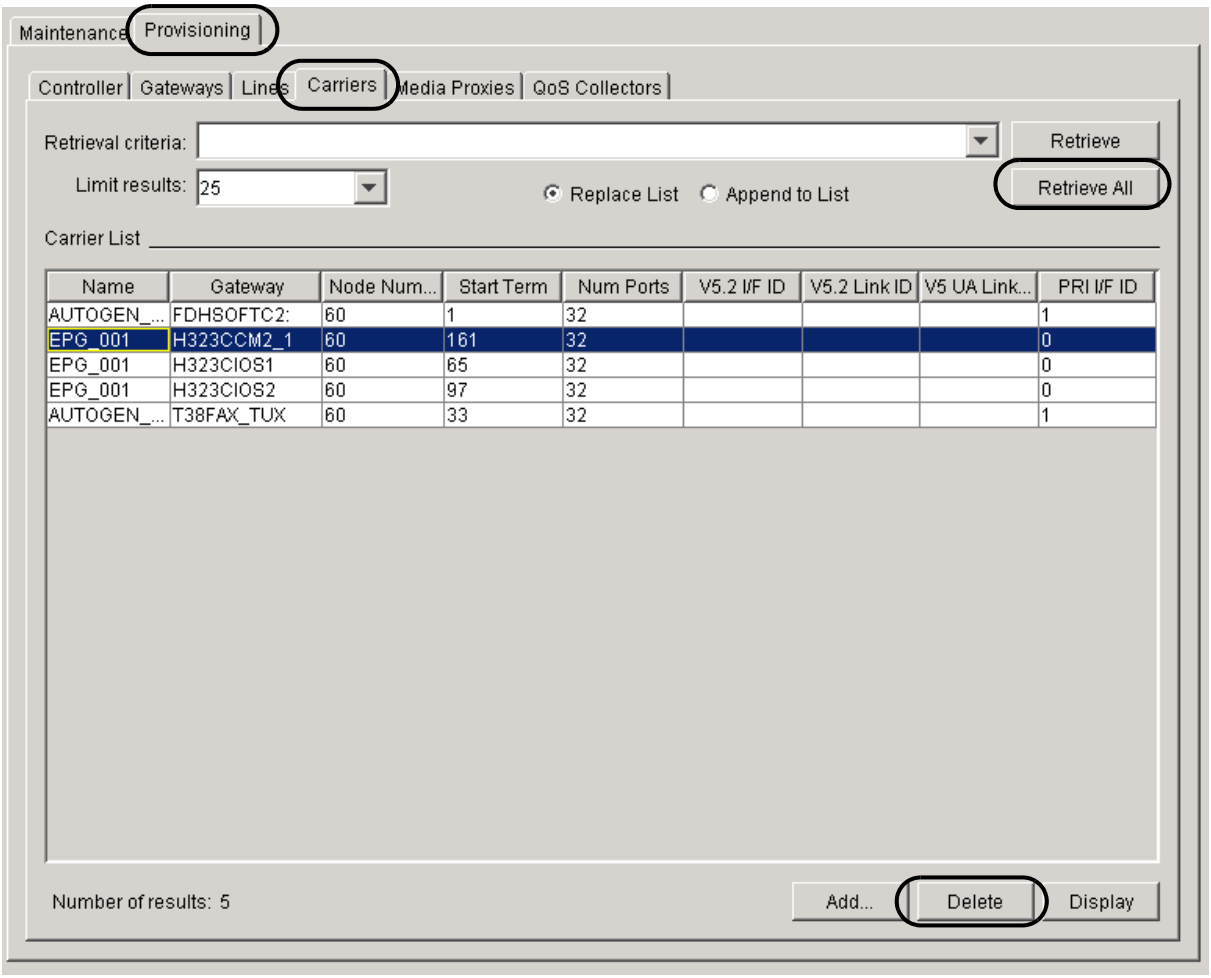
5 Click the **Retrieve All** button to retrieve all carriers on the specified GWC node.

6 From the Carrier List, select the carrier you wish to delete.

Your selection is highlighted.

Note: You can delete only one carrier at a time.

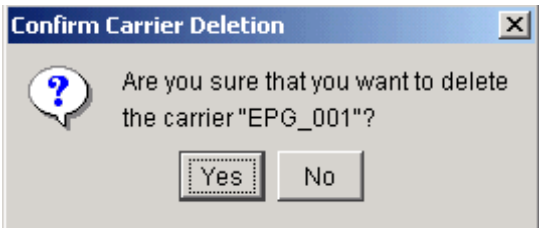
7 Click the **Delete** button at the bottom screen.



8

CAUTION
Possible partial service disruption
If endpoints associated with a carrier are deleted from the GWC and not from the Computing Module (CM), you will encounter call processing problems. Refer to the *CS 2000 Configuration Management* NTP for your solution to remove corresponding trunk data from the XA-Core tables.

At the confirmation box, click **Yes** to confirm that you wish to delete the carrier.



Note: The carrier list is automatically updated following a successful deletion.

9 Repeat this procedure for other carriers you wish to delete on this GWC node.

10 The procedure is complete.

View carrier provisioning data for a GWC node

Purpose of this procedure

Use this procedure to view carrier (endpoint group) provisioning data for a selected Gateway Controller (GWC) node.

Note: Starting in SN07, this procedure supports viewing carriers provisioned on H.323 gateways.

When to use this procedure

Use this procedure when you require specific provisioning information about carriers associated with a specific GWC node.

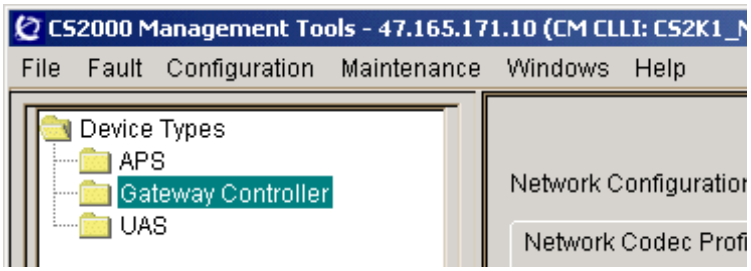
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

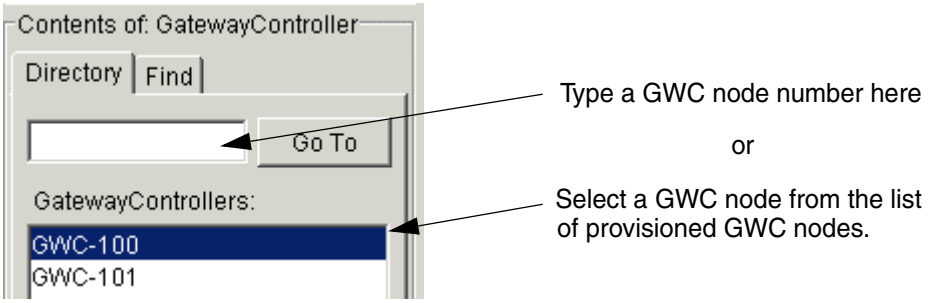
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

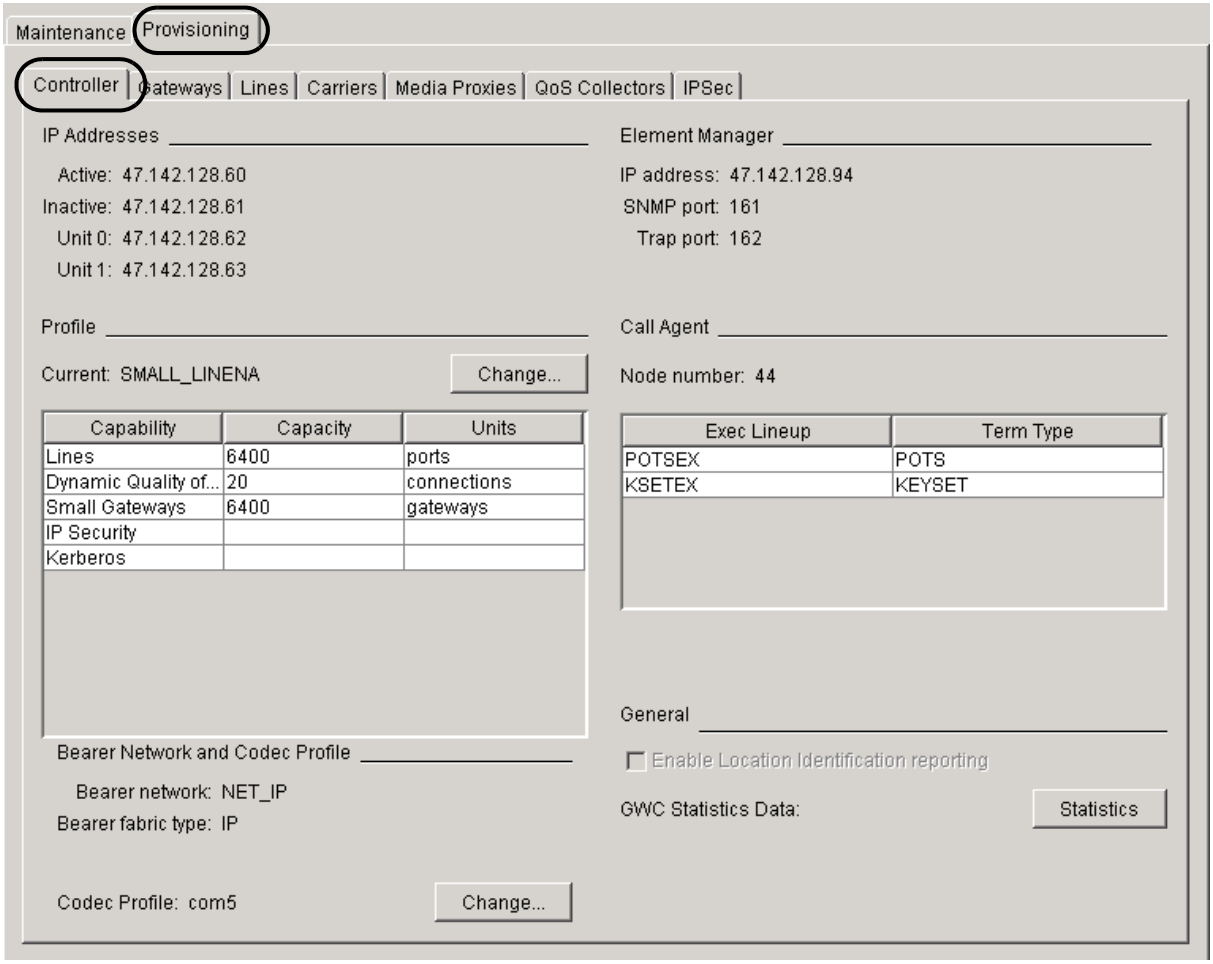


2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.

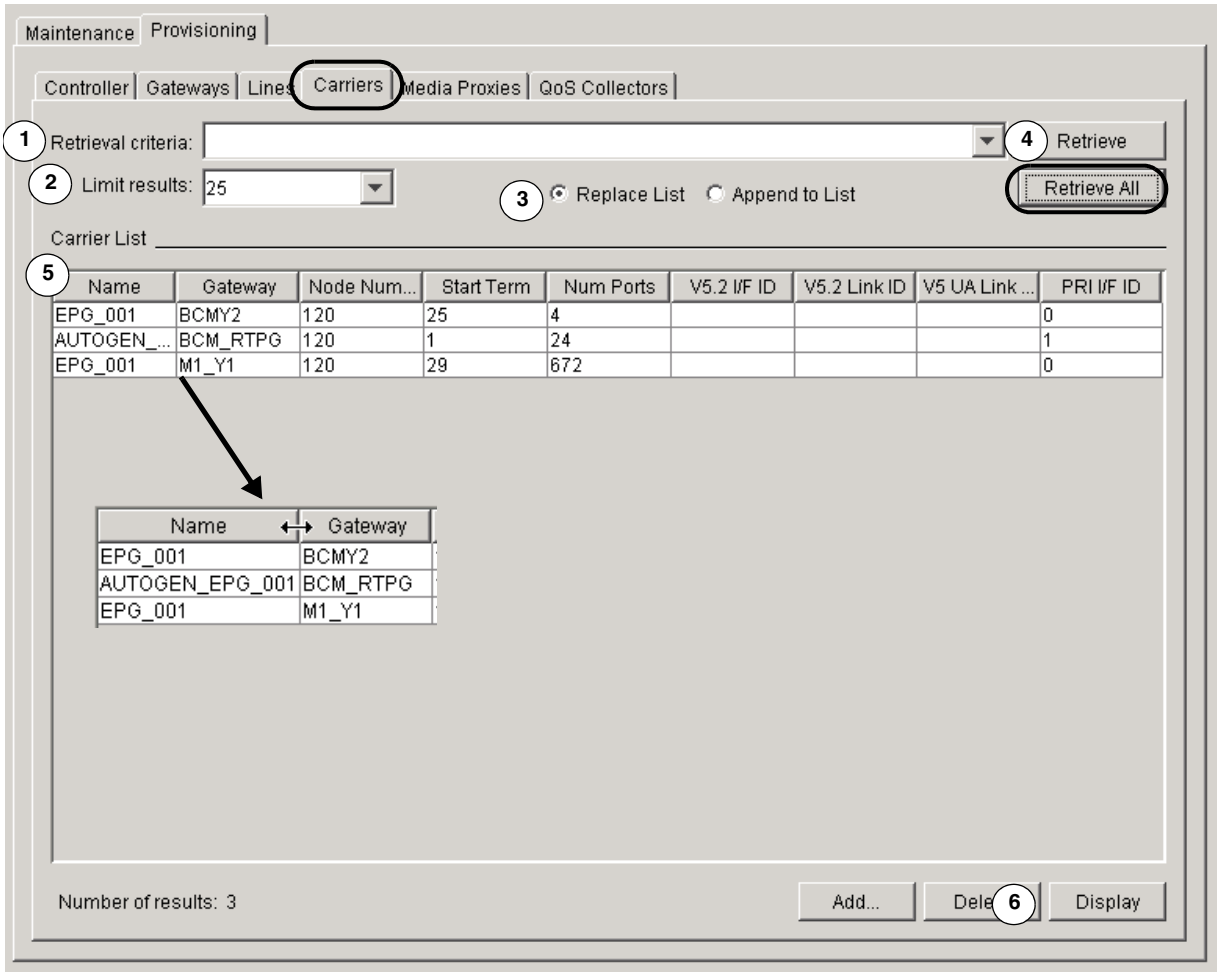
4 Click the **Controller** tab to view general provisioning information for the GWC node selected.



5 Click the **Carriers** tab to view information related to carriers (endpoint groups) belonging to gateways associated with the GWC node selected previously.

Select the edge of any tab to adjust the display.

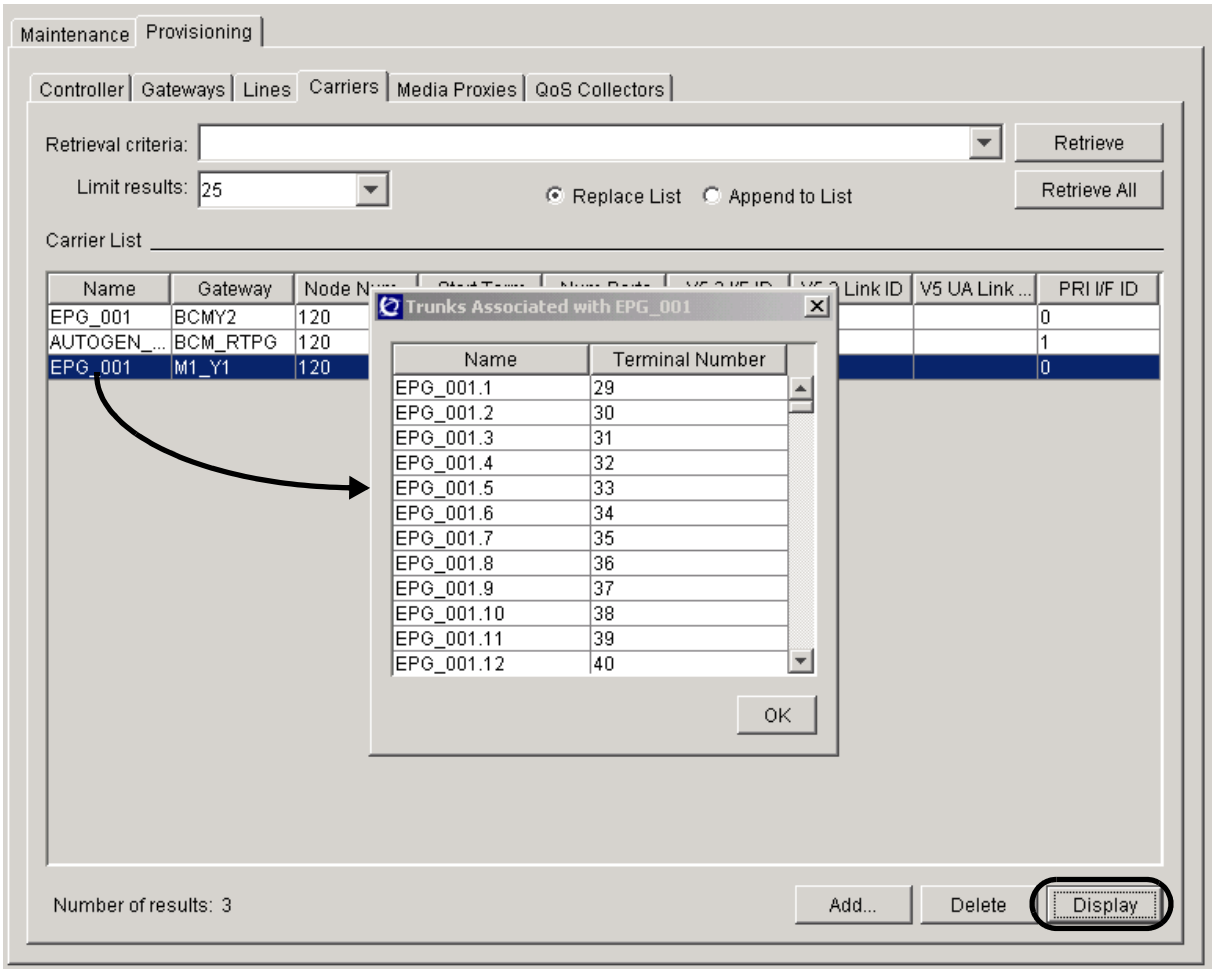
Note: For H.323 carriers, the existing auto-generated carrier names from release SN06.2 also appear in release SN8. Any new H.323 carriers assigned in SN08 are added manually based on the naming convention for H.323 carriers.



6 Click the **Retrieve All** button to view carrier endpoint data.

Note: The table Description of carrier endpoint search criteria functions on page 235 contains information about the search functions (see the numbers in the figure above).

7 If you wish to view the trunk endpoints and terminal numbers associated with a specific carrier, click the carrier entry and click the **Display** button.



8 Repeat this procedure as required for carrier endpoints you wish to view on this or other GWC nodes.

9 The procedure is complete.

The following table describes the carrier endpoint search criteria functions.

Description of carrier endpoint search criteria functions (Sheet 1 of 3)

Step	Menu component	Description
1	Retrieval criteria: selection box and drop-down list	Enter a search criteria string in this field. Up to 20 search strings are saved during the session. Previous search strings can be recalled by selecting from the drop-down list. Refer to the table Examples of carrier search criteria on page 237 at the end of this procedure for more details about using search strings.
2	Limit results: selection box and drop-down list	Select a value from the drop-down list. This value limits the number of matching entries returned in response to the query. Valid values are as follows: 25, 50, 100, 250, 500, 1000, and “no limit”. ***Note:*** The “no limit” value is still itself limited by the maximum number of entries currently downloadable, which is 4094.
3	Replace List radio button	Deselect this option if you do not want the query results to replace previously existing data displayed in the table. The default selection is to replace the existing data.
	Append to List radio button	Select this option if you want the query results to be appended to the existing data displayed in the table.

Description of carrier endpoint search criteria functions (Sheet 2 of 3)

Step	Menu component	Description
4	Retrieve button	This selection retrieves data from the CS 2000 GWC Manager server database matching the specified search retrieval criteria. The data presented is a “snapshot” of the CS 2000 GWC Manager database based on the currently provisioned data. The view is not updated in real time. ***Note:*** Newly added or deleted data will not be added to or deleted from the displayed table view except when there is a deletion of endpoints. If an carrier endpoint is selected from the table and deleted using the **Delete** button, then the endpoint will be removed from the table if deletion was successful. Endpoint deletion using this interface is limited to carrier endpoints only. Line endpoints are added automatically when you provision lines to a GWC. For instructions on how to add or delete lines, refer to the *CS 2000 Configuration Management* NTP applicable to your solution.
	Retrieve All button	This selection retrieves all the gateway or endpoint data, up to the maximum of 4094 entries. Values in the “Retrieval criteria” and “Limit results” are ignored.
5	Carrier List table	This is the tables where the search results are displayed. By clicking on a column header, you can sort the rows in ascending order, based on the values in that column. By clicking on the column header a second time, you can sort the rows in descending order. ***Note:*** The data is not preserved once another GWC node is selected; however, the retrieval criteria are maintained in the drop-down list so the same search can be re-executed.

Description of carrier endpoint search criteria functions (Sheet 3 of 3)

Step	Menu component	Description
6	Display	Highlight a carrier name and click this button if you wish to view the endpoints trunk and terminal numbers associated with a specific carrier.

Note 1: Use the Add button to add carriers (endpoint groups). For more information, refer to procedure Add carriers to a GWC on page 201.

Note 2: Use the Delete button to delete carriers. For more information, refer to procedure Delete carriers from a GWC on page 227.

Note 3: Line endpoints are added automatically when you provision lines on a GWC. For instructions on how to add or delete lines, refer to procedures in the *CS 2000 Configuration Management* NTP for your solution.

Examples of carrier search criteria (Sheet 1 of 2)

Examples of carrier search criteria

The gateway and endpoint panels use the same search functionality. The functionality is similar to that available in web search engines.

- One or more strings can be entered in the Retrieval Criteria: box, separated by space(s).
- Each string in the criteria is compared with the value in each column. If a match is found in any column, the record will be returned.
- Each string in the criteria is automatically wildcard at the beginning and end of the string. (For example, the string "gate" will match "MYGATEWAY" and "GATEWAY1".)
- Two special characters are supported as modifiers: the plus "+" and minus "-" signs.

  The "+" plus character prefixed to the string (for example, "+gate") means the value must match. The "-" character prefixed to the string (for example,. "-gate") means the value must not match.

  The "+" character is assumed, and therefore is not typically used.
- The search is not case sensitive. A string using "gate" will return records where the following strings are found: "MYGATEWAY", "MyGateway", or "mygateway".

Example Retrieval Criteria: "DS3"

Expected Results: Returns all records where the string is found in any column. A match for the example string will only be found in the Gateway name column.

Examples of carrier search criteria (Sheet 2 of 2)

Example Retrieval Criteria: "aspen"

Expected Results: Returns all records where the string is found, in any column. A match for the example string could be found in the Protocol column.

Retrieval Criteria: "47.108.2 -aspen"

Expected Results: Returns all records where the string "47.108.2" is found in any column and the string "aspen" is not found. The search will return the records of gateways where the subnet equals "47.108.2" and the protocol is not Aspen.

View characteristics of a GWC node

Purpose of this procedure

Use this procedure to view the basic characteristics currently defined for a selected Gateway Controller (GWC) node.

When to use this procedure

Use this procedure when you require the following specific information about a GWC node:

- IP addresses applicable to the GWC node
- IP address of the CS 2000 GWC Manager and port numbers used for SNMP and traps
- GWC profile assigned to the node, and the capability, capacity and units associated with the profile
- node number assigned to the GWC by the Call Agent
- bearer network and fabric type as well as the codec used by the node
- the number of endpoints reserved for the gateways currently associated with the selected GWC

Note: If you wish to view the Core IP addresses, refer to the General Network Settings on the main GWC network panel.

Prerequisites and guidelines

There are no prerequisites for this procedure.

GWC nodes and IP addressing

Four consecutive IP addresses are used for each GWC node (redundant card pair):

- 1 physical address for unit (card) 0
- 1 physical address for unit (card) 1
- 1 logical address for the active unit
- 1 logical address for the inactive unit

The physical addresses are provisioned at the CS 2000 SAM21 Manager. The active and inactive IP addresses are determined automatically by the CS 2000 SAM21 Manager. Although the active IP address is determined automatically, it must also be configured at the CS 2000 GWC Manager. The active unit IP address is required by other network elements, such as UAS nodes.

Logically, a GWC node is a single entity that can be accessed through a single IP address. Physically, however, a GWC node consists of two separate GWC cards, each of which has its own 10/100 BaseT Ethernet port. At a given moment, one of these cards is active and the other is inactive. The following list describes each type of address:

- Active unit - The IP address of the current active unit is used by other network entities. This address is used by the Call Agent, media gateways controlled by the GWC, and other GWCs for sending messages related to call-handling. This is the IP address specified when the GWC is datafilled in table SERVRINV.

  The active unit IP address is a floating address - the address is always the same, but the underlying physical unit changes in the event of a SWACT.

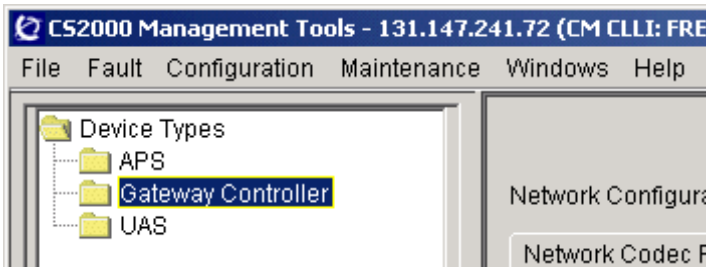
- Inactive unit - The IP address of the current inactive unit is used only for synchronization and for heartbeat messaging to and from the corresponding active GWC unit.

- Physical IP addresses - These are the static addresses for OAM&P and physical access to each GWC card (unit 0 and unit 1). These addresses are mapped on to Layer 2 media access control (MAC) addresses, Ethernet physical addresses.

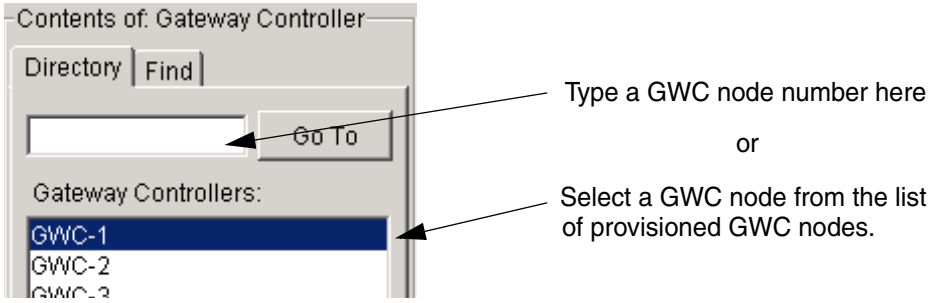
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.

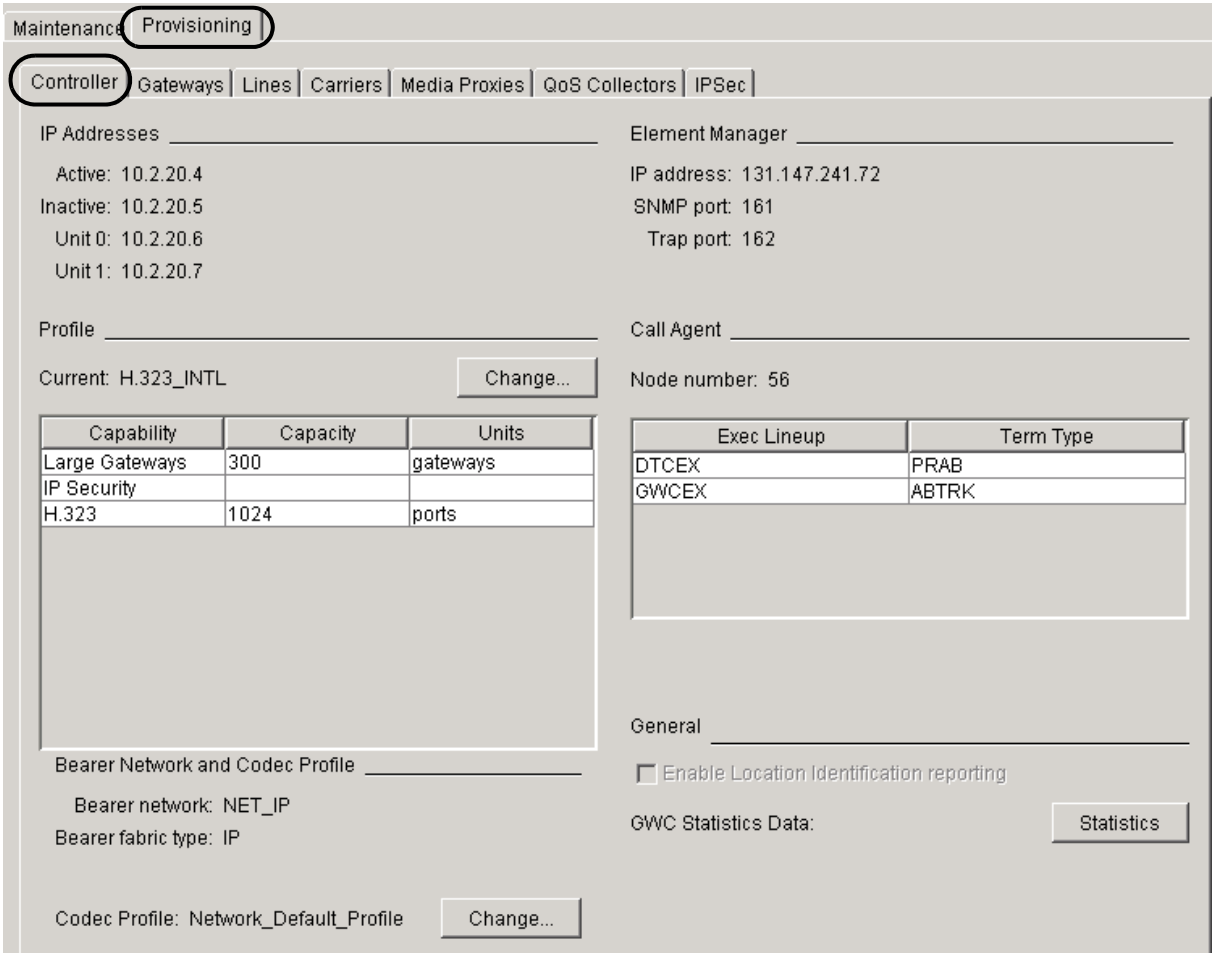


3 Click the **Provisioning** tab.

4 Click the **Controller** tab to view general node provisioning information for a selected GWC node.

This information includes the Gateway Controller service profile shown under the Profile heading.

Note: Refer to the table at the end of this procedure for an explanation of the information provided on this screen.



5 Repeat this procedure as required for other GWC nodes.

6 The procedure is complete.

Description of GWC node characteristics

Screen area	Description
IP Addresses	This area lists the IP addresses for the GWC node, including the active and inactive card, as well as unit 0 and unit 1.
Element Manager	This area provides the IP address of the CS 2000 GWC Manager used for node provisioning. It also includes the port numbers for SNMP and the trap log.
Profile	This area indicates the Gateway Controller service profile assigned to the node. It also provides the capability, capacity and units associated with the profile.
Call Agent	This area indicates the number assigned to the GWC node by the Call Agent. It also provides the specific Exec Lineup and Term Type characteristics assigned to the Call Agent to support the GWC node.
Bearer Network and Codec Profile	This area indicates the bearer network, bearer network fabric type and the codec profile used by the GWC node.
GWC Statistics Data:	Click the **Statistics** button to display the total number of endpoints reserved for all gateways currently associated with the selected GWC.

Note: Refer to procedure Enable or disable CICM location change reporting on page 313 for information on the General Settings area.

For information on using the Change buttons displayed on the screen, refer to the following procedures:

- Change the service profile of a GWC node on page 259
- Change the network codec profile for a GWC node on page 299

View gateway provisioning data for a GWC node

Purpose of this procedure

Use this procedure to view gateway data for a selected Gateway Controller (GWC) node.

When to use this procedure

Use this procedure when you require specific information about the gateways associated with a GWC node:

- gateways names
- IP addresses
- profiles used
- maximum and reserved terminations
- protocol used, including version and port
- PEP server or application layer gateways (ALG) used
- adjacent internet transparency zones
- root zones used (Centrex IP Client Manager gateways only)
- node name and number
- frame/unit/slot number
- logical group location (LGRPLOC)

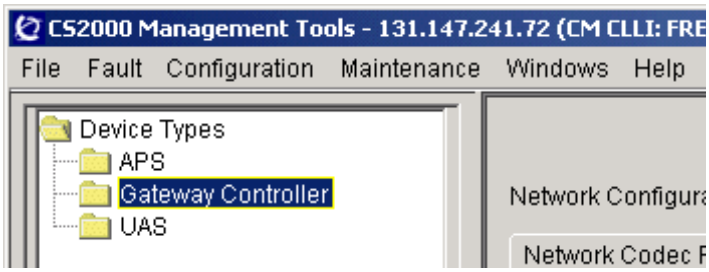
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

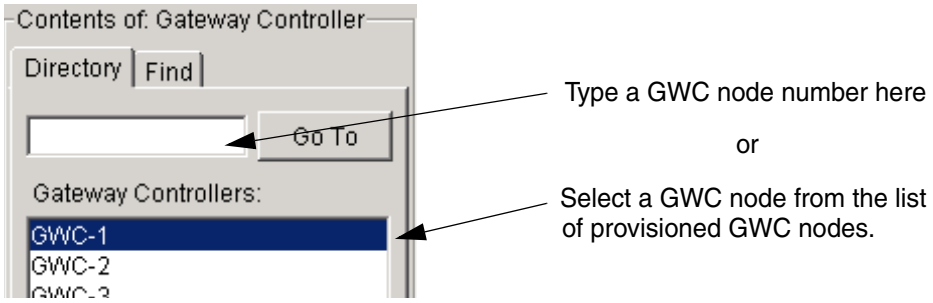
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.

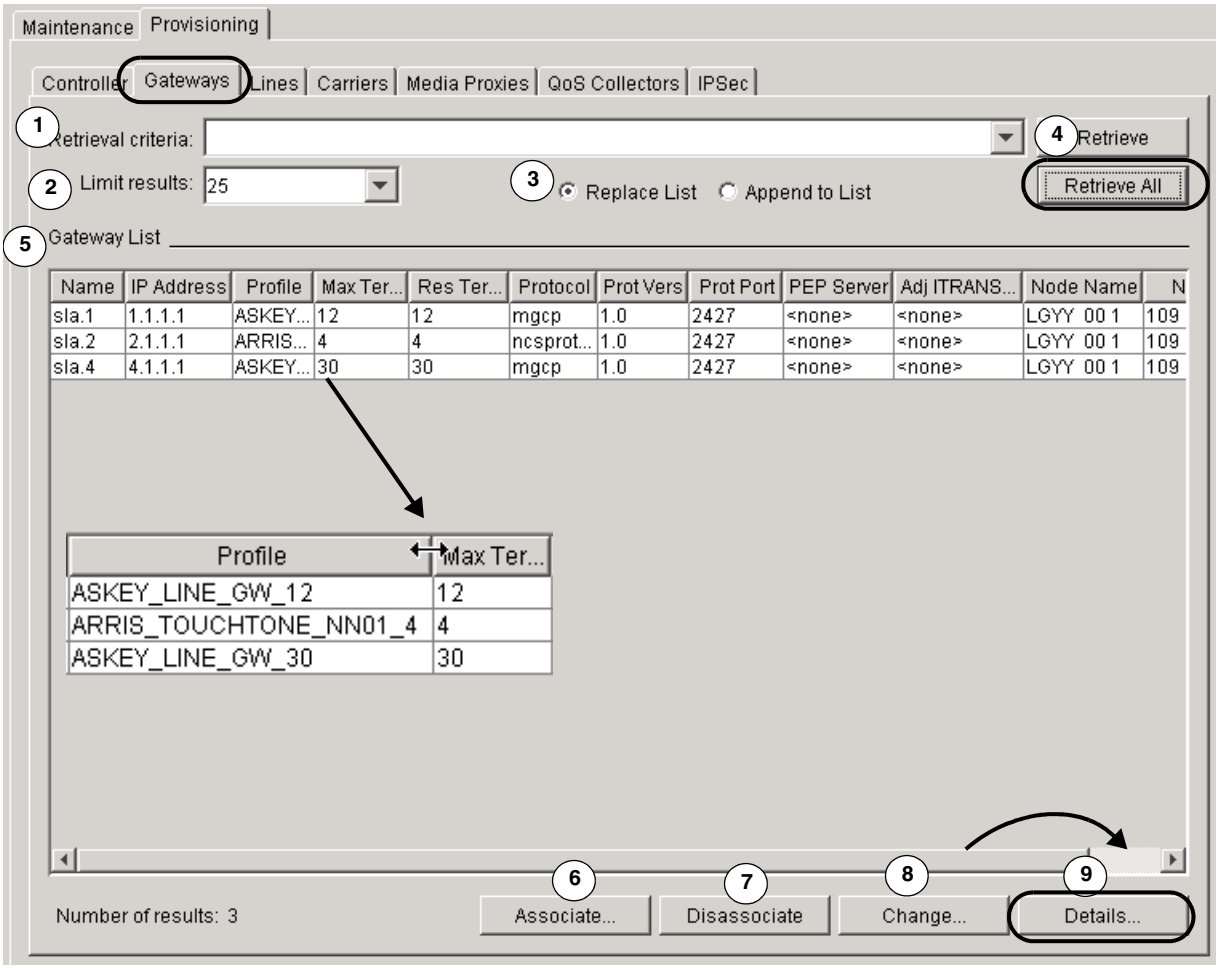


3 Click the **Provisioning** tab.

4 Click the **Gateways** tab and then click the **Retrieve All** button to view information about gateways associated with the selected GWC node. Any newly-created gateways are added to the end of the list. The list contains all gateways added using the CS 2000 GWC Manager and the XML interface of the OSSgate application.

Refer to the table at the end of this procedure to review the search functions.

Select the edge of any tab to adjust the display. To view any hidden gateway information, slide the horizontal scroll bar near the bottom of the screen to the right.



Note: The name UE9000MG may appear in the gateway list. This gateway is automatically entered in the list when a Media Gateway (MG) 9000 is provisioned in the system as a Virtual Media Gateway (VMG).

5 For Centrex IP Client Manager (CICM) gateways only, you can display any root middleboxes configured to interact with a gateway. Perform the following steps:

a Select a CICM gateway in the list.

b Click the **Details** button at the bottom of the screen.

Any root middleboxes configured for this gateway are displayed in the Gateway Details information box.

c Click the **OK** button to close the information box.

6 Repeat this procedure as required for gateways you wish to view on other GWC nodes.

7 The procedure is complete.

The following table describes the gateway search criteria functions.

Gateway search criteria functions (Sheet 1 of 3)

	Menu component	Description
1	Retrieval criteria selection box and drop-down list	Enter a search criteria string in this field. Up to 20 search strings are saved during the user's session. Previous search strings can be recalled by selecting from the drop-down list. Refer to the table Examples of gateway search criteria on page 251 at the end of this procedure for more details about using search strings.
2	Limit results selection box and drop-down list	Select a value from the drop-down list. This value limits the number of matching entries returned in response to the query. Valid values include: 25, 50, 100, 250, 500, 1000 and "no limit". ***Note:*** The "no limit" value is still itself limited by the maximum number of entries currently downloadable, which is 4094.
3	Replace List radio button	Deselect this option if you do not want the query results to replace previously existing data displayed in the table. The default selection is to replace the existing data.
	Append to List radio button	Select this option if you want the query results to be appended to the existing data displayed in the table.

Gateway search criteria functions (Sheet 2 of 3)

	Menu component	Description
4	Retrieve button	This selection retrieves data from the CS 2000 GWC Manager server database matching the specified search retrieval criteria. The data presented is a “snapshot” of the CS 2000 GWC Manager database based on the currently provisioned data. The view is not updated in real time. ***Note:*** Newly added or deleted data will not be added to or deleted from the displayed table view except when there is a deletion of endpoints. If an carrier endpoint is selected from the table and deleted using the Delete button, then the endpoint will be removed from the table if deletion was successful .
	Retrieve All button	This selection retrieves all the gateway up to the maximum of 4094 entries. Values in the “Retrieval criteria” and “Limit results” are ignored.
5	Gateways table	These are the tables where the search results are displayed. By clicking on a column header, you can sort the rows in ascending order, based on the values in that column. By clicking on the column header a second time, you can sort the rows in descending order. ***Note:*** The data is not preserved once another Gateway Controller node is selected; however, the retrieval criteria are maintained in the drop-down list so the same search can be re-executed.
6	Associate Button	Use this button to associate a line, trunk, UAS or gateway to the GWC.
7	Disassociate Button	Use this button to disassociate a gateway from this GWC node.

Gateway search criteria functions (Sheet 3 of 3)

	Menu component	Description
8	Change button	Use this button to change certain attributes of the gateway. For details, refer to procedure Change gateway attributes on page 277 in this NTP.
9	Details button	Use this button to view any root middleboxes provisioned for a CICM gateway.

Examples of gateway search criteria (Sheet 1 of 2)

Examples of gateway search criteria

The gateway panels utilize the same search functionality. The functionality is similar to that available in web search engines.

- One or more strings can be entered in the Retrieval Criteria, separated by space(s).
- Each string in the criteria is compared with the value in each column. If a match is found in any column, the record will be returned.
- Each string in the criteria is automatically wildcarded at the beginning and end of the string. (For example, the string "gate" will match "MYGATEWAY" and "GATEWAY1".)
- Two special characters are supported as modifiers: the plus "+" and minus "-" signs.

  The "+" plus character prefixed to the string (e.g. "+gate") means the value must match. The "-" character prefixed to the string (e.g. "-gate") means the value must not match.

  The "+" character is assumed, and therefore is not typically used.
- The search is not case sensitive. A string using "gate" will return records where the following strings are found: "MYGATEWAY", "MyGateway", or "mygateway".

Examples of gateway search criteria (Sheet 2 of 2)

Example Retrieval Criteria: "gate"

Expected Results: Returns all records where the string is found in any column. A match for the example string should only be found in the Gateway name column.

Example Retrieval Criteria: "aspen"

Expected Results. Returns all records where the string is found, in any column. A match for the example string could be found in the Protocol column.

Retrieval Criteria: "47.108.2 -aspen"

Expected Results: Returns all records where the string "47.108.2" is found in any column and the string "aspen" is not found. The search should return the records of gateways where the subnet equals "47.108.2" and the protocol is not Aspen.

View lines provisioning data for a GWC node

Purpose of this procedure

Use this procedure to view lines provisioning data for a selected Gateway Controller node.

When to use this procedure

Use this procedure when you require specific lines provisioning information associated with a GWC node.

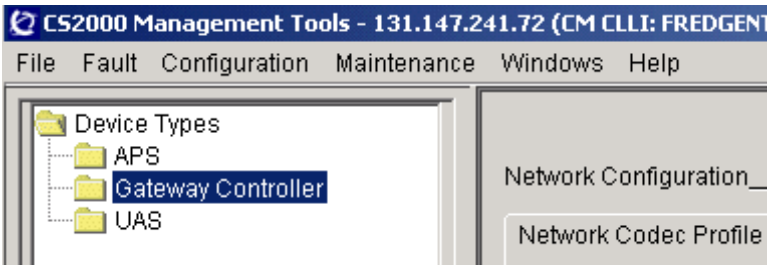
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

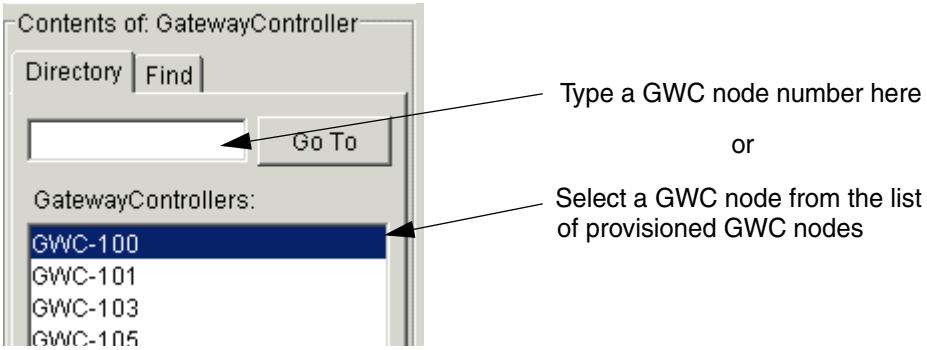
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

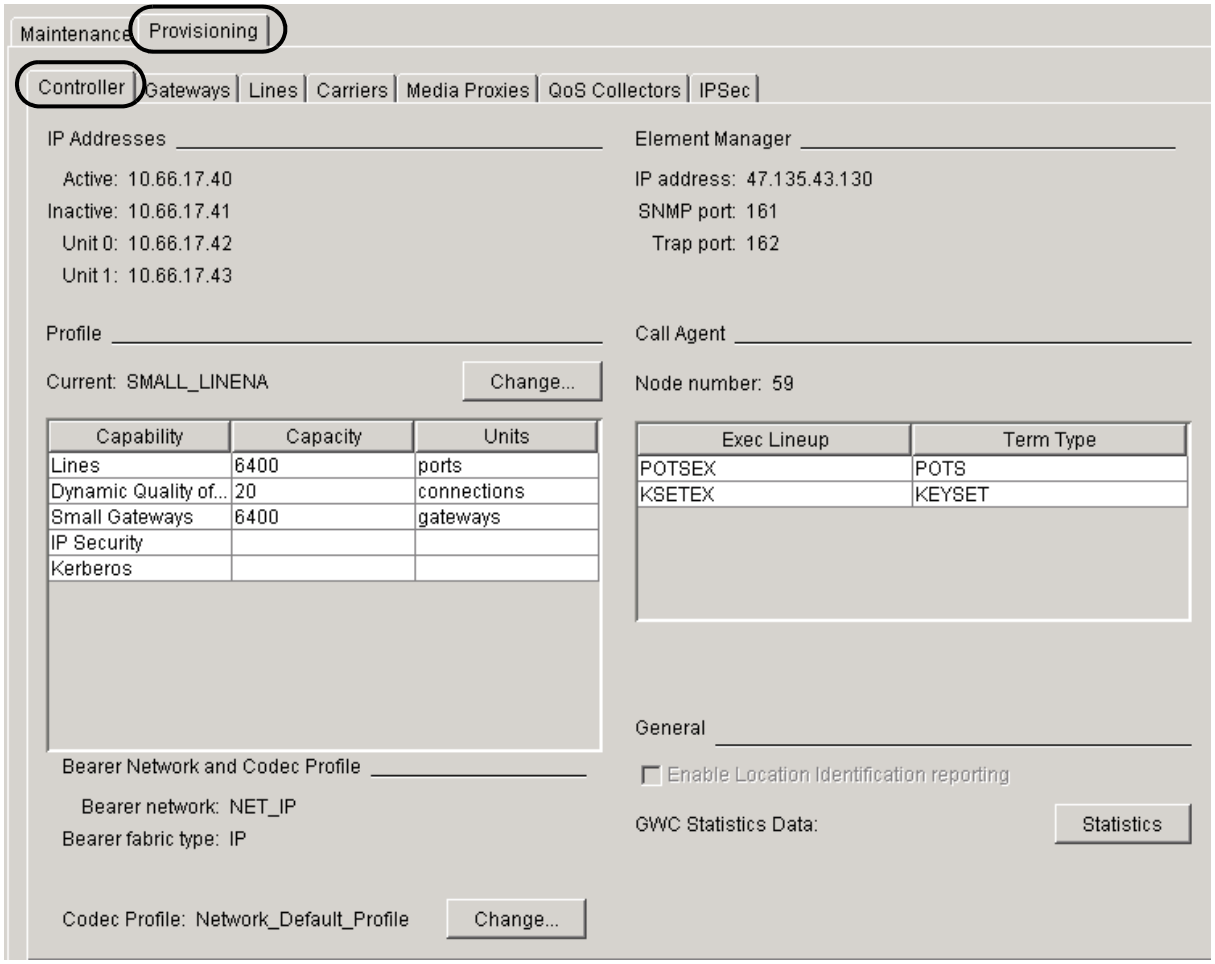


2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.

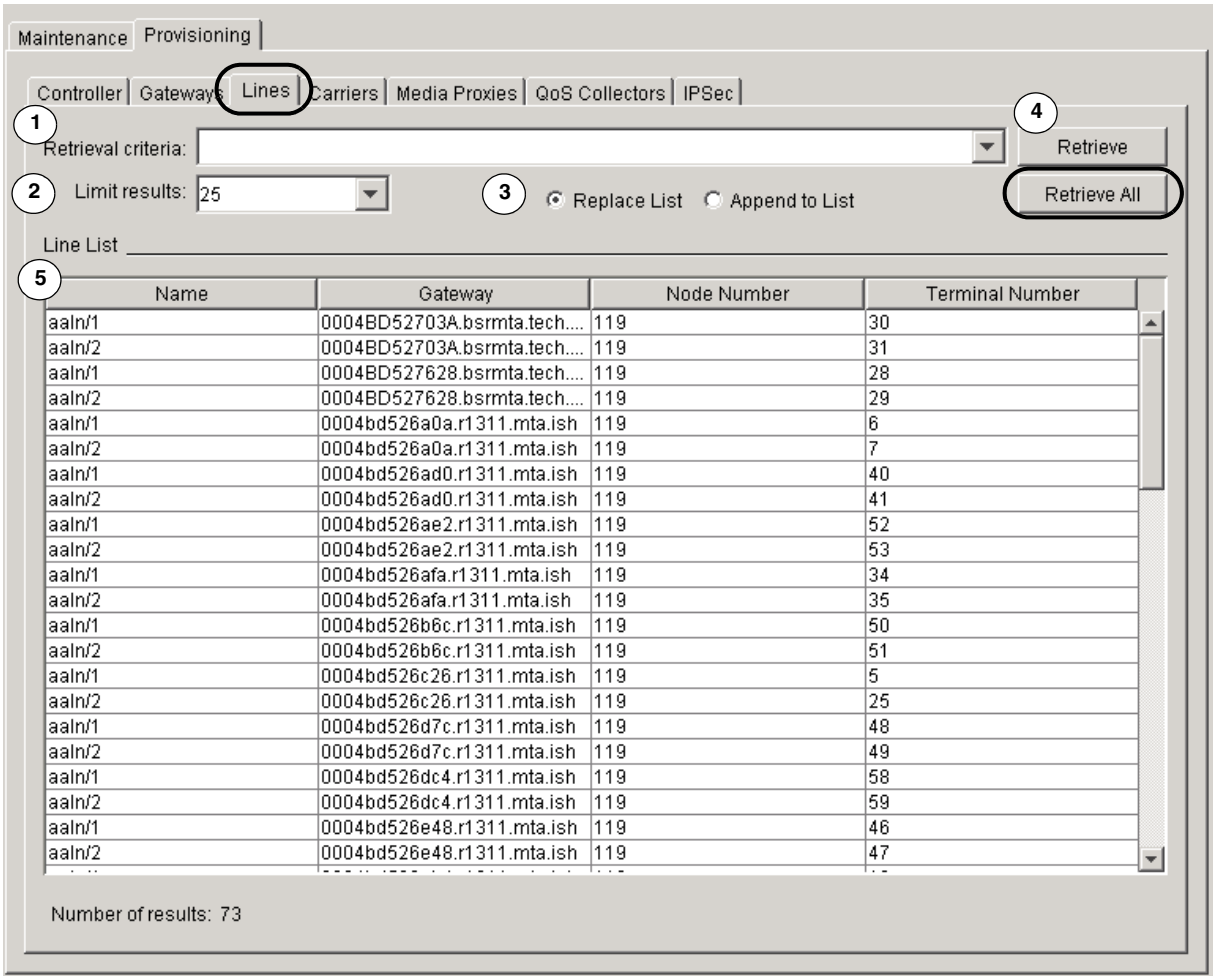
4 Click the **Controller** tab to view general node provisioning information for a selected GWC node.



5 Click the **Lines** tab.

6 Click the **Retrieve All** button tab to view all information related to line endpoints associated with the selected GWC node.

Note: Refer to the table Line endpoint search criteria functions on page 256 to review the numbered search functions.



7 Repeat this procedure as required to view line endpoints on other GWC nodes.

8 The procedure is complete.

The following table describes the line endpoint search criteria functions.

Line endpoint search criteria functions (Sheet 1 of 2)

Step	Menu component	Description
1	Retrieval criteria selection box and drop-down list	Enter a search criteria string in this field. Up to 20 search strings are saved during the user's session. Previous search strings can be recalled by selecting from the drop-down list. Refer to the table *Line endpoint search criteria examples* at the end of this procedure for more details about using search strings.
2	Limit results selection box and drop-down list	Select a value from the drop-down list. This value limits the number of matching entries returned in response to the query. Valid values include: 25, 50, 100, 250, 500, 1000 and "no limit". ***Note:*** The "no limit" value is still itself limited by the maximum number of entries currently downloadable, which is 4094.
3	Replace List radio button	Deselect this option if you do not want the query results to replace the existing data displayed in the table. The default selection is to replace the existing data.
	Append to List radio button	Select this option if you want the query results to be appended to the existing data displayed in the table.

Line endpoint search criteria functions (Sheet 2 of 2)

Step	Menu component	Description
4	Retrieve button	This selection retrieves data from the CS 2000 GWC Manager server database matching the specified search retrieval criteria. The data presented is a “snapshot” of the CS 2000 GWC Manager database based on the currently provisioned data. The view is not updated in real time. ***Note:*** Newly added or deleted data will not be added to or deleted from the displayed table view except when there is a deletion of endpoints. If an carrier endpoint is selected from the table and deleted using the Delete button, then the endpoint will be removed from the table if deletion was successful .
	Retrieve All button	This selection retrieves all the gateway or endpoint data, up to the maximum of 4094 entries. Values in the “Retrieval criteria” and “Limit results” are ignored.
5	Lines table	These are the tables where the search results are displayed. By clicking on a column header, you can sort the rows in ascending order, based on the values in that column. By clicking on the column header a second time, you can sort the rows in descending order. ***Note:*** The data is not preserved once another Gateway Controller node is selected; however, the retrieval criteria are maintained in the drop-down list so the same search can be re-executed.

Line endpoint search criteria examples

The search functionality is similar to that available in web search engines.

- One or more strings can be entered in the Retrieval Criteria, separated by space(s).
- Each string in the criteria is compared with the value in each column. If a match is found in any column, the record will be returned.
- Each string in the criteria is automatically wildcarded at the beginning and end of the string. (For example, the string "gate" will match "MYGATEWAY" and "GATEWAY1".)
- Two special characters are supported as modifiers: the plus "+" and minus "-" signs.

  The "+" plus character prefixed to the string (e.g. "+gate") means the value must match. The "-" character prefixed to the string (e.g. "-gate") means the value must not match.

  The "+" character is assumed, and therefore is not typically used.
- The search is not case sensitive. A string using "gate" will return records where the following strings are found: "MYGATEWAY", "MyGateway", or "mygateway".

Example Retrieval Criteria: "gate"

Expected Results: Returns all records where the string is found in any column. A match for the example string should only be found in the Gateway name column.

Example Retrieval Criteria: "ncs"

Expected Results. Returns all records where the string is found, in any column. A match for the example string could be found in the Protocol column.

Retrieval Criteria: "47.108.2 -ncs"

Expected Results: Returns all records where the string "47.108.2" is found in any column and the string "ncs" is not found. The search should return the records of gateways where the subnet equals "47.108.2" and the protocol is not “ncs”.

Retrieval Criteria: "47.108.2 -aspen"

Expected Results: Returns all records that don’t use aspen trunking protocol, where the string "47.108.2" is found in any column and the string "aspen" is not found. The search should return the records of gateways where the subnet equals "47.108.2" and the protocol is not “aspen”.

Change the service profile of a GWC node

Purpose of this procedure

Use this procedure to display the Gateway Controller (GWC) service profile currently provisioned for a specific GWC node and change the node's service profile without having to re-provision the node.

Note: Only the change options indicated in the table Supported Gateway Controller profile changes on page 260 are supported. No other GWC service profile changes can be made without re-provisioning the node.

When to use this procedure

Use this procedure when wish to do change a GWC profile without re-provisioning the node.

Prerequisites and guidelines

Prerequisites

You must first busy the GWC node services using the CS 2000 GWC Manager before changing the service profile of a GWC node. Refer to the procedure Busy a GWC node on page 513 to accomplish this task.

In addition, the following prerequisites apply to performing this procedure:

- If you are using this procedure to change an audio controller to one with an RMGC profile, before completing this procedure you must first complete procedure Add or change the RMGC default domain on page 63 to ensure that a valid default domain name is in the GWC Manager database.
- Refer to your solution level documentation for other network requirements before completing this procedure.
- All steps in this procedure must be completed in order for the change profile process to be successful.

Supported change options

ATTENTION

The APG functionality has been removed in the SN07 release. All GWC service profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, SIP_T_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. For more information, refer to the *Gateway Controller Basics* NTP, NN10189-111.

Refer to the following table to determine which gateway profiles can be changed.

Supported Gateway Controller profile changes

Change from	Change to
AUDIOCNTL	AUDCNTL_RMGC
AUDCNTLINTL	AUDCNTL_RMGCINTL
AUDCNTL_RMGC	AUDIOCNTL
AUDCNTL_RMGCINTL	AUDCNTLINTL

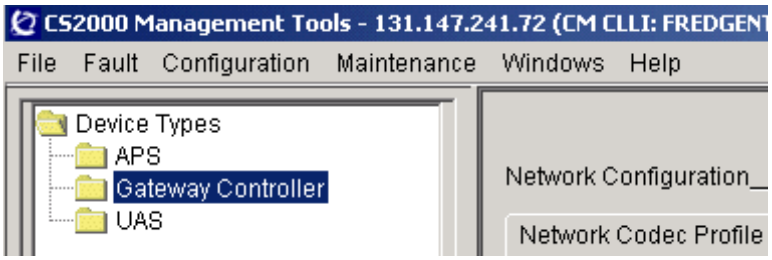
Note 1: No other change options are supported.

Note 2: This task cannot be performed using the OSSGate application.

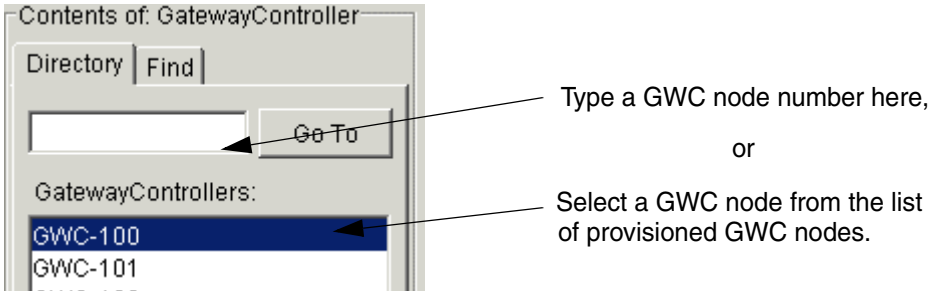
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



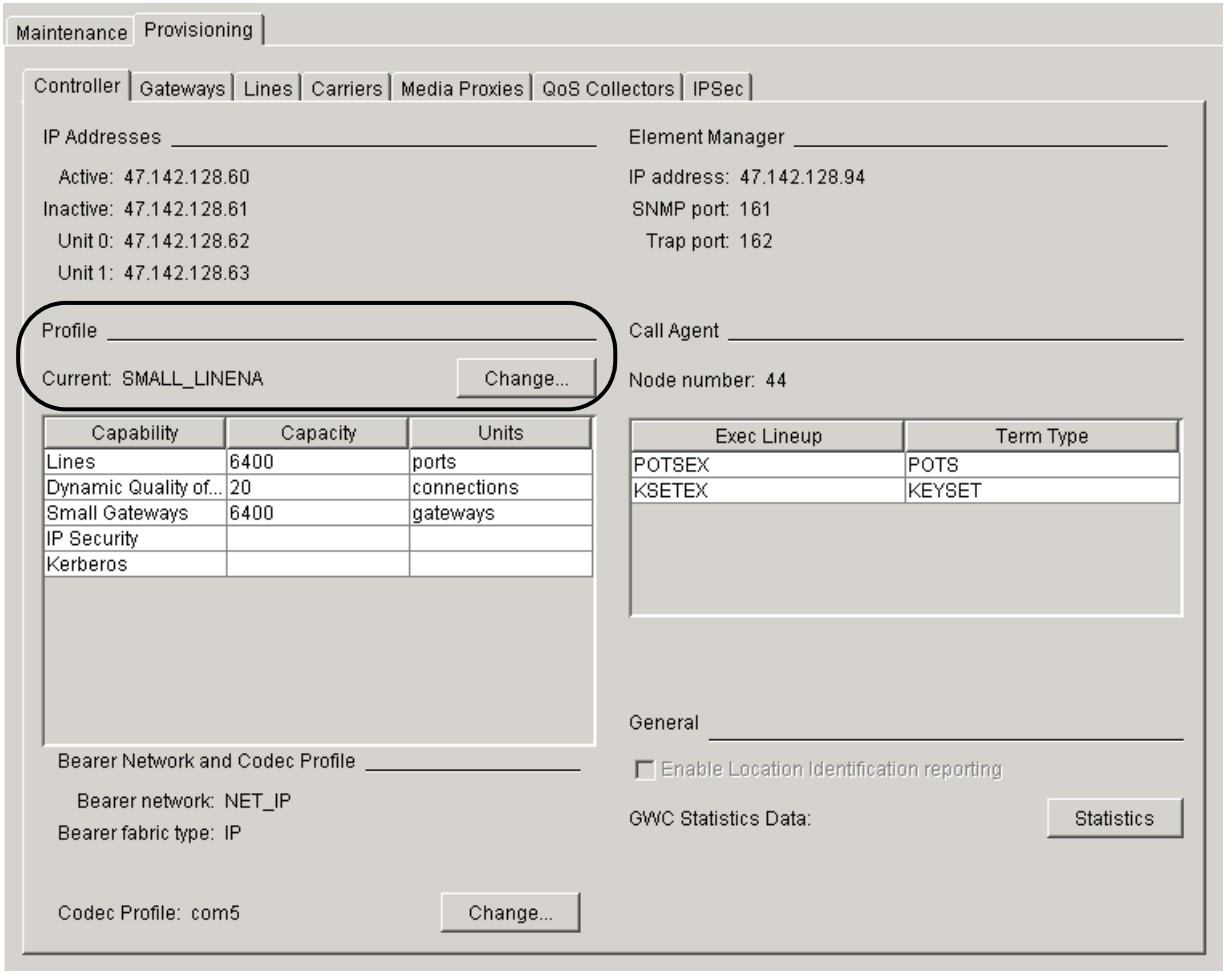
2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to change a profile for.



3 Click the **Provisioning** tab.

4 Click the **Controller** tab.

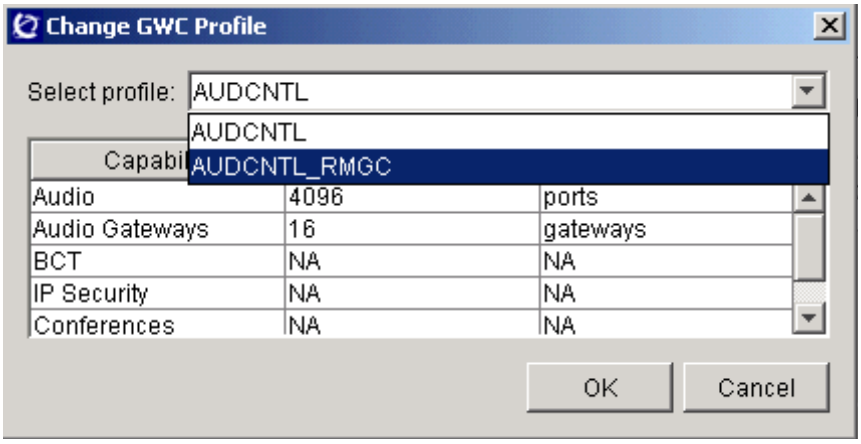
The **Profile** section displays the Gateway Controller profile for the node selected.



5 Click the **Change** button to display the Change GWC Profile dialog box

6 Select a new profile from the drop-down list.

The set of capabilities associated with the new profile is displayed.



Note 1: The system provides only those options to which you can change the current profile.

Note 2: The table Supported Gateway Controller profile changes on page 260 indicates which profiles can be changed.

7 Click the **OK** button to initiate the change.

Following the successful change, a dialog box is displayed to inform the user the GWC must be reloaded to enable the change. If the change request fails, a dialog is presented to the user containing a description of the failure reason.

8 Perform the following steps to complete the profile change:

a Busy the inactive unit. Follow procedure “Disable (Busy) GWC card services” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

b Lock the inactive unit. Follow procedure Lock a GWC card on page 519 in this NTP.

A data mismatch alarm is raised for this unit by the alarm manager. No action is required

c Unlock the inactive unit. Follow procedure Unlock a GWC card on page 523 in this NTP.

The card is booted and provisioning data is downloaded following the unlock operation.The data mismatch alarm condition is cleared for this unit.

d Return the inactive unit to service. Follow procedure “Enable (RTS) card GWC services” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

e Swact the GWC cards in the node. Follow procedure “Invoke a manual protection switch (warm swact)” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

f Repeat step a through step d for the mate GWC unit (now inactive) in the node.

9 The procedure is complete.

Add a certificate file for a third-party gateway

Purpose of this procedure

This procedure describes how to create and add to the system a certificate file - an XML file that defines a profile for a new third-party gateway. You can also create a new certificate (profile) if you wish to change some attributes of an existing gateway. For more information, refer to procedure Change gateway attributes on page 277.

CAUTION
Possible service disruption
Introducing and using a new gateway profile may cause some service disruptions if the certificate created for that profile has not been properly tested. If required, contact your next level of support.

Once a certificate file is defined and placed in the /ThirdPartyCertificates directory, it becomes available to be transferred to the Gateway profile name: drop-down list at the Associate Media Gateway dialog box. Every 5 minutes, the system checks the directory for any changes and updates the gateway profile list.

If the system detects any problems related to a certificate file, a CMT301 minor alarm is raised and the new certificate is not placed on the gateway profile list. To clear the alarm, you must correct the problem described in the alarm, then place the corrected file in the directory. During the next directory check, the system detects the new certificate and transfers it to the gateway profile list.

Note: For the description of the CMT301 alarm conditions, refer to log report CMT301 in the *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909

This procedure also describes how to remove an obsolete certificate file.

When to use this procedure

Use this procedure when you need to create a certificate file to define a new profile for the following third-party gateways:

- a new gateway that you wish to associate with a Gateway Controller (GWC)
- an existing gateway, for which you want to change some attributes.

Prerequisites and guidelines

The following prerequisites and guidelines apply to this procedure:

- The CS 2000 Management Tools server, GWC cards, and XA-Core must be upgraded to the SN08 load.
- Before starting this procedure, obtain the IP address of the CS 2000 Management Tools server.

  Note: Only the root user can perform this procedure.

- Make sure that you are familiar with all the fields in the certificate file. Refer to table Certificate file configuration fields on page 272 for the description of each field. Obtain the correct value for each field before starting the procedure. If necessary, contact your next level of support to obtain these values.
- If you want to change the profile currently assigned to a gateway, do not modify the certificate file associated with the profile. Instead, add a new certificate (profile) that will include the new attribute values, then execute Change Profile option from the Change Gateway dialog box. For more information, refer to procedure Change gateway attributes on page 277.

  Note: Changing a GW to a different profile is potentially a risky operation. Thorough interop testing must be performed before creating a certificate with the Compatible Profiles field set to a profile other than itself. While some error checking is performed, it is the responsibility of the certificate creator to make the final decisions whether one profile is truly compatible with another.

- If you want to remove a certificate, make sure that there are no gateways associated with the profile defined by this certificate.
- If the system detects any problems related to a certificate file (such as, incorrect format or an attempt to delete a certificate currently used by some gateways), a CMT301 minor alarm is raised. For detailed information, refer to the description of log report CMT301 in the *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

Action

At your workstation

1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the CS 2000 Management Tools server.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the certificates directory by typing

```
$ cd  /opt/nortel/NTsesm/properties/certificates/
```

and pressing the Enter key.

This directory contains the following sub-directories:

- /NortelCertificates
- /ThirdPartyCertificates

6

ATTENTION
Do not add, remove, or modify any files in the /NortelCertificates directory. However, you can use an existing file in the /NortelCertificates or /ThirdPartyCertificates directory as a template for your new certificate file.

If you wish to view the current list of certificates in one of the above sub-directories, complete the following sub-steps. Otherwise, continue with step 7.

a Access the directory that you want to view by typing

`$ cd <sub-directory>`

and pressing the Enter key.

where

sub-directory
is NortelCertificates or ThirdPartyCertificates

b List the existing certificates by typing

`$ ls`

and pressing the Enter key.

Example response:

```
$ ls
AFC.certificate
AMBIT_LINE_GW_16.certificate
AMS.certificate
ARRIS_TOUCHTONE_NN01_4.certificate
ARRIS_TOUCHTONE_NN02_4.certificate
ASKEY_LINE_GW_12.certificate
ASKEY_LINE_GW_30.certificate
ASKEY_LINE_GW_4.certificate
AUDIOCODES.certificate
```

Note: Each file name (without the extension ".certificate") reflects the gateway profile name listed in the Gateway profile name: drop-down menu at the Associate Media Gateway dialog box.

c Return to the previous directory by typing

`$ cd ..`

and pressing the Enter key.

7 Choose a certificate file most similar to the new one that you want to create and copy it (with a new name) to the /ThirdPartyCertificates directory by typing

$ cp ./<sub-directory>/<file_name> ./ThirdPartyCertificates/<new_file_name>

and pressing the Enter key.

where

sub-directory
is NortelCertificates or ThirdPartyCertificates

file_name
is an existing certificate file name that you are using as a template

new_file_name
is the new certificate file name, consisting of the upper-case new profile name and the lower-case extension ".certificate". For example, ABC_40.certificate.

Example
$ cp ./NortelCertificates/ASKEY_LINE_GW_12.certificate ./ThirdPartyCertificates/MY_NEW.certificate

Note 1: You must insert space after the <file_name>.

Note 2: Certificate names are not case sensitive, however, the recommendation is to use upper case (except for the extension). Once the certificate is imported into the system, it is listed in upper case. This is particularly important when registering a gateway using OSSGate application, when you must use the upper case name regardless of the certificate file name case.

Note 3: Certificate names must be unique (including the case) within both sub-directories. For example, if the ABC.certificate file exists in one of the certificate sub-directories, you cannot add a new ABC.certifcate or abc.certificate file to the ThirdPartyCertificates sub-directory. If the system detects duplicate names, an alarm is generated. For more information, refer to the description of log report CMT301 in the *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

8 Access the ThirdPartyCertificates directory by typing

```
$ cd ThirdPartyCertificates
```

and pressing the Enter key.

9 Open the newly added file using an available text editor. If you are using UNIX vi tool, type

```
$ vi <new_file_name>
```

and pressing the Enter key.

where

new_file_name
is the new certificate file name that you added in step 7

Example
Field names are listed in brackets (for example, <MaxEndpoints>) on both sides of the configuration value.

```
<certificate>

 <MaxEndpoints>30</MaxEndpoints>
 <Category>SMALL</Category>
 <EndpointType>managedLens</EndpointType>
 <GenerateLGRP>false</GenerateLGRP>
 <ResvTermMandatory>false</ResvTermMandatory>
 <ChangeIPAvailable>false</ChangeIPAvailable>
 <DispPhyLocation>false</DispPhyLocation>
 <InventoryType>Small Line Gateway</InventoryType>
 <InventoryRole>Media Gateway</InventoryRole>
 <SupportedProtocol>
  <protocolName>mgcp</protocolName>
  <version>1.0</version>
 </SupportedProtocol>
 <GWCProfileNumber>49</GWCProfileNumber>
 <EPIDGenDesc>manual</EPIDGenDesc>
 <ServiceTypeList>line</ServiceTypeList>
 <ServiceTypeList>ITRANS</ServiceTypeList>
 <CompatibleGWProfileList>ASKEY_LINE_GW_30</CompatibleGWProfileList>

 <GatewayNameFormatList>
  <nameFormat formatKey="GATEWAY.UE511" enabled="true">
      <delimiters>.</delimiters>
      <minLength>1</minLength>
      <maxLength>32</maxLength>
      <minTokens>1</minTokens>
      <maxTokens>16</maxTokens>
      <name>IAD Gateway</name>
```

10 Navigate your cursor to each field that you want to change for your new profile and replace the existing value with a new value.

Refer to table Certificate file configuration fields on page 272 for the description of each field.

11 When all the changes are complete, save the file making sure that no hidden characters (such as, ^M) are included in the document.

Every 5 minutes, the system checks the ThirdPartyCertificate directory and updates the Gateway profile name: drop-down list at the Associate Media Gateway dialog box.

If the system detects any problems with the certificate, a minor alarm is generated. To clear the alarm, change the content of the certificate file as described in log CMT301. For more information, refer to refer to the description of log report CMT301 in the *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909.

Use the following table to determine your next step.

If you	Do
need to change a certificate file currently not assigned to any gateway	repeat steps 9 to 11
need to change a certificate file currently assigned to a gateway, without creating a new certificate	contact your next level of support
need to remove a certificate file	go to step 12
do not need to make any further changes	go to step 15

12 Make sure that there are no gateways associated with the profile defined by this certificate. If necessary, complete one of the following steps:

- Remove all gateways that have the selected certificate (profile) assigned to them. If required, refer to procedure Disassociate a media gateway on page 305.
- Change the gateway profile to a different profile. Refer to procedure Change gateway attributes on page 277.

13 Access the ThirdPartyCertificates directory by typing

```
$ cd /opt/nortel/NTsesm/properties/certificates
    /ThirdPartyCertificates
```

and pressing the Enter key.

14 Remove the required certificate file by typing

```
$ rm <file_name>
```

and pressing the Enter key.

file_name
is the certificate file name that you want to remove

15 The procedure is complete.

Certificate file configuration fields

The following table lists certificate fields and values that define a gateway profile.

Certificate file configuration fields (Sheet 1 of 5)

Field	Description
<MaxEndpoints>	Defines the maximum number of the endpoints that can be added to a gateway. This value must be lower or equal to the maximum number of endpoints that can be assigned to a GWC with which this gateway will be associated.
<Category>	Defines endpoint lookup algorithms used in the GWC device. There are four available values: • SMALL - for gateways with small capacities (31 endpoints or less) • LARGE - for gateways with large capacities (more than 31 endpoints) • AUDIO - special category used with audio gateways. These gateways use pools of endpoints. • APG - special category used for APG gateways.

Certificate file configuration fields (Sheet 2 of 5)

Field	Description
<EndpointType>	Defines how endpoints are managed within Carrier Voice over IP products. This field affects the ability of a gateway to pre-provision endpoints and alters where and when endpoints are provisioned. Use one of the following values: • managedLens - line gateways with managed logical groups (LGRP) • ue9000Lens - UE9000 gateway unique processing • cicmLens - CICM gateway unique processing • carrierTrksGwcNN - trunk gateways, no LGRPs • carrierTrksSubNN - trunks gateways, no LGRPs • nocarrierTrkGwcNN - H.323 gateways • asynchronousBridg - ABI • thirdPartyLens - large line third-party gateway unique processing
<GenerateLGRP>	Indicates whether a new logical group (LGRP) is created when a gateway with this profile is associated. This field applies to line gateways that allow the system to manage TID allocation. Use one of the following values: • true - a gateway that is added will cause a new LGRP to be created. • false - the existing LGRPs that still have capacity will be used.
<ResvTerm Mandatory>	The value of "true" forces the user to specify a reserved terminations client value (at the Associate Media Gateway dialog box), instead of using the system default. Currently, only gateways that use the H.323 protocol need this restriction. For all other gateway types, this field is set to "false".
<ChangeIP Available>	Indicates whether the "Change gateway IP address" option is available at the Change Gateway dialog box. Currently, only H.323 gateways support this option. For all other gateways, this field is set to "false".
<DispPhyLocation>	Indicates whether additional fields describing the LGRP physical location should be datafilled when associating media gateway to a GWC. Currently, these fields apply to third-party large line and CICM profiles only. For all other gateways, this field should be set to "false".

Certificate file configuration fields (Sheet 3 of 5)

Field	Description
<InventoryType>	Similar to the EndPoint Type field, defines how endpoints are provisioned. Unique behavior is associated with each available value. The following values are available: • Large Trunk Gateway • H.323 Gateway • Audio Server • Large Line Gateway • Small Line Gateway • CICM • UE9000MG • Third Party
<InventoryRole>	Defines the expected use of a gateway. Currently, the only available value is "Media Gateway".
<Supported Protocol>	Defines protocol associated with the certificate (profile). Only one protocol can be associated with each certificate. If a gateway supports more than one protocol, a separate certificate must be created for each protocol. The following values are available for this field: • NCS_PROTOCOL • ASPEN • DSM-CC • MEGACO • MGCP • TGCP • H.323
<GWCProfile Number>	This field is used in the GWC device and it dictates the behavior of the GWC. Contact your next level of support to determine which number you must use.

Certificate file configuration fields (Sheet 4 of 5)

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><EPIDGenDesc></td><td>The EPID Generation field describes the behavior of endpoint groups that are expanded. It describes properties, such as using a "." (period) or "/" (slash) as naming delimiter. Refer to the following table for the endpointDesc mappings.
<table>
<tr><th>Element value</th><th>Delimiter</th><th>Channel start</th><th>Pad supported</th></tr>
<tr><td>manual</td><td></td><td>1</td><td>N</td></tr>
<tr><td>auto1</td><td>.</td><td>1</td><td>N</td></tr>
<tr><td>auto2</td><td>.</td><td>1</td><td>Y</td></tr>
<tr><td>auto3</td><td>/</td><td>1</td><td>N</td></tr>
<tr><td>auto4</td><td>/</td><td>1</td><td>Y</td></tr>
<tr><td>auto5</td><td>/</td><td>0</td><td>N</td></tr>
<tr><td>auto6</td><td>/</td><td>0</td><td>Y</td></tr>
<tr><td>auto7</td><td>.</td><td>0</td><td>N</td></tr>
<tr><td>auto8</td><td>.</td><td>0</td><td>Y</td></tr>
</table></td></tr>
<tr><td><ServiceTypeList></td><td>Defines the capabilities of the gateway. Some gateways can have multiple capabilities within the same list and have several values assigned to them. For example, a gateway can be a "line" type and have DQOS capability. The following values can be configured for this field:
• line
• trunk
• audio
• APG
• DQOS
• ITRANS
• H323
• ITRANS_ROAM</td></tr>
<tr><td><CompatibleGW ProfileList></td><td>Describes which profiles are compatible with the profile that you are defining. Enter the names of all profiles compatible with this profile (at minimum, the name of the profile being defined).</td></tr>
</table>

Certificate file configuration fields (Sheet 5 of 5)

Field	Description
<GatewayName FormatList>	Defines the syntax for the name of the gateway associated with this certificate (profile). Gateways that do not conform to this definition cannot be associated with a GWC.
<EndpointName Format>	Defines the syntax for the name of the endpoints added to a gateway associated with this certificate (profile). The system does not allow to add any endpoints that do not conform to this definition.

Change gateway attributes

Purpose of this procedure

Use this procedure to change attributes of a media gateway associated with a Gateway Controller (GWC) node. Some attributes can be changed without disassociating and reassociating gateways to a GWC node. The following attributes can be changed for one or more qualifying gateways:

- gateway IP discovery
- PEP (policy enforcement point) server
- application layer gateway (ALG)
- adjacent network zone
- root network zone
- gateway capacity
- gateway IP address and port number; applicable only to H.323 gateways that are behind an IP-VPN (NAT)-type network zone
- gateway profile

When to use this procedure

In general, use this procedure when you wish to change the attributes for a previously associated gateway without having to delete and re-add endpoints and disassociate and reassociate gateways. Specifically, use this procedure when you need to do the following tasks:

- Change the IP address or port number for a specific gateway (applicable only to H.323 gateways that are behind a NAT-type network zone).
- Decrease or increase a gateway's reserved port capacity.
- Insert a service zone in the network between the GWC and the gateway.
- Change the network service zone used by the GWC by changing the network address translator (NAT) device or limited bandwidth link (LBL) associated with the GWC.
- Change any of the root zones configured to interact with a Centrex IP Client Manager (CICM) gateway.
- Move a gateway to a different policy enforcement point (PEP) server in a cable network.
- Associate the gateway with a different ALG.
- Change the gateway profile assigned to the selected gateway.

Prerequisites and guidelines

You must first busy the GWC node services using the CS 2000 GWC Manager before changing gateway attributes. Refer to the procedure Busy a GWC node on page 513 to accomplish this task.

Only compatible gateway profiles support the change gateway profile option. All other attempts to change a profile are rejected by the system.

For any gateway that uses an associated middlebox or network zone, refer to the *ATM/IP Solution-level Configuration Management* NTP, NN10409-500, to determine if the middlebox or zone you are using has been configured with the appropriate bind, IP address and port to accommodate a change in IP or port addresses, or both.

When using this procedure to increase a gateway's endpoint capacity, refer to Table of media gateway profiles and characteristics on page 294 and observe the following guidelines:

- The gateway capacity cannot be changed to a value higher than the maximum capacity defined by the gateway profile. For example, if a gateway profile is defined to have a maximum capacity of 24, then the gateway capacity cannot be increased above this level (although it can be any number greater than 0 and less than or equal to this maximum).

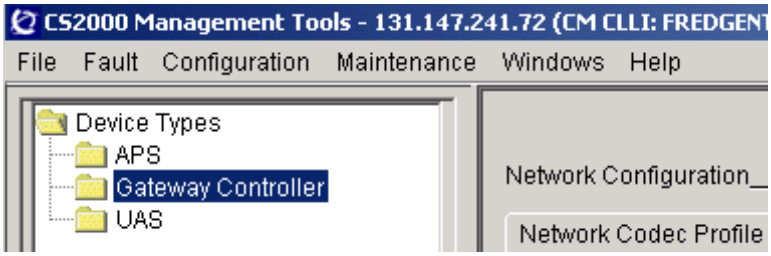
  Note: If you want to change the maximum capacity for the gateway, you must create a new profile (certificate), then perform the change gateway profile operation. For more information, refer to section Change the gateway profile on page 290.

- The capacity of the gateway cannot be changed to a value that results in overloading the total capacity of the GWC with which it is associated. Total GWC capacities can be viewed by clicking the **Provisioning** tab and then the **Controller** tab for a GWC and by reviewing the Profile section of this page. For example a change gateway capacity request is rejected if:
  - — a GWC is defined with profile "SMALL_LINENA" having a Lines capacity of 6400 ports
  - — the GWC already has enough gateways with reserved capacity that totals 6351, and the user attempts to increase an existing gateway's capacity by 50 lines or more.

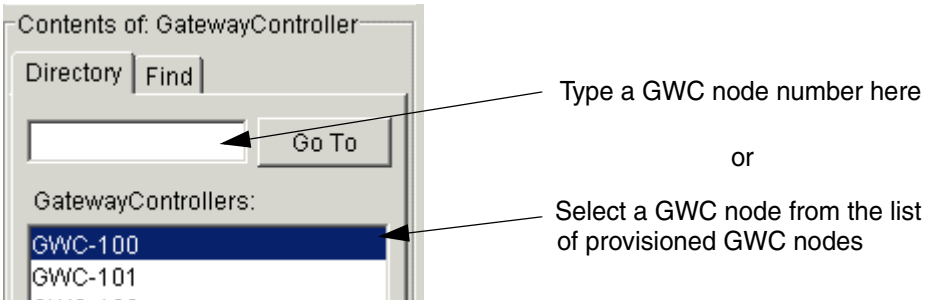
Action

At the CS 2000 GWC Manager client

1 At the CS2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree.



2 From the Contents of: Gateway Controller frame, select a GWC node.



3 Click the **Provisioning** tab.

4 Click the **Gateways** tab.

5 Refer to the following table to determine your next step:

If you wish to	Do
set gateways for IP discovery	go to step 6
perform any other *change* gateway operation	go to step 7

6 Perform the following set of steps to set gateway IP discovery for all gateways on the selected GWC node.

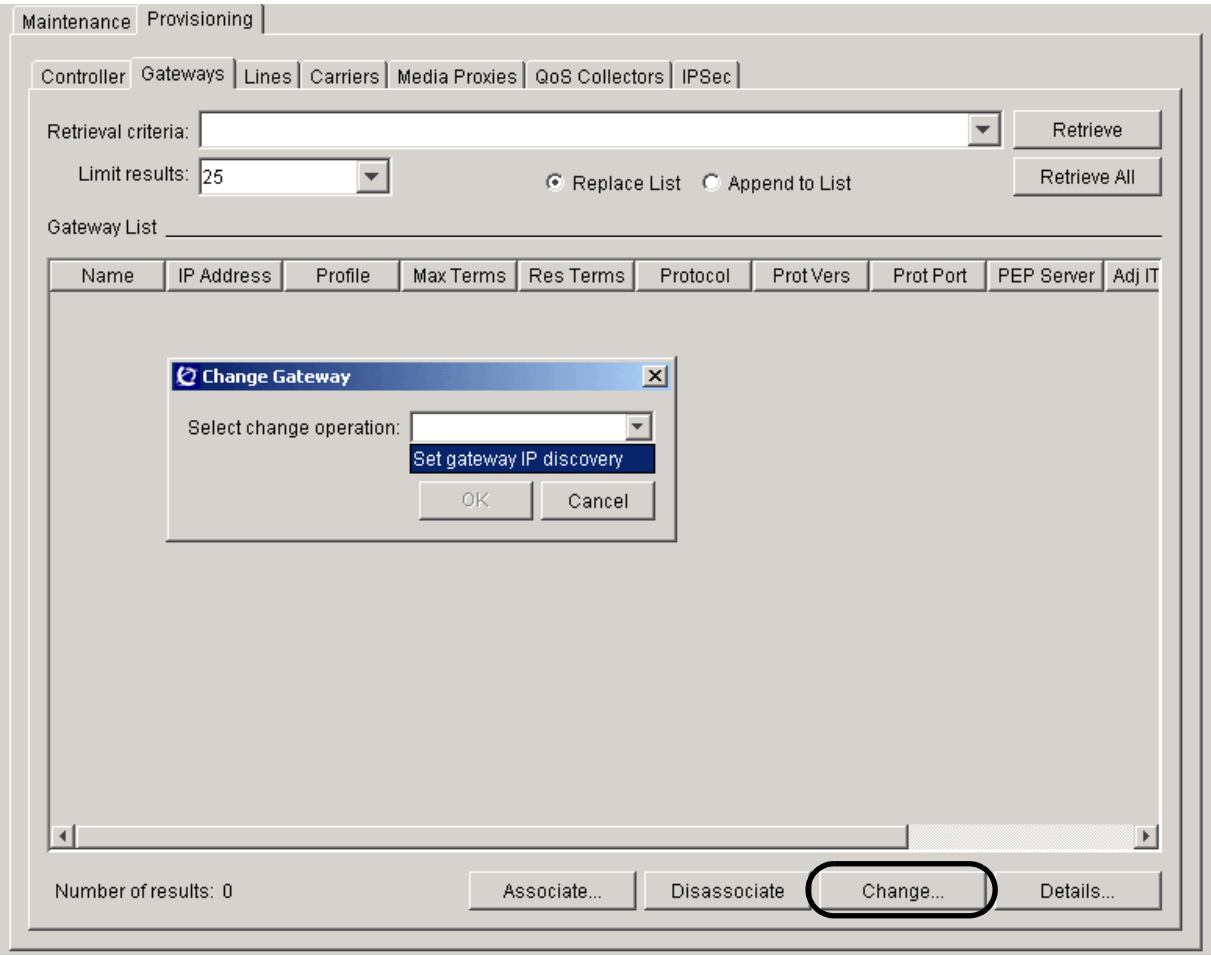
Note 1: IP discovery operates across all gateways on the GWC and cannot be applied to a single gateway.

Note 2: The IP discovery capability applies only to small gateways. To identify small gateways, refer to the Gateway Category column in Table of media gateway profiles and characteristics on page 294.

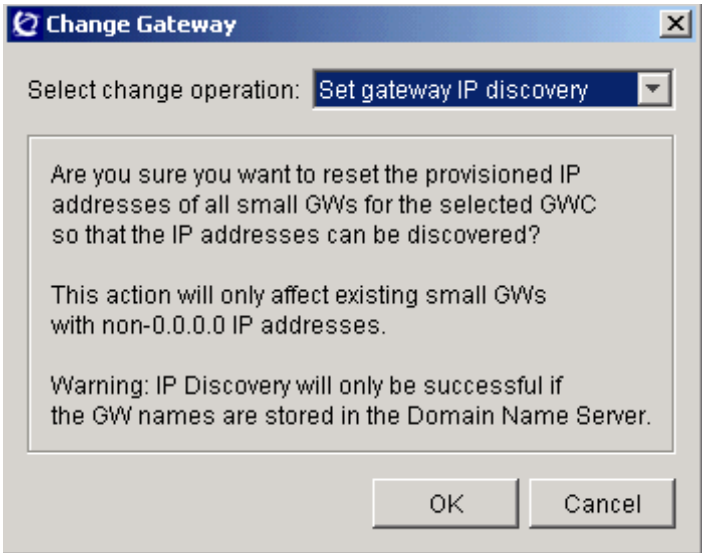
If necessary, refer to procedure View gateway provisioning data for a GWC node on page 245 to review details about fields in the gateways view.

a Click the **Change** button.

b From the drop-down menu, select **Set gateway IP discovery** and click **OK**.



This process will reset the IP addresses for all gateways associated with this GWC.



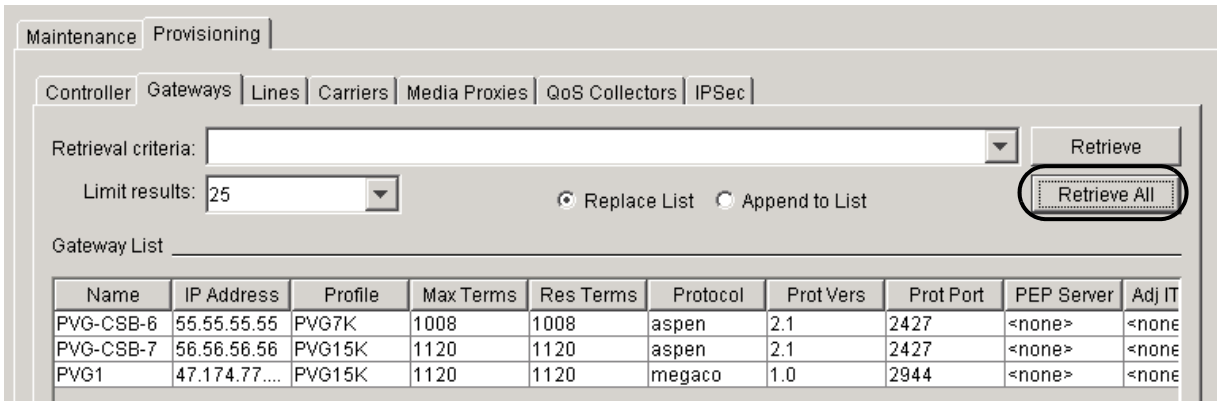
c Read the Change Gateway prompt, and click **OK** to proceed with the change.

d If prompted, click **OK** to confirm the change.

e Go to step 13.

7 Click the **Retrieve All** button to view information about all gateways currently associated with the selected GWC node.

Note: If necessary, refer to procedure View gateway provisioning data for a GWC node on page 245 to review details about the fields in the gateways view.



8 Select one or more gateways from the list.

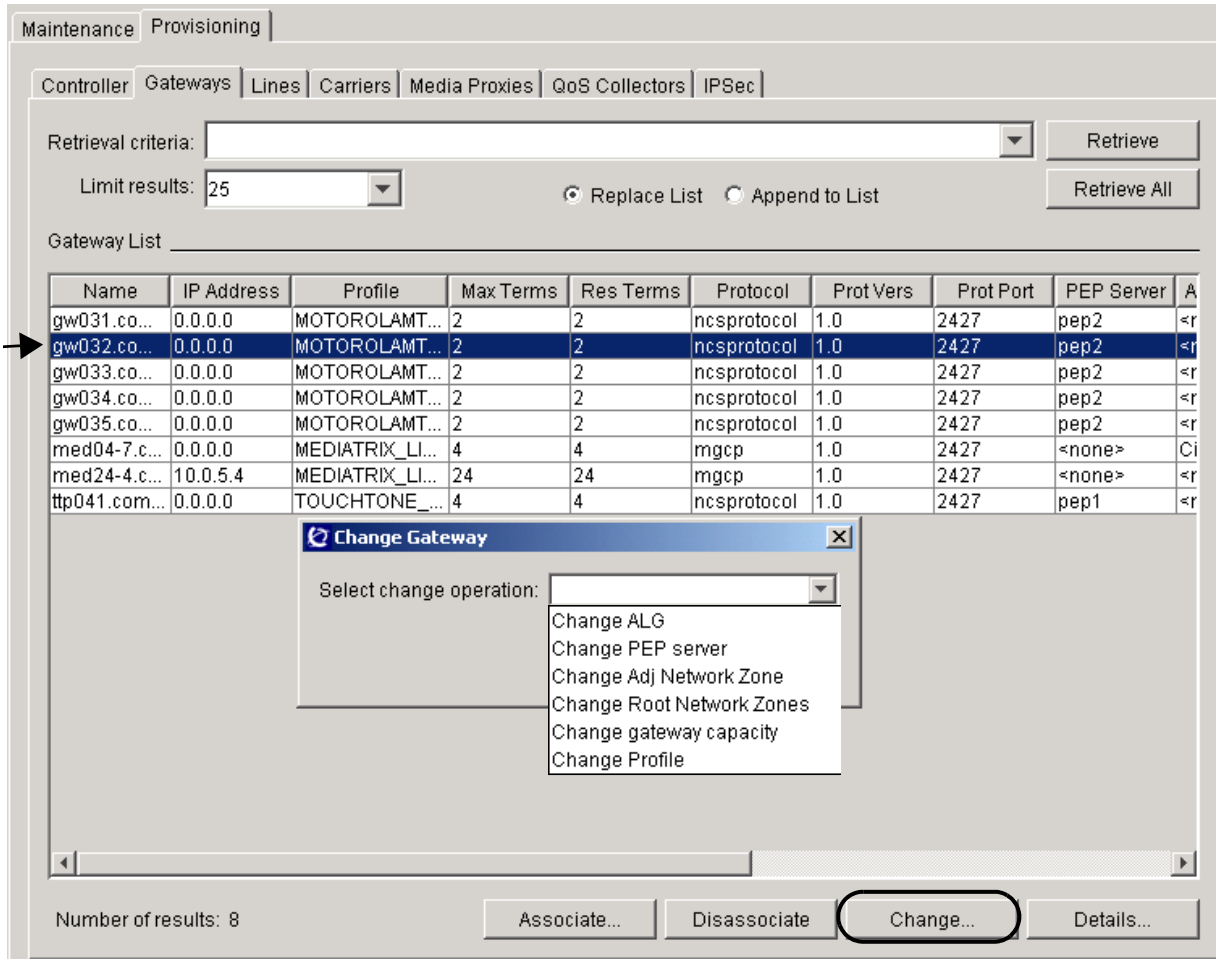
To select multiple gateways, hold down the Shift key and select each gateway entry.

Your selection is highlighted.

Note: You cannot select multiple gateways if you wish to change the IP address of the gateways. A gateway's IP address must be changed one at a time.

9 Click the **Change** button.

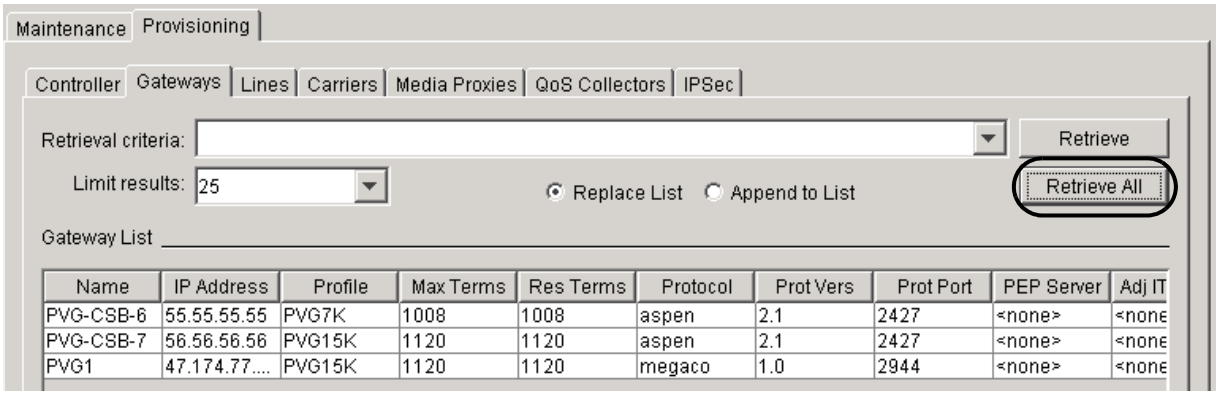
10 At the Change Gateway dialog box, select the attribute you wish to change from the drop-down menu.



11 Refer to the following table to determine your next step.

If you selected to change the	Do: go to section
ALG	Change the ALG on page 284
PEP server	Change the PEP server on page 285
adjacent network zone	Change the adjacent network zone on page 285
root network zone for a CICM gateway	Change the root network zones on page 287
gateway capacity	Change the gateway capacity on page 288
gateway IP address	Change the gateway IP address on page 289
gateway profile	Change the gateway profile on page 290

12 Click the **Retrieve All** button and verify the attribute changes you made to the gateway or gateways are shown in the Gateway List.



13 Refer to the following table to determine your next step.

If you	Do
need to make additional attribute changes to the same gateway or other gateways associated with this GWC node	return to step 5
need to make attribute changes to gateways associated with a different GWC node	return to step 2
are finished making attribute changes	go to step 14

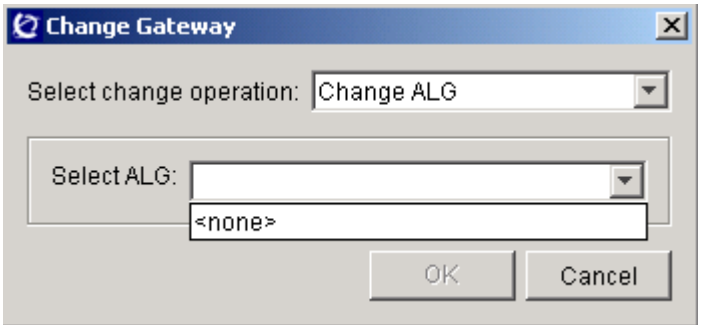
14 The procedure is complete.

Change the ALG

Complete the following steps to change the application layer gateway (ALG) associated with the selected gateway or gateways.

At the Change Gateway dialog box

1 Select the new ALG from the Select ALG: drop-down menu or select **<none>,** then click the **OK** button.



2 If prompted, click **OK** to confirm the change.

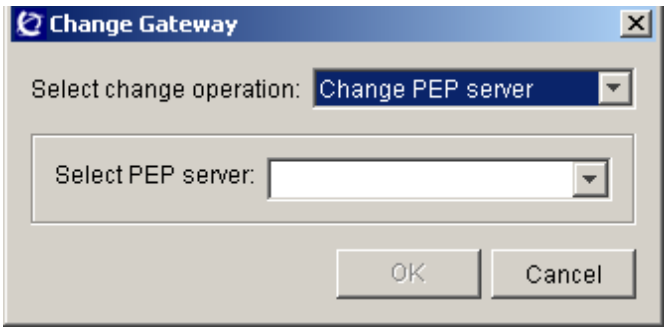
3 Return to step step 12.

Change the PEP server

Complete the following steps to change the PEP server associated with the selected gateway or gateways.

At the Change Gateway dialog box

1 Select a PEP server from the drop-down menu or select **<none>**, then click the **OK** button.



2 If prompted, click **OK** to confirm the change.

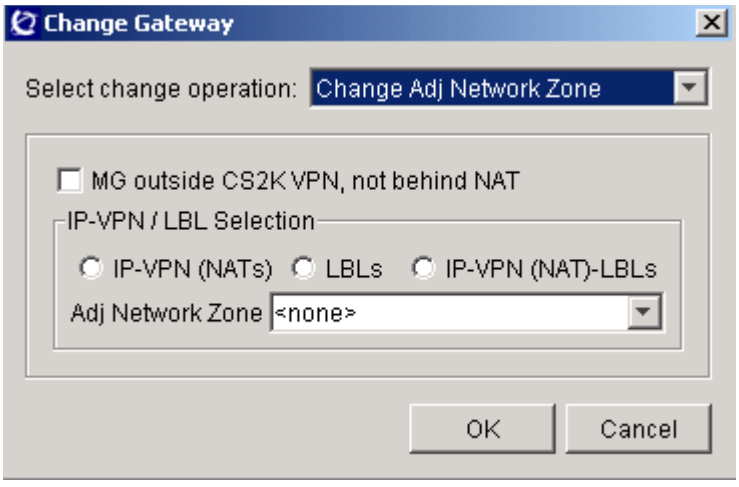
3 Return to step 12.

Change the adjacent network zone

Complete the following steps to change the adjacent network zone associated with the selected gateway or gateways.

At the Change Gateway dialog box

1 Use the following list to determine your selection.



- Select the check box provided if your gateway is outside the CS 2000 network (that is, the customer VPN).

- If the gateway is behind a network service zone in a private IP network or VPN, do not select the check box. Instead, select the name of a network zone in the Adj Network Zone text field.
  - — Select the radio button for IP-VPN (NATs), LBLs, or IP-VPN (NAT)-LBLs to restrict your search.
  - — Click in the Adj Network Zone field.
  - — If desired, type text characters of a zone name in the field to fine tune your display. The system displays all zones with a name that matches the characters you typed.
  - — Select adjacent network zone for the gateway from the list in the drop-down menu.

    Note 1: You can only select the zone names that are datafilled and appear in the Network Zones panel of the CS 2000 GWC Manager. Refer to procedure Review available network devices on page 99.

    Note 2: For an H.323 or any small line gateway configured with IP address other than 0.0.0.0, you cannot remove an adjacent network zone if the zone, or any member of topology chain towards the CS 2000 network core, is a NAT device. You must remove and reconfigure the entire gateway instead.

- If the gateway is not on the customer VPN and does not use a service zone, select the check box and leave the Adj Network Zone field empty.
- If no network service zone is being used and the gateway is on the customer VPN, then do not select the check box and do not select zone.

2 Click **OK** to confirm the changes.

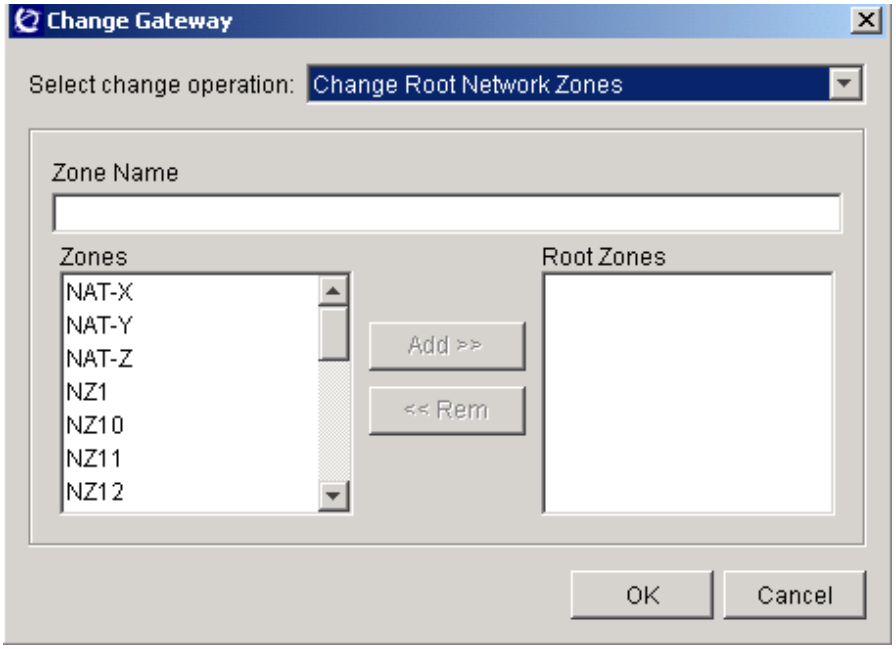
3 Return to step 12.

Change the root network zones

Complete the following steps to change any root network zones selected to interact with CICM gateways.

At the Change Gateway dialog box

1 Use the following list to determine your selection.



- You can remove a network service zone from the Root Zones list. Select a zone and click the **<< Rem** button.
- You can select a root network zone to interact with the gateway from the list of Zones.

  If desired, type text characters in the Zone Name field to display a specific group of network zones. The system displays all zones with a name that matches the characters you type.
- Click the **Add >>** button to add your selection to the list of Root Zones.
- Repeat the previous steps until you have completed your changes and have an updated list of root network zones.

  Note 1: To remove all root zones associated with a gateway, ensure there are no names remaining under the heading Root Zones.

  Note 2: A maximum of five root zones can be configured on a gateway.

2 Click **OK** to confirm the changes.

3 Return to step 12.

Change the gateway capacity

Complete the following steps to increase or decrease the endpoint capacity of the gateway.

Note 1: Changing the capacity of a gateway does not add carriers (endpoint groups) to the gateway or delete carriers from the gateway. Changing the capacity only affects the number of endpoints that can be provisioned on the gateway.

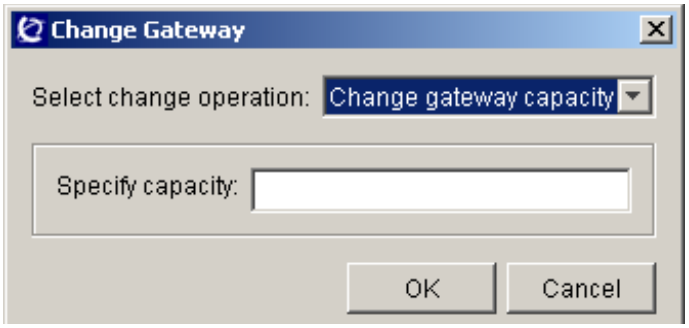
Note 2: You may decrease the capacity of a gateway provided if you change it to a value greater than or equal to the number of endpoints currently allocated.

If you wish to change the capacity to a value that is less than the number of endpoints provisioned, first remove carriers to reduce endpoint demand, and then change capacity of the gateway using this procedure. Remove carriers using procedure Delete carriers from a GWC on page 227.

Note 3: Starting in SN07, you can change the capacity of an H.323 gateway using the Change Gateway dialog box.

At the Change Gateway dialog box

1 Enter a new value for the gateway endpoint capacity and click **OK**.



2 If prompted, click **OK** to confirm the change.

Note 1: If you attempt to increase the endpoint capacity beyond what is available on the GWC, or beyond what is defined for the gateway profile, the request is rejected. Refer to Table of media gateway profiles and characteristics on page 294 to determine the endpoint capacity defined for a particular gateway.

Note 2: If are increasing the capacity of the gateway, you can then add carriers using procedure Add carriers to a GWC on page 201.

3 Return to step 12.

Change the gateway IP address

CAUTION
Partial service disruption
Changing the IP address or port number of a gateway will cause a temporary service outage on that gateway.

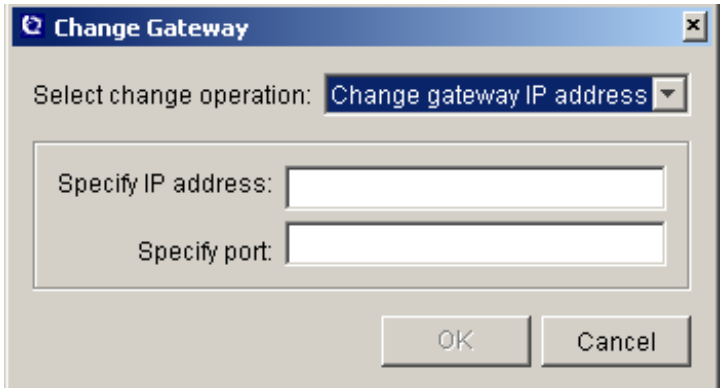
Complete the following steps to change a single gateway's IP address or port number, or both.

Note 1: Only H.323 gateways that are behind an IP-VPN (NAT)-type network zone support the ability to change an IP address and/or port value using this option.

Note 2: For any gateway that uses an associated NAT device, refer to the *Configuration Management* NTP applicable to your solution, to determine if the NAT device you are using has been configured with the appropriate bind, IP address and port to accommodate a change in IP and/or port addresses.

At the Change Gateway dialog box

1 Enter a new IP address or port number, or both and click **OK**.



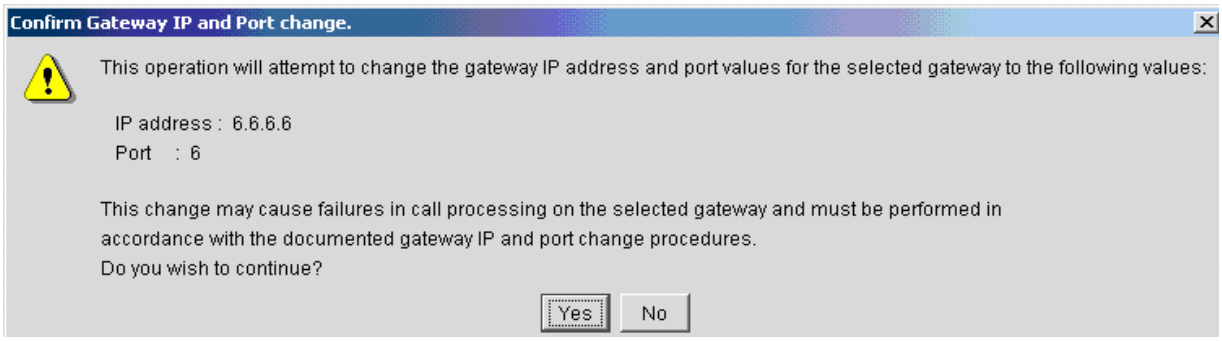
Note: If you intend to change only one of these values, you must type the current value (which you are not changing) in the other field.

Example
Your current IP address is 47.154.133.55 and your current

port setting is 4721. To change the port setting to 4800, type 47.154.133.55 in the Specify IP address field and type 4800 in the Specify port field.

2 When prompted, click **Yes** to confirm the change.

Note: If you enter the same IP and port address that is currently assigned to the gateway, an error message box will report the error and the change request will be ignored by the system.



3 Return to step 12.

Change the gateway profile

CAUTION
Possible service disruption
Changing profiles by introducing a new certificate, as described below, may cause some service disruptions if the new certificate has not been tested.

Changing a GW to a different profile is potentially a risky operation. Thorough interop testing must be performed before creating a certificate with the Compatible Profiles field set to a profile other than itself. While some error checking is performed, it is the responsibility of the certificate creator to make the final decisions whether one profile is truly compatible with another.

Complete the following steps to change a profile assigned to a gateway or gateways.

Use this functionality if you want to modify some of the gateway attributes defined by the currently assigned profile.

If a compatible profile with the appropriate attribute values does not exist, you can add a new profile by creating an appropriate certificate

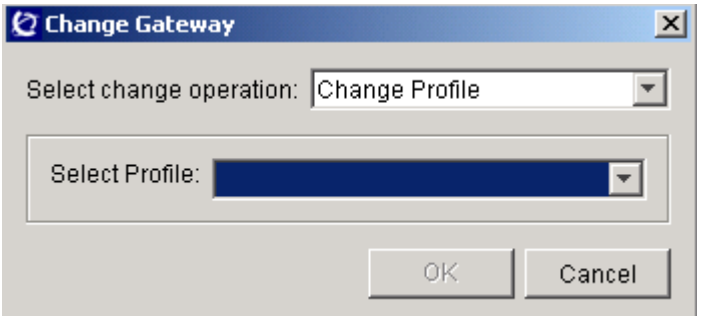
file, which will include the desired attribute values. You can change (with limitations) a profile assigned to a gateway with the following attributes having different values:

- a profile name
- the maximum number of endpoints
- endpoint name format
- supported protocol
- display physical location
- reserve terminal mandatory
- gateway name format
- compatible profiles

Note: Refer to procedure Add a certificate file for a third-party gateway on page 265 for detailed information on how to create, add, and remove a certificate file. If you want to remove a certificate, make sure that there are no gateways still using the profile defined by this certificate.

At the Change Gateway dialog box

1 From the Select Profile: drop-down menu, select the new profile that you want to associate with the selected gateway or gateways.



You can perform the change operation only between compatible profiles. Currently, only the following pairs of profiles are defined as compatible:

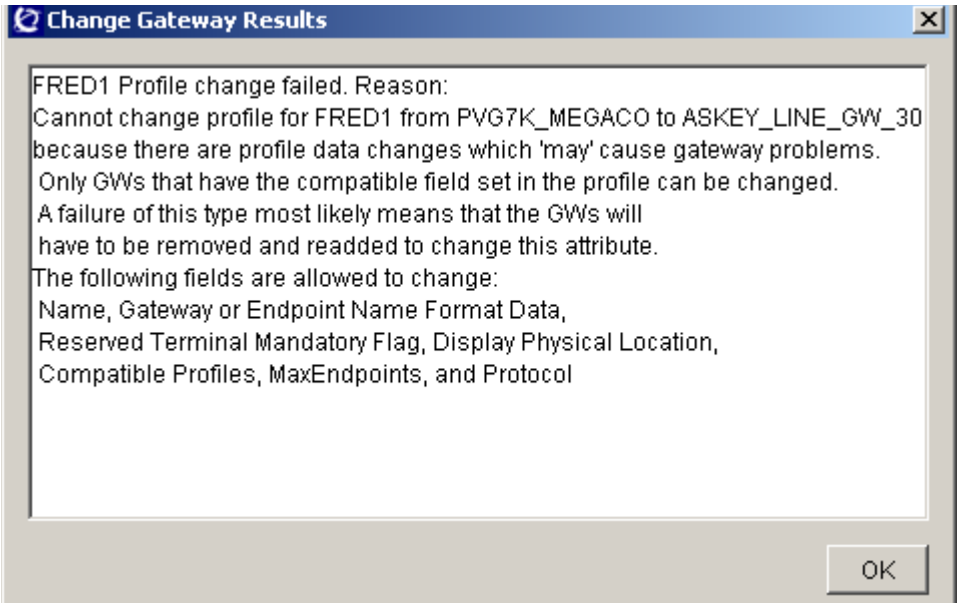
NUERA_GX_ASPEN	NUERA_GX_MEGACO
PVG_7K_ASPEN	PVG_7K_MEGACO
PVG_15K_ASPEN	PVG_15K_MEGACO
PVG_15K_1000_ASPEN	PVG_15K_1000_MEGACO
PVG_15K_PARTIAL_ASPEN	PVG_15K_PARTIAL_MEGACO
PVG_VSP3_ASPEN	PVG_VSP3_MEGACO
PVG_APG_VSP3_ASPEN	PVG_APG_VSP3_MEGACO
PVG_APG_ASPEN	PVG_APG_MEGACO

Note 1: The APG functionality has been removed in the SN07 release. All GWC service profiles and gateway profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, PVG_APG_ASPEN) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles.

Note 2: Refer to procedure Add a certificate file for a third-party gateway on page 265 for information on how to define a compatible profile in a certificate file.

2 Click the **OK** button.

Note: If you attempt to change the gateway to a non-compatible profile, the operation fails and the system displays the following error message. If required, contact your next level of support.



3 Return to step 12.

Media gateway profiles

The following table contains information about the different profiles supported on a Gateway Controller. Some profiles support multiple gateways. Contact your Nortel Networks account prime for the gateways supported using a profile.

Note 1: Newly supported gateways may be added to the list and are not shown in this table.

Note 2: In SN08, the SN06_CICM profile is present in the GWC Manager GUI, but it is not supported.

Table of media gateway profiles and characteristics (Sheet 1 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Maximum Port/Endpoint Capacity
Anchor packet gateways - profiles obsolete in the SN07 release						
PVG_APG_ASPEN	APG	ASPEN	2.1	2427		1120
PVG_APG_MEGACO	APG	MEGACO	1.0	2944		1120
PVG_APG_VSP3_ASPEN	APG	ASPEN	2.1	2427	APG	2016
PVG_APG_VSP3 _MEGACO	APG	MEGACO	1.0	2944	APG	2016
Note: The APG functionality has been removed in the SN07 release. The above profiles are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles.						
Audio gateways						
UAS (includes Nortel Media Server 2000 Series)	Audio	MEGACO	1.0	2944	Audio	n/a
AMS	Audio	MEGACO	1.0	2944	Audio	120
Note: Media Server 2010 gateways associated with the AMS (audiocodes media server) profile supply the Packet Media Anchor functionality, which replaces the APG device.						
H.323 gateways (See Note 1 and Note 2)						
CISCO_2600	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_3600	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_AS5300	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_H323_IOS	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
H323_PROXY	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)

Table of media gateway profiles and characteristics (Sheet 2 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Maximum Port/Endpoint Capacity
NORTEL_BCM	large	H.323	4.0	n/a	H.323, ITRANS	1032 (Intl) 1024 (Intl)
SUCCESSION_1000	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl)
WESTELL	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl))
Line gateways (wireline market)						
AFC	Large	MEGACO	1.0	2944	Line	1023
AMBIT_LINE_GW _16	Small	MGCP	1.0	2427	Line, ITRANS	16
ASKEY_LINE_GW_4	Small	MGCP	1.0	2427	Line, ITRANS	4
ASKEY_LINE_GW _12	Small	MGCP	1.0	2427	Line, ITRANS	12
ASKEY_LINE_GW _30	Small	MGCP	1.0	2427	Line, ITRANS	30
CICM	Large	MEGACO	1.0	2944	Line, ITRANS _ROAM	1024
MEDIATRIX_GW_4	Small	MGCP	1.0	2427	Line, ITRANS	4
MEDIATRIX_GW_24	Small	MGCP	1.0	2427	Line, ITRANS	24
MGCP_IAD_40	Small	MGCP	1.0	2427	Line, ITRANS	40
MGCP_LINE_GW_1	Small	MGCP	1.0	2427	Line, ITRANS	1
Line gateways (cable market)						
ARRIS_TOUCHTONE _NN01_4	Small	NCS	1.0	2427	Line, DQoS	4
ARRIS_TOUCHTONE _NN02_4	Small	NCS	1.0	2427	Line, DQoS	4

Table of media gateway profiles and characteristics (Sheet 3 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Maximum Port/Endpoint Capacity
DOMAIN_NAME	Small	NCS	1.0	2427	Line, DQos	1
Note: The DOMAIN_NAME profile provides the capability to configure a common domain name for all MTA gateways associated with the selected GWC. For more information, refer to procedure "Configure the domain name for MTA gateways (cable market) in the *Gateway Controller Configuration Management* NTP, NN10205-511.						
MOTOROLA MTA_1	Small	NCS	1.0	2427	Line, DQoS	1
MOTOROLA MTA_2	Small	NCS	1.0	2427	Line, DQoS	2
MOTOROLA MTA_4	Small	NCS	1.0	2427	Line, DQoS	4
TOUCHTONE_NN01_1	Small	NCS	1.0	2427	Line, DQoS	1
TOUCHTONE_NN01_2	Small	NCS	1.0	2427	Line, DQoS	2
TOUCHTONE_NN01_3	Small	NCS	1.0	2427	Line, DQoS	3
TOUCHTONE _NN0_4	Small	NCS	1.0	2427	Line, DQoS	4
Trunk gateways						
AUDIOCODES (Nortel Media Gateway 3200)	Large	MEGACO	1.0	2944	Trunk	280
CVX1800_2688	Large	DSM-CC	5.2	13818	Trunk	2688
CVX600_612	Large	DSM-CC	5.2	13818	Trunk	612
NUERA_BTX4K	Large	TGCP	1.0	2427	Trunk	4032
NUERA_GX_ASPEN	Large	ASPEN	2.1	2427	Trunk	2108
NUERA_GX_MEGACO	Large	MEGACO	1.0	2944	Trunk	2108
PVG7K_ASPEN	Large	ASPEN	2.1	2427	Trunk	1008
PVG7K_MEGACO	Large	MEGACO	1.0	2944	Trunk	1008
PVG15K_ASPEN	Large	ASPEN	2.1	2427	Trunk	1120

Table of media gateway profiles and characteristics (Sheet 4 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Maximum Port/Endpoint Capacity
PVG15K_MEGACO	Large	MEGACO	1.0	2944	Trunk	1120
PVG15K_1000_ASPEN	Large	ASPEN	2.1	2427	Trunk	1000
PVG15K_1000_MEGACO	Large	MEGACO	1.0	2944	Trunk	1000
PVG15K_PARTIAL _ASPEN	Large	ASPEN	2.1	2427	Trunk	624
PVG15K_PARTIAL _MEGACO	Large	MEGACO	1.0	2944	Trunk	624
PVG_VSP3_ASPEN	Large	ASPEN	2.1	2427	Trunk	2016
PVG_VSP3_MEGACO	Large	MEGACO	1.0	2944	Trunk	2016
TGCP	Large	TGCP	1.0	2427	Trunk	4032

Note 1: When associating an H.323 gateway with a GWC, the protocol port must be set as follows:

- Use a value of **0** for auto-discovery. This enables the system to discover the protocol port when the gateway registers. Use this value for all CISCO profiles and for H.323_PROXY.

  or

- Use the specific port value of the static bind that has been configured on the NAT for the H.323 gateway. Do not use the port value of 1719.

  or

- Use a value of 1720 to enable an operation mode in which no registration, admission, and status (RAS) messages are exchanged between a gateway and a GWC (RAS-less mode). This functionality applies only to H.323 gateways without NAT or with a NAT configuration of 1:1, in Carrier Hosted Services (CHS) solutions only. A 1:1 (one to one) NAT configuration means that a NAT is configured to translate an IP address only and each gateway uses one and only one IP address.

Note 2: For H.323 gateways, the endpoint capacity indicated is a recommended value based on the GWC capacity. The actual endpoint capacity supported depends on the details of your specific installation. For the H.323 profiles listed above, refer to the corresponding product documentation to determine the recommended endpoint maximum supported on a specific gateway.

Change the network codec profile for a GWC node

Purpose of this procedure

Use this procedure to change the network codec profile configured on a Gateway Controller (GWC) node.

When to use this procedure

Use this procedure when you need to change the codec profile assigned to a GWC node.

Prerequisites and guidelines

The following prerequisite applies to this procedure.

In order to change a network codec profile, you must have already configured more than one profile for a single bearer network type (IP, AAL1, or AAL2). To view available codec profiles, refer to procedure View a network codec profile on page 31. To add a new profile, refer to procedure Add a network codec profile on page 19.

The following guidelines apply to this procedure:

- You can change the specific network codec profile supported, but any new profile must use the same bearer network type as the codec you were using.

  Note: Only one bearer network type can be selected for a GWC node.

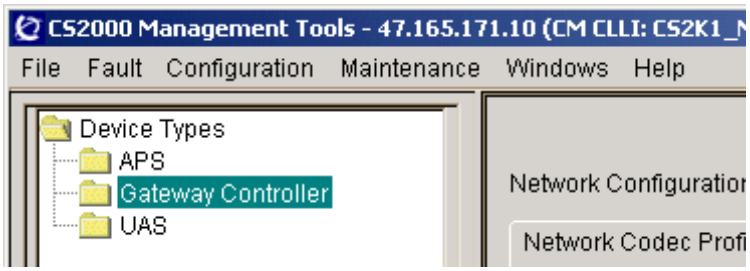
- If you wish to change the bearer network type assigned to a GWC node, refer to the general procedure Re-configure a GWC node in the network on page 10.
- If one card in the GWC node is out of service, you will need to reboot the card to load the new profile on that card. If both cards are out of service, you will need to reboot both cards in the node to load the new profile.

  Refer to this procedure for details.

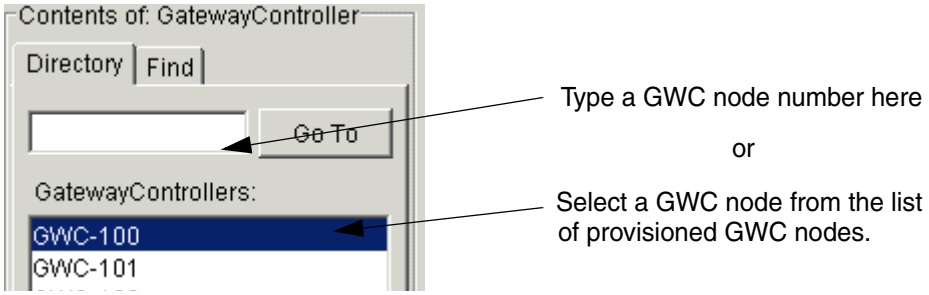
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node for which you wish to change a codec profile.



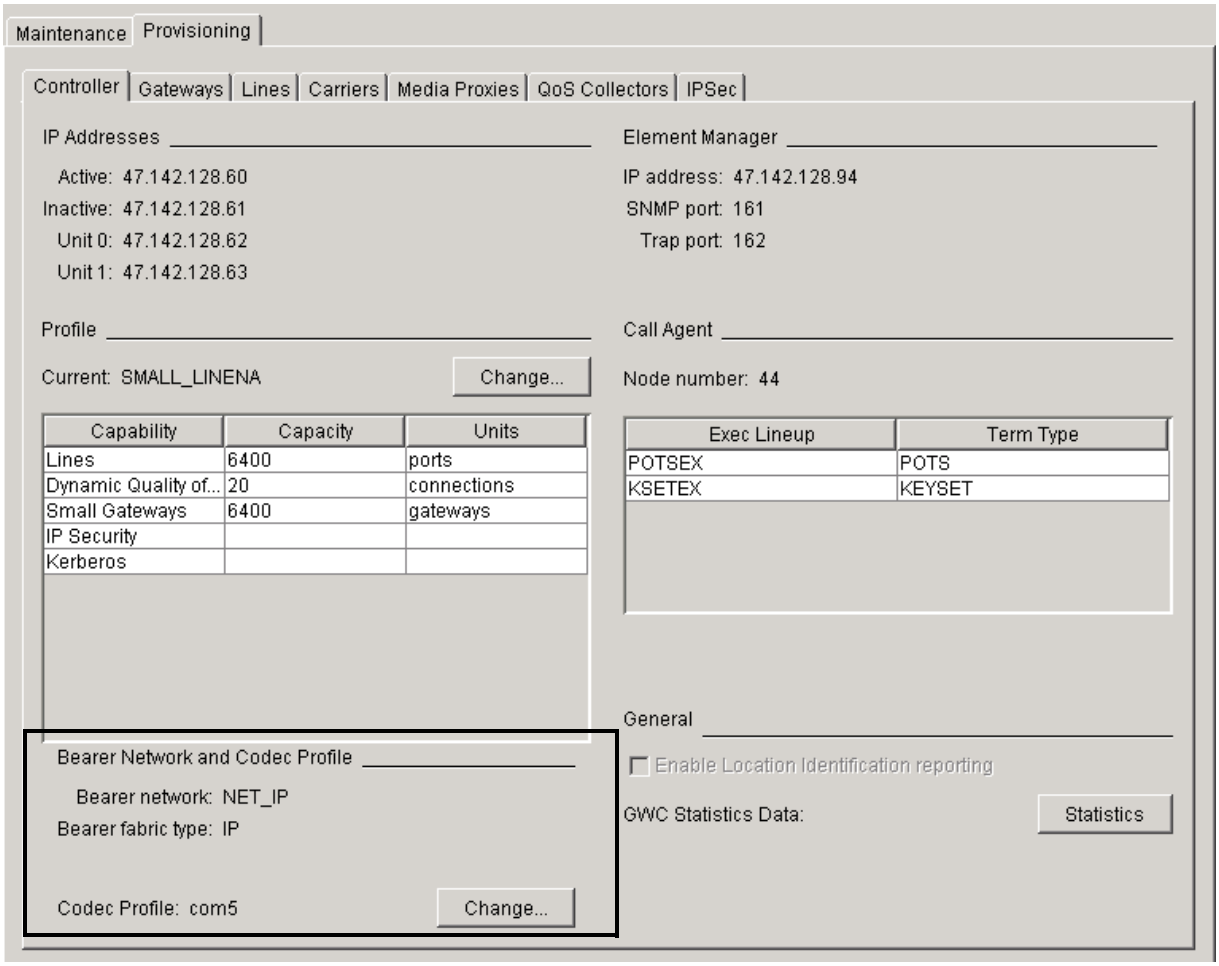
3 Click the **Provisioning** tab.

4 Click the **Controller** tab (if necessary) to display provisioning information for the GWC node.

Locate the Bearer Network and Codec Profile pane at the bottom of the screen.

Note that the following items are displayed for the GWC node selected:

- Bearer network
- Bearer fabric type
- Codec profile

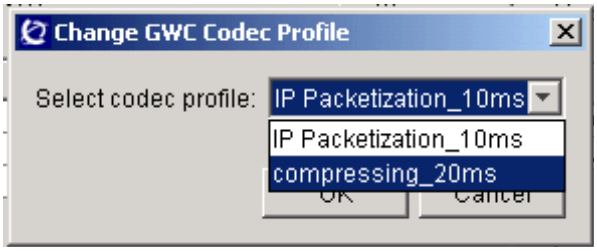


5 Click the **Change** button in the Bearer Network and Codec Profile pane.

The Change GWC Codec Profile dialog box is displayed.

6 Select a new codec profile using the drop-down menu.

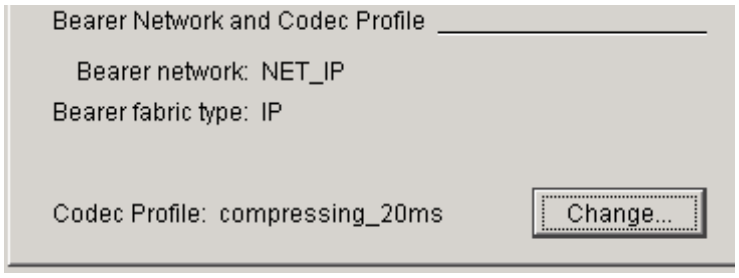
Only the codec profiles for the network bearer type selected will be available. The profile currently selected will not appear in the list.



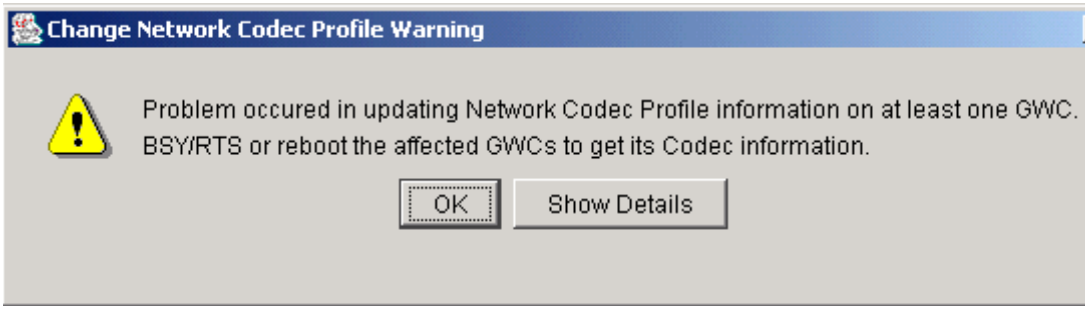
7 Click the **OK** button to make the change.

8 Click **Yes** at the Confirm Codec Profile Change prompt.

If both cards are in service, the new codec profile is changed on your GWC node. Observe that the new profile is displayed in the Bearer Network and Codec Profile pane.



9 If one card in the GWC node is out of service, or if both cards are out of service, the following message will be displayed:



Perform the following steps to ensure that both cards in the node load the new codec profile.

Note: If only one card in the node is out of service, perform step a through step d (inclusive) on that card to load the new profile. You may omit the remaining steps.

a Busy the inactive unit. Follow procedure “Disable (Busy) GWC card services” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

b Lock the inactive unit. Follow procedure Lock a GWC card on page 519 in this NTP.

A data mismatch alarm is raised for this unit by the CS 2000 GWC Manager alarm manager. No action is required.

c Unlock the inactive unit. Follow procedure Unlock a GWC card on page 523 in this NTP. The card is booted and provisioning data is downloaded following the unlock operation.

The data mismatch alarm condition is cleared for this unit.

d Return the inactive unit to service. Follow procedure “Enable (RTS) card GWC services” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

e Swact the GWC cards in the node. Follow procedure “Invoke a manual protection switch (warm swact)” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

f Repeat step a through step d for the mate GWC unit (now inactive) in the node.

Note: Both cards in the GWC node are now using the new codec profile.

10 The procedure is complete.

Disassociate a media gateway

Purpose of this procedure

Use this procedure to remove (disassociate) any type of gateway resource from a selected GWC node.

Note: Starting in SN07, H.323 gateway carriers (endpoint groups) must be removed manually before disassociating an H.323 gateway from a GWC node.

Carriers for all other gateway types must also be removed manually.

When to use this procedure

Use this procedure when it is necessary to reallocate gateway resources to a different GWC node or if you wish to re-configure the GWC node to use a different gateway type.

Prerequisites and guidelines

Ensure that you perform the following steps before disassociating a media gateway:

1. Place all endpoints on a gateway in a state of Installation Busy (INB):

   To place trunk groups on the XA-Core in a state of INB refer to procedure “Performing trunk maintenance using the Trunk Maintenance Manager" in the *ATM/IP Solution-level Fault Management* NTP, NN10408-900.

   Note: Endpoints may also be in a state of UNKNOWN (core datafill is missing).

2. Remove all carriers (endpoint groups) from the selected gateway. Refer to procedure Delete carriers from a GWC on page 227.

Note: If you remove datafill for a gateway using the CS 2000 GWC Manager and you leave the corresponding datafill for the gateway on the XA-Core, a mismatch will occur between the two databases. This mismatch may not be detected by a database audit.

To remove datafill for trunks in the XA-Core, refer to procedure "Deleting trunks" in the *CS 2000 Configuration Management* NTP for your solution.

CAUTION

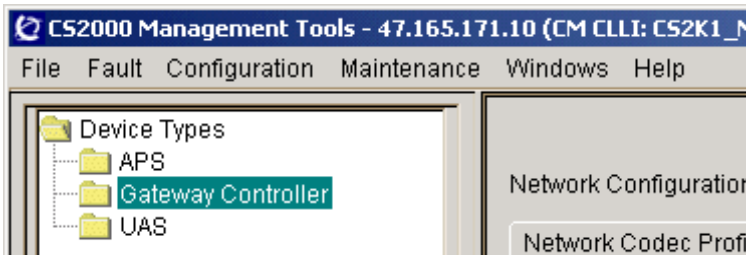
Before a gateway can be deleted, it is important to avoid taking down active calls by verifying that the gateway is not currently in use.

All associated trunks or lines should be in an installations busy (INB) state out to ensure that no calls can originate during the deletion process. Failure to do this may result in the system denying the delete request.

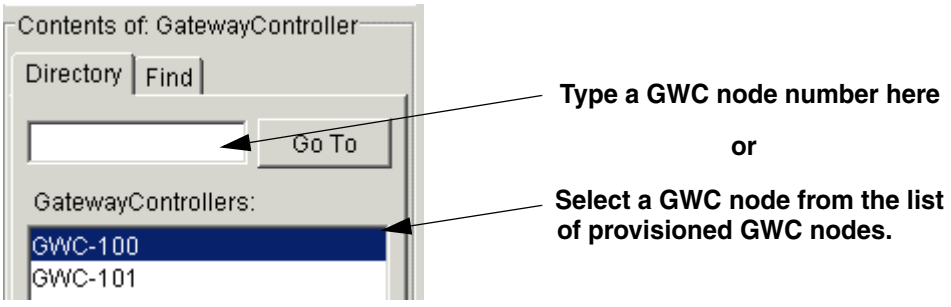
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.

4 Click the **Gateways** tab to view information about the gateways associated with the selected GWC.

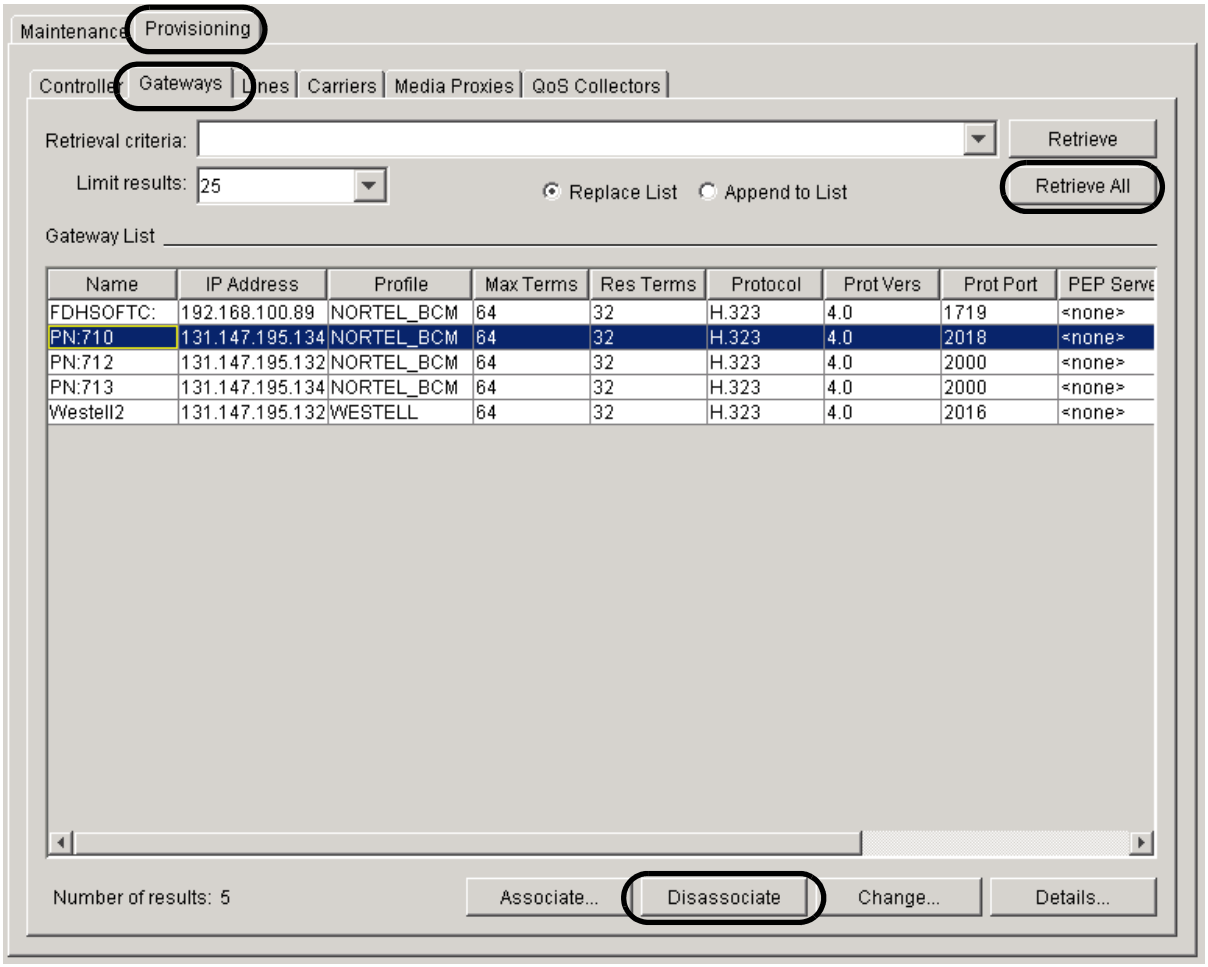
5 Click the **Retrieve All** button to view a complete list of gateways associated with the GWC.

6 From the Gateway List, select the gateway you wish to disassociate.

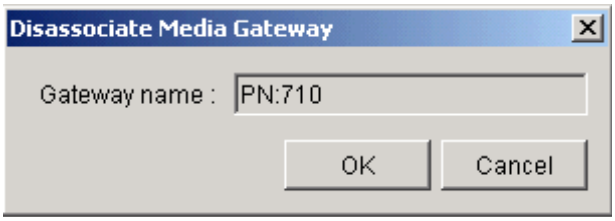
The gateway is highlighted.

Note: You can only delete one gateway at a time.

7 Click the **Disassociate** button at the bottom of the screen.



8 The name of the gateway you wish to disassociate is displayed.



9 Click the **OK** button to confirm the deletion.

The system may take a few moments to process the request.

A dialog box indicates if the gateway deletion is successful.

Note: If the deletion fails, click the **Show Details** button in the response dialog box to display the reason for the failure.

10 At the top of the screen, click the **Windows** menu and select **Refresh GWC Status** to update the Contents of Gateway Controller view to reflect any changes made.

11 If necessary, repeat this procedure to disassociate other gateways.

12 The procedure is complete.

Delete a GWC node

Purpose of this procedure

Use this procedure to remove a GWC node from the CS 2000 GWC Manager database.

When to use this procedure

Use this procedure when you need to remove a GWC node from the CS 2000 GWC Manager database. You can do this to permanently remove a GWC node or to re-provision the node.

Prerequisites and guidelines

The following activities must be completed before deleting a GWC node:

- Ensure that all endpoints have been removed for the selected gateways associated with the GWC node.

  Refer to procedure Delete carriers from a GWC on page 227 in this NTP for instructions on removing carrier endpoints from a gateway.

  Refer to the *CS 2000 Configuration Management* NTP applicable to your solution for instructions on removing line endpoints from a gateway.

- Ensure the GWC node you wish to delete has had both of its GWC cards locked.

  Refer to procedure Lock a GWC card on page 519 in this NTP for instructions on locking a GWC card. Remember to lock both GWC cards for the GWC node being removed.

Note 1: If you are removing a UAS Gateway Controller, ensure that UAS datafill for tables SERVSINV, ANNMEMS, and CONF3PR has been properly removed prior to performing this procedure.

Refer to the *CS 2000 Configuration Management* NTP applicable to your solution for instructions on removing datafill from XA-Core tables.

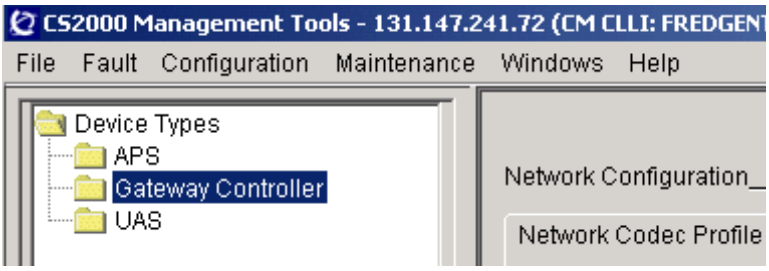
Note 2: If you are removing a SIP-T or VRDN Gateway Controller, ensure that datafill for table SERVSINV has been properly removed prior to performing this procedure.

Refer to the *CS 2000 Configuration Management* NTP applicable to your solution for instructions on removing datafill from XA-Core tables.

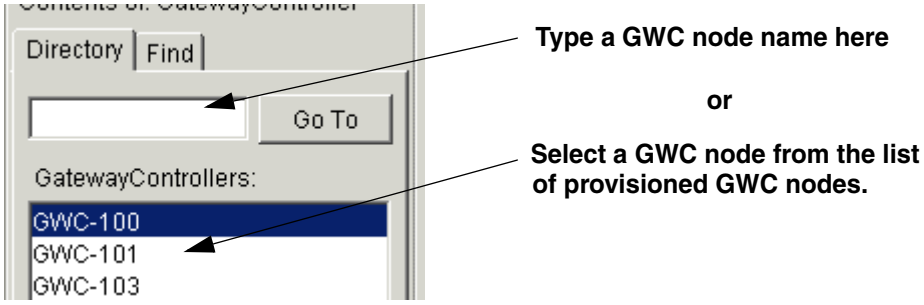
Action

From the CS 2000 GWC Manager client

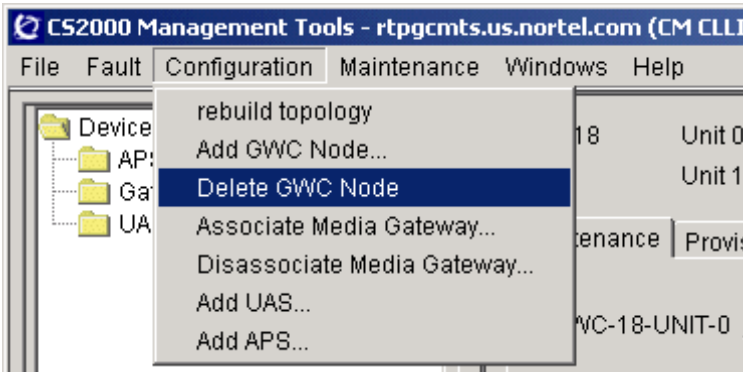
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 Locate the GWC node to delete from the list of provisioned GWC nodes displayed in the Contents of: Gateway Controller pane.



3 At the main CS 2000 GWC Manager window, click on the **Configuration** menu from the top menu bar and select **Delete GWC Node**.



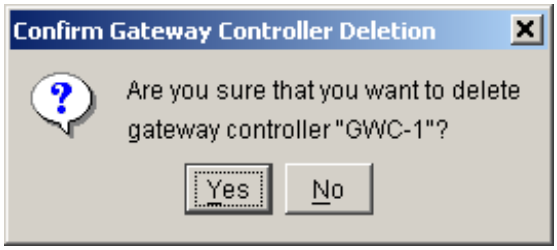
4

CAUTION

Ensure the GWC node you wish to delete has had both of its GWC cards locked.

Refer to procedure Lock a GWC card on page 519 in this NTP for instructions on locking a GWC card. Remember to lock both GWC cards for the GWC node being removed.

At the prompt, click **Yes** to confirm that you wish to delete the GWC node.



A response dialog is displayed when the operation is complete. If any error occurred during the deletion, click the **Show Details** button for information on where the transaction failed.

5 Verify that the GWC node has been removed from the Contents of: Gateway Controller frame.

6 The procedure is complete.

Enable or disable CICM location change reporting

Purpose of this procedure

Use this procedure to enable or disable location change reporting of Centrex IP Client Manager (CICM) telephony clients on a Gateway Controller (GWC) node.

You can configure the destination (or recipient) of CICM location information using procedure Configure a destination for CICM location information on page 77.

When to use this procedure

Use this procedure when you need to enable or disable location change reporting of CICM telephony clients on a GWC node.

For example, you need to use this procedure if you are changing the platform of the location recipient, or if you are moving a gateway that provides location information to a different GWC node.

Prerequisites and guidelines

For location information to be sent to the location recipient you must first perform the network-level procedure Configure a destination for CICM location information on page 77.

> ***Note:*** If you try to perform this procedure without configuring a destination for CICM location information, you will see an error message.

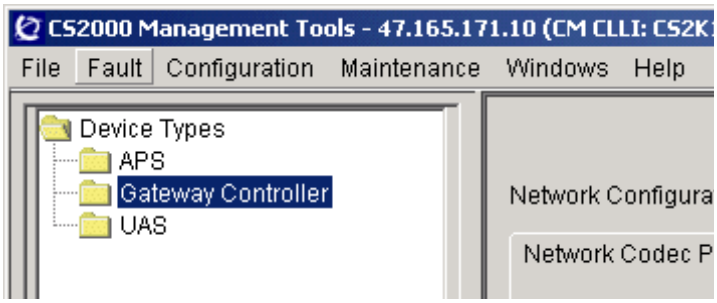
You can enable location change reporting only for GWC nodes provisioned with the following GWC service profiles:

- LARGE_LINEINTL
- LARGE_LINENA

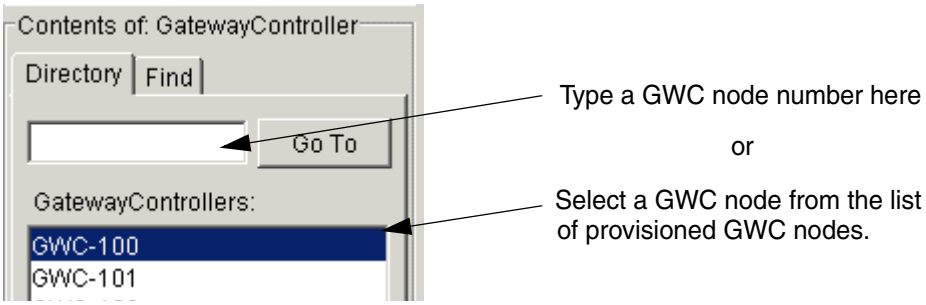
Action

At the CS 2000 GWC Manager client

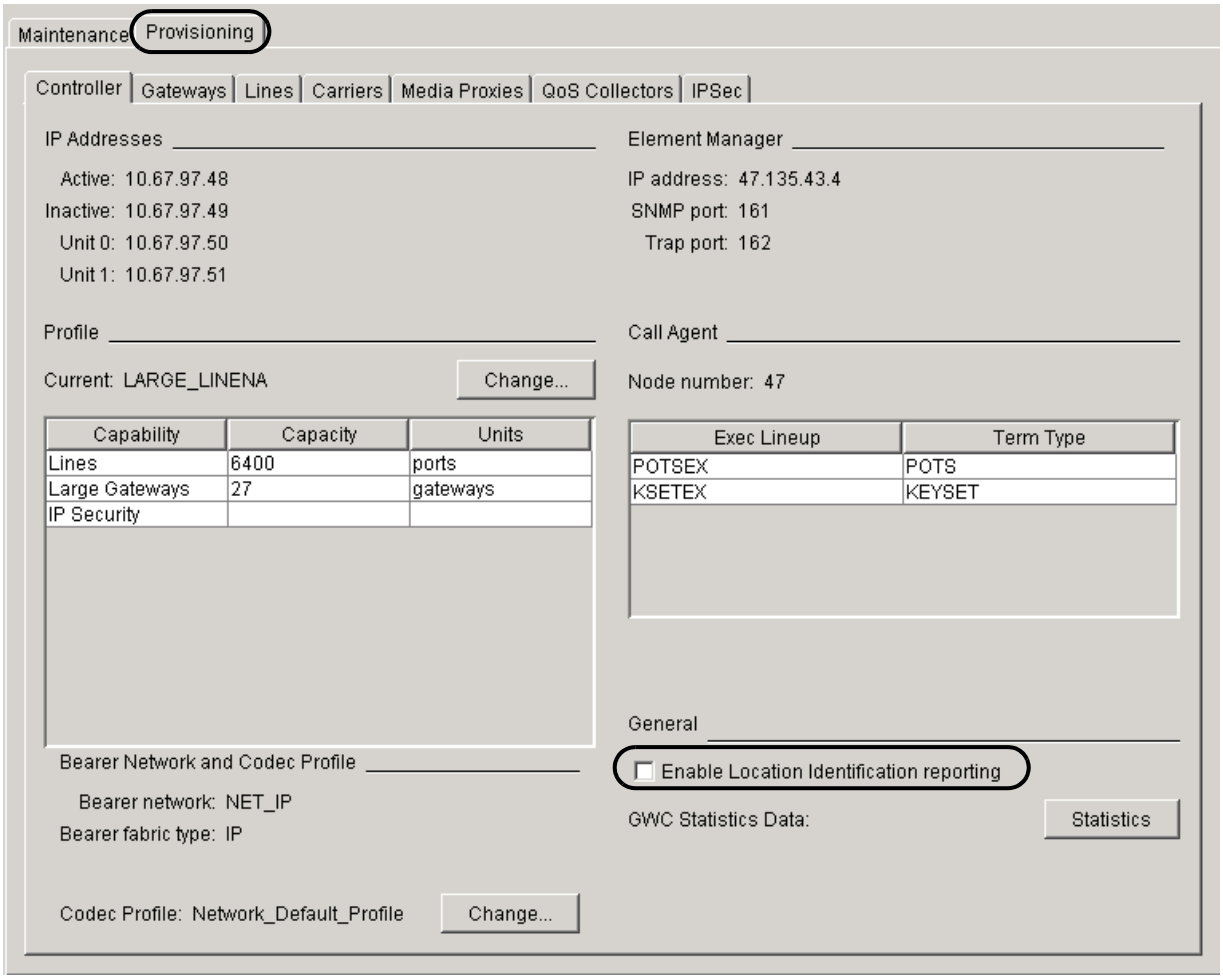
1 Select Gateway Controller from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.



4 To enable CICM location change reporting on the GWC node, select the Enable Location Identification reporting check box.

Confirm that the system accepts the check box selection.

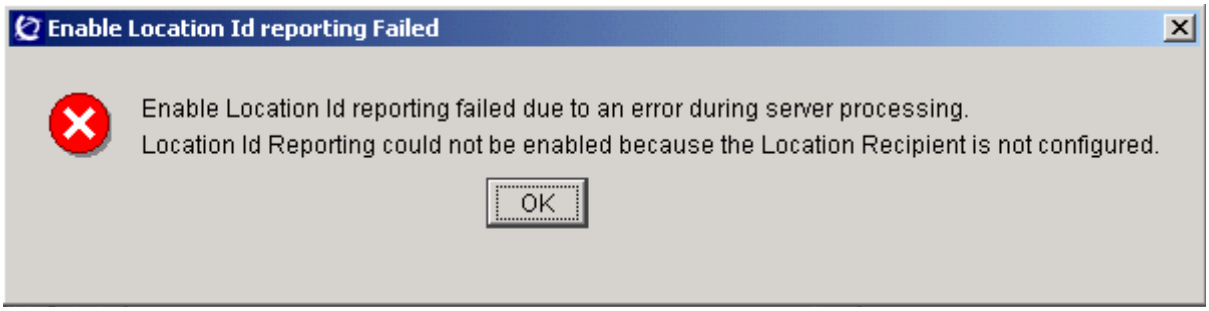
Note 1: You can only enable location change reporting for GWC nodes provisioned with the following Gateway Controller profiles:

- LARGE_LINEINTL
- LARGE_LINENA

You can view the Gateway Controller service profile provisioned for the GWC node in the Profile section of this screen.

The Enable Location Identification reporting check box is not available to be used for GWC nodes provisioned with other profiles.

Note 2: If you have not configured a destination for CICM location information, you will see the following error message. Refer to network-level procedure Configure a destination for CICM location information on page 77 to perform this task. Then, perform this procedure.



5 To disable CICM location change reporting on the GWC node, de-select the Enable Location Identification reporting check box.

Confirm that the system accepts the de-selection of the check box.

6 The procedure is complete.

Add an IP-VPN (NAT) zone

Purpose of this procedure

Use this procedure to define and add an IP-VPN network address translator (NAT)-type network service zone to the Gateway Controller (GWC) database.

ATTENTION

If your network configuration includes the Policy Controller, all network zones must be configured identically: first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller. Once you add a new IP-VPN (NAT) zone to the CS 2000 system, you must immediately add it to the Policy Controller. Otherwise, the Network VCAC may not function properly.

For information on how to configure a NAT-type zone on the Policy Controller, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

Due to the need to conserve IP addresses across enterprise networks, the CS 2000 is often located on one IP VPN and the gateways are located on different IP VPNs. Therefore, in order for the CS 2000 to communicate with the gateways, a NAT-type service zone is needed. A NAT zone provides the gateways with a temporary public IP address. A GWC will select and then setup a media proxy based on call flow. A pool of media proxies can be made available to perform NAT traversal functions by assigning one or more proxy devices to a GWC node using procedure Associate a media proxy with a GWC node on page 373.

The system automatically assigns the zone identifier (ID) of the NAT. This ID incorporates the call agent ID assigned to the CS 2000.

This procedure also allows you to specify a zone ID for the NAT, instead of allowing the system to automatically assign the zone ID. Manually configuring a zone ID allows two or more CS 2000s to share the same NAT service zone.

Note: You cannot change the zone ID after adding an IP-VPN(NAT) zone.

This procedure includes the option to select a parent zone in the network hierarchy for the zone you are configuring. A parent zone is defined as a network zone that is closer to the network core (CS 2000) than the zone you are adding. (Therefore, the IP-VPN(NAT) zone would

be closer to the gateways at the edge of the network.) A parent zone can be an IP-VPN(NAT), an LBL, or a composite NAT-LBL zone.

When to use this procedure

Use this procedure when you need to add one or more IP-VPN(NAT) service zones to the network before associating gateways that use NAT-type zones with the GWC.

As part of the procedure to add an IP-VPN(NAT) zone, you have the option to manually configure the zone ID of a NAT. You can do this instead of allowing the system to automatically assign a zone ID. Use this capability when you wish to configure a NAT-type zone that is shared with another CS 2000. Manually configuring a zone ID allows two or more CS 2000s to share the same IP-VPN(NAT) zone.

Prerequisites and guidelines

The following prerequisites apply to this procedure:

- The call agent ID must be set for your CS 2000 before you add a NAT-type service zone. Refer to procedure Set the call agent identifier on page 67 for details.

  Note: Disregard this item if the call agent ID is already set.

- If you intend to configure an IP-VPN(NAT) service zone that is already configured on another CS 2000 (that is, a shared zone configuration), you need to determine the ID of the zone on the other CS 2000. Refer to procedure View a network zone ID on page 355 for details.

The following guidelines apply to this procedure:

- NAT-type service zones must be configured before any media gateways that use NAT service are associated to a GWC. The data for an IP-VPN(NAT) zone will be sent down to the GWC when the zone is associated with a media gateway.
- Multiple NAT devices that all implement the same IP-VPN and share a single exit point should be configured as a single IP-VPN(NAT) zone.
- There is only one IP-VPN(NAT) exit point from a local network. If two gateways are behind the same IP-VPN(NAT) zone, they can setup a call without requiring a media proxy.
- The Integrated Access Cable solution uses DQoS and PEP servers while the Integrated Access Wireline solution uses ITRANS (internet transparency) and NATs as media proxies. These two solutions are mutually exclusive as defined in the gateway profile

service type. In other words, DQOS and ITRANS cannot be defined together in a single GWC profile when associating media gateways to a GWC.

- The maximum number of sequentially linked service zones in a network hierarchy is five.

Note: Media proxies are configured using the Multimedia Communications System (MCS) Manager application. Refer to the MCS documentation for details.

The following table lists the distinct combinations of NAT-type service zones supported using this procedure.

Combination	Shared zone	Parent zone
1	Not shared	Does not have a parent zone
2	Not shared	Has a parent zone
3	Shared	Does not have a parent zone
4	Shared	Has a parent zone

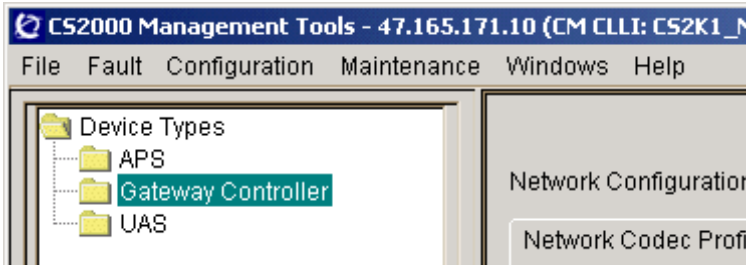
A shared IP-VPN(NAT) service zone is defined as zone that is shared with another CS 2000.

A parent zone is defined as a network zone that is closer to the network core (the CS 2000) than the IP-VPN(NAT) zone you are adding.

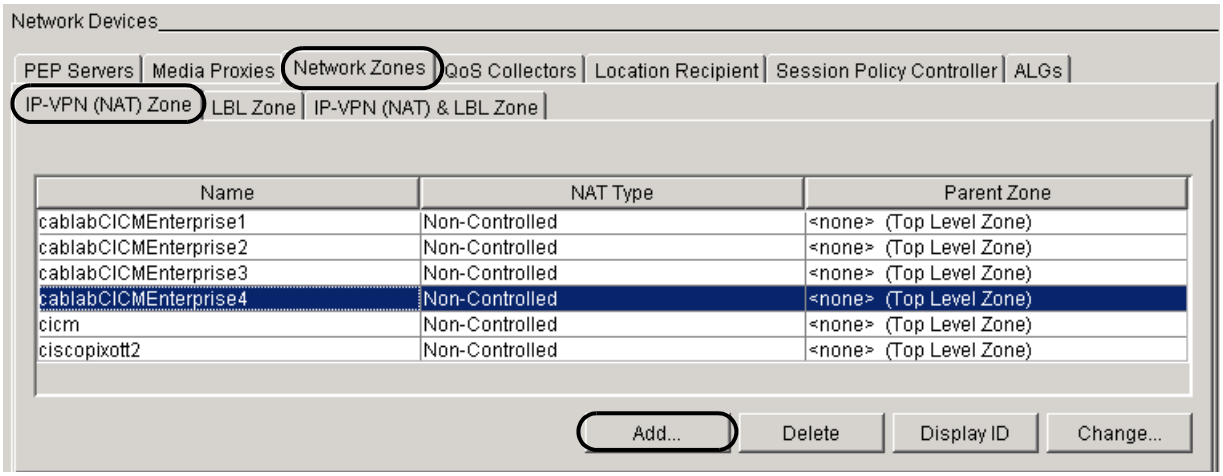
Action

At CS 2000 GWC Manager client

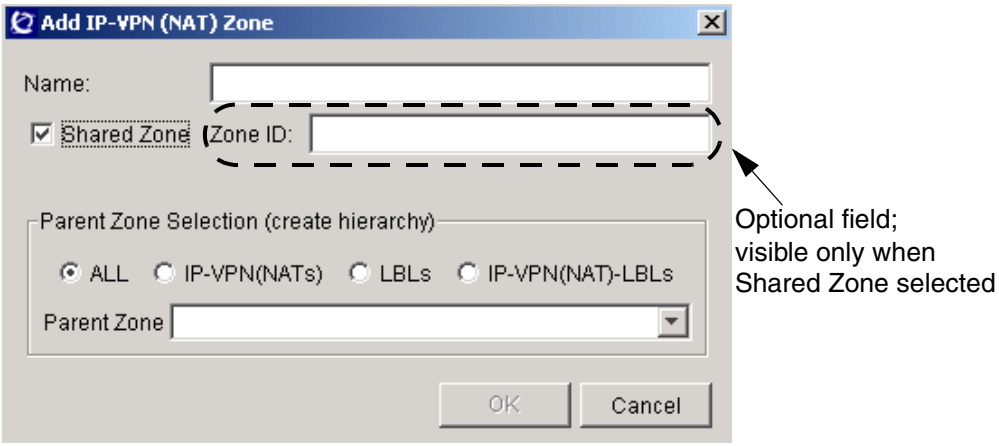
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Network Devices panel, click the **Network Zones** tab, then click the **IP-VPN (NAT) Zone** tab to display the IP-VPN (NAT) Zone panel.



3 Click the **Add** button to display the Add IP-VPN(NAT) Zone dialog box.



4 Click in the Name: field and type a unique alphanumeric name for the IP-VPN(NAT) zone. If necessary, contact your site system administrator for assistance with this task.

Note: If you intend to share this zone with another CS 2000, it is recommended that the name of the zone corresponds to the name used on the other CS 2000. However, this is not a requirement.

5 If you want the zone to be shared, complete the following sub-steps. Otherwise, continue with step 7.

Note 1: The zone ID of the shared zone is required for this procedure. Access the GWC Manager for a CS 2000 that is already configured with the zone you intend to share. Display

and record the zone ID for that zone. Refer to procedure View a network zone ID on page 355 for details.

Note 2: If necessary, contact your site system administrator to identify the zone ID you must use.

a Select the Shared Zone check box. The dialog box extends to include the Zone ID: field.

b Assign the zone ID of the NAT device you intend to share with another CS 2000.

Note: The zone ID must match the existing ID for the IP-VPN(NAT) zone already configured on another CS 2000.

The range of valid values is between 2 and 16777215 inclusive (1 is reserved). If necessary, contact your site system administrator to determine the zone ID you must use.

If the value entered is invalid, the text field is outlined in red and the OK button is disabled.

6 Use the following table to determine your next step.

If the new zone	Do
has a parent zone in the network	go to step step 7
does not have a parent zone in the network	leave the Parent Zone: field blank or select <none>, then go to step 8

7 Select a parent zone for the new zone using the following sub-steps.

Note: A parent zone is defined as a zone that is closer to the network core (the CS 2000) than the NAT-type zone you are adding.

a In the Parent Zone Selection area, select one of the radio buttons to choose the scope of your zone selection. The options are:

- ALL - includes all zones
- IP-VPN(NATs) - restricts the selection to IP-VPN (NAT) zones
- LBLs - restricts the selection to LBL zones
- IP-VPN(NAT)-LBLs - restricts the selection to composite NAT-LBL zones

b Click the Parent Zone: field and from the list in the drop-down menu, select a parent zone for the new NAT-type zone.

Note: If desired, first type text characters of a zone name in the field to fine tune your display. The system displays all NAT, LBL, or composite NAT-LBL zones with a name that matches any of the characters you type.

8 Click the **OK** button at the bottom of the dialog box to accept all the settings for the new NAT-type zone.

Note: If you did not assign the Zone ID manually, the system automatically assigns it. This ID incorporates the call agent ID assigned to the CS 2000.

If the name or the shared ID assigned is already in use, you will see an error message. If an error was made when adding the zone, delete it from the network using procedure Delete a network service zone on page 359. Then re-add the zone using this procedure.

9 Confirm that the new zone appears in the IP-VPN (NAT) Zone table.

Note: If your network configuration includes the Policy Controller, you must now add this new zone to the Policy Controller using the same zone name, ID, and parent selection. If you did not assign the zone ID manually, obtain the ID assigned by the system using procedure View a network zone ID on page 355.

10 The procedure is complete.

Configure resource usage data for limited bandwidth links (LBL)

Purpose of this procedure

ATTENTION

This procedure does not apply if your network configuration includes the Policy Controller, and the Network VCAC (virtual call admission control) status is ON. If required, refer to procedure Review available network devices on page 99 to check your network configuration.

Use this procedure only if the Network VCAC status is set to OFF, that is, the virtual call admission control is performed by each Gateway Controller (GWC), instead of the Policy Controller.

Use this procedure to configure resource usage parameters to be used over limited bandwidth links (LBL) for virtual call admission control (VCAC).

When the Network VCAC status is OFF, an LBL is configured to support a maximum count value representing the call set-up capacity through the link. Call set-up through an LBL causes a running total of bandwidth capacity used to be incremented. Call take-down causes the running total to be decremented. If a call set-up would cause the running total of capacity used to exceed the maximum capacity of the LBL, then the call attempt is rejected and routed to NBLN (network blocking load normal) treatment.

Note: For additional information on the NBLN treatment datafill, refer to section Additional information on page 337 in procedure Add a limited bandwidth link (LBL) zone.

Each resource usage entry has a set of values representing the bandwidth used for each call. These values depend on the codec and packetization rate used on the call. The resource usage entry assigned to an LBL defines the specific amount incremented to (or decremented from) the running total of used bandwidth capacity when a call is set up (or terminated).

When to use this procedure

Use this procedure when you need to identify a resource usage profile to be available for LBLs in your network (only if your network configuration does not include the Policy Controller and the Network VCAC status is OFF).

Prerequisites and guidelines

A resource usage profile must be configured, before it can be used when configuring an LBL. If required, refer to one of the following procedures:

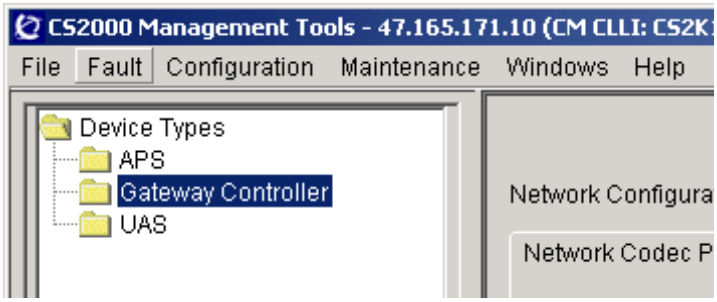
- Add a limited bandwidth link (LBL) zone on page 331
- Change attributes of a network zone on page 349

You cannot delete a resource usage profile that is used by an LBL. You can, however, change the parameters of a resource usage profile that is used by an LBL. The changes will be propagated to the GWC.

Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



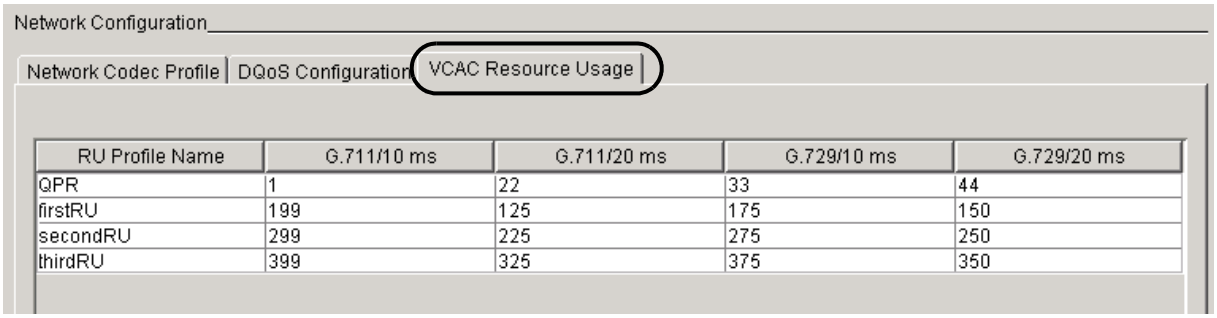
2 Determine your next step using the following table:

If you wish to	Do
view all resource usage (RU) profiles	step 3
add an RU profile	step 4
change an RU profile	step 5
delete an RU profile	step 6

3 Perform the following steps to view all RU profiles configured.

a From the Network Configuration panel click the **VCAC Resource Usage** tab to display the VCAC Resource Usage pane.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



All existing resource usage (RU) profiles are displayed in the following columns:

- RU profile name
- G.711/10 ms - Per-call bandwidth using G.711 codec at a packetization rate of 10 milliseconds.
- G.711/20 ms - Per-call bandwidth using G.711 codec at a packetization rate of 20 milliseconds.
- G.729/10 ms - Per-call bandwidth using G.729 codec at a packetization rate of 10 milliseconds
- G.729/20 ms - Per-call bandwidth using G.729 codec at a packetization rate of 20 milliseconds.

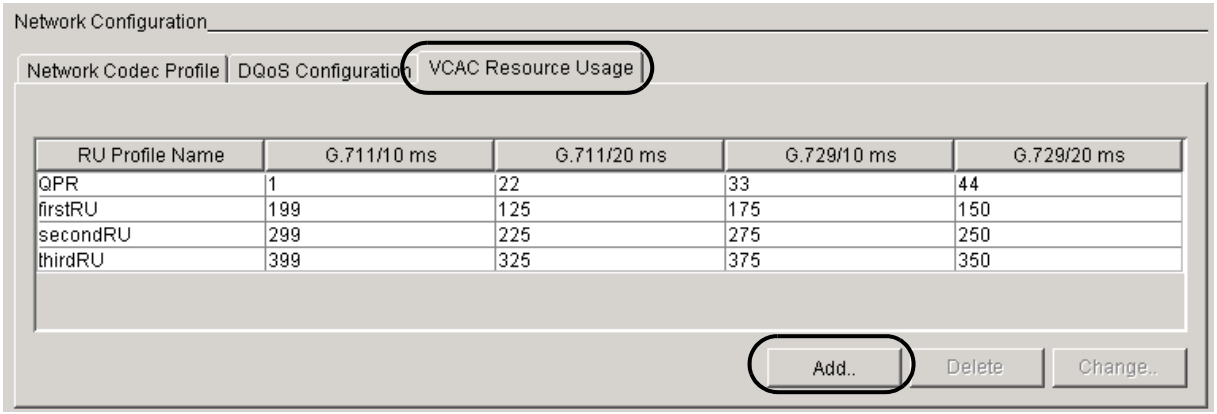
The per-call bandwidth values can be compared to the total bandwidth available through an LBL.

b Go to step 7.

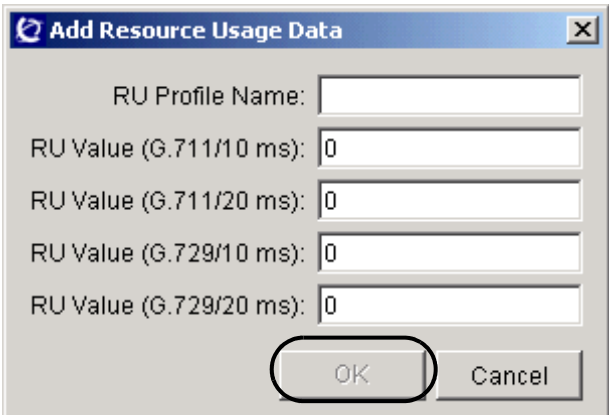
4 Perform the following steps to add an RU profile.

a From the Network Configuration panel click the **VCAC Resource Usage** tab to display the VCAC Resource Usage pane.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



b Click the **Add** button to display the Add Resource Usage Data dialog box.



Note 1: RU values set in the following steps are required for every codec and packetization rate combination that has been created for your network. If a value is not required, leave the default setting "0", which means that every call will use zero bandwidth (unlimited calls).

Note 2: The per-call RU values can be compared to the total bandwidth available through an LBL (referred to as Max Count).

Example
If you set the codec/packetization rate for an RU Profile Name to 5 and the Max Count for the same RU Profile Name to 10 (when adding an LBL), then there is enough bandwidth available for two calls. The third call is rejected since the Max Count has been exceeded.

Note 3: The per-call RU values set in the following steps are defined as part of network engineering.

Note 4: All RU values must be non-negative integers.

c In the RU Profile Name: field, type a name for the new profile. Use a unique alphanumeric text string to identify the profile.

d In the RU Value (G.711/10 ms): field, type a per-call bandwidth value using G.711 codec at a packetization rate of 10 milliseconds.

e In the RU Value (G.711/20 ms): field, type a per-call bandwidth value using G.711 codec at a packetization rate of 20 milliseconds.

f In the RU Value (G.729/10 ms): field, type a per-call bandwidth value using G.729 codec at a packetization rate of 10 milliseconds.

g In the RU Value (G.729/20 ms): field, type a per-call bandwidth value using G.729 codec at a packetization rate of 10 milliseconds.

h Click the **OK** button to add the RU profile.

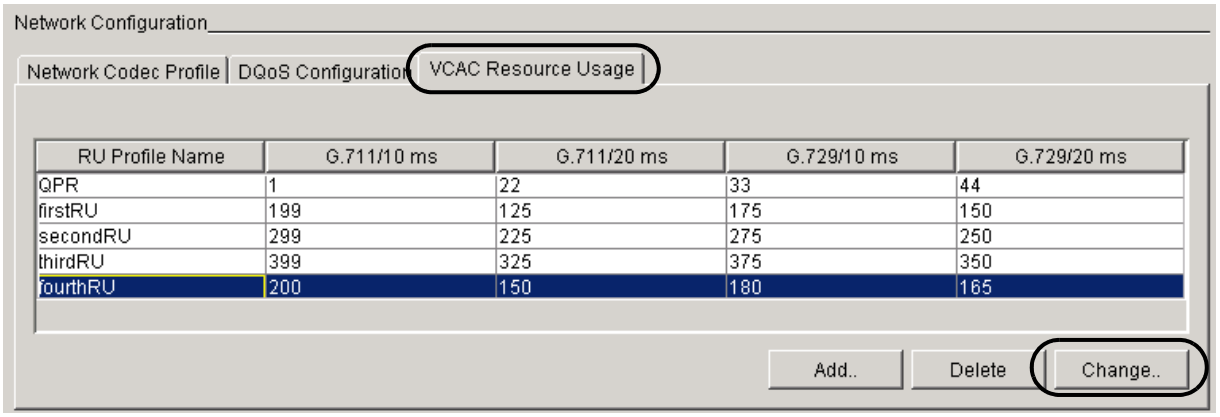
The new profile appears on the list of RU profiles and is available to be used on an LBL.

i Go to step 7.

5 Perform the following steps to change the parameters of an existing RU profile.

a From the Network Configuration panel click the **VCAC Resource Usage** tab to display the VCAC Resource Usage pane.

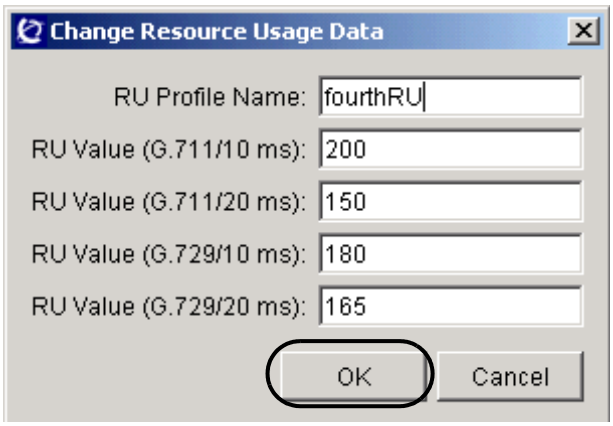
Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



b Select one of the existing RU profiles in the list.

Your selection is highlighted.

c Click the **Change** button to display the Change Resource Usage Data dialog box.



You can change the RU profile name or any of the RU values displayed.

Note 1: RU values set in the following steps are required for every codec and packetization rate combination that has been created for your network. If a value is not required, leave the default setting "0".

Note 2: The per-call RU values can be compared to the total bandwidth available through an LBL (referred to as Max Count).

Note 3: The per-call RU values set in the following steps are defined as part of network engineering.

Note 4: All RU values must be non-negative integers.

d If necessary, change the RU Profile Name. Use a unique alphanumeric text string to identify the profile.

e If necessary, change the RU Value (G.711/10 ms). This represents the per-call bandwidth value using G.711 codec at a packetization rate of 10 milliseconds.

f If necessary, change the RU Value (G.711/20 ms). This represents the per-call bandwidth value using G.711 codec at a packetization rate of 20 milliseconds.

g If necessary, change the RU Value (G.729/10 ms). This represents the per-call bandwidth value using G.729 codec at a packetization rate of 10 milliseconds.

h If necessary, change the RU Value (G.729/20 ms). This represents the per-call bandwidth value using G.729 codec at a packetization rate of 10 milliseconds

i Click the **OK** button to change the RU profile.

The changed profile is reflected on the list of RU profiles and is available to be used on an LBL.

Note: If the RU profile is assigned to an LBL, the changes to the profile will be propagated to the LBL. If you change the name of an RU profile assigned to an LBL, simply re-select the **LBL Zone** tab to view the propagated change.

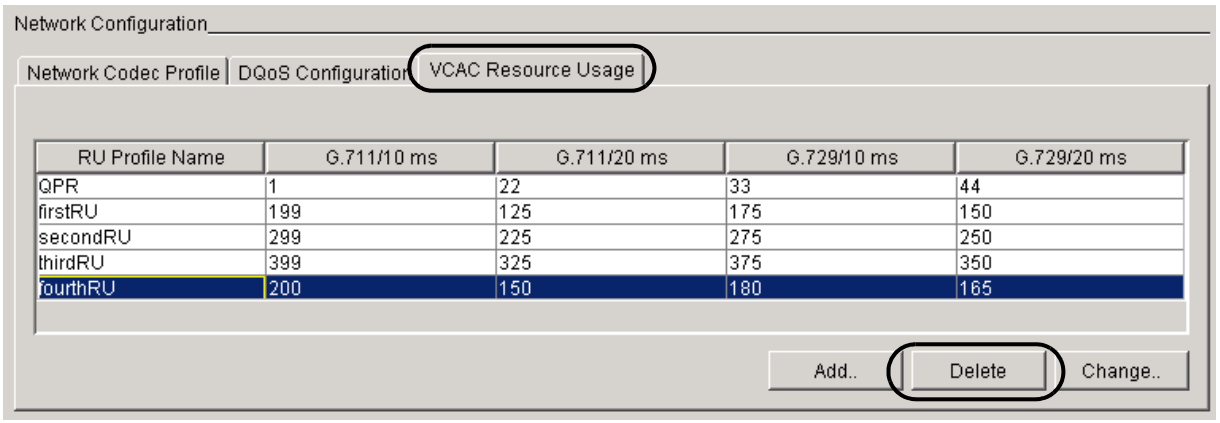
j Go to step 7.

6 Perform the following steps to delete an existing RU profile.

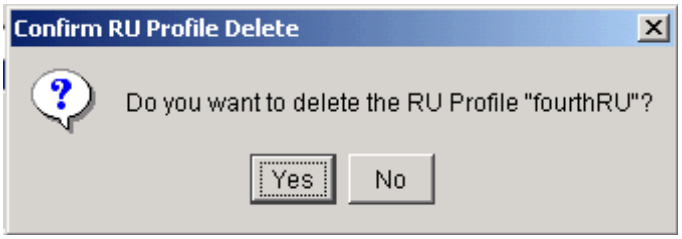
a From the Network Configuration panel click the **VCAC Resource Usage** tab to display the VCAC Resource Usage pane.

Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.

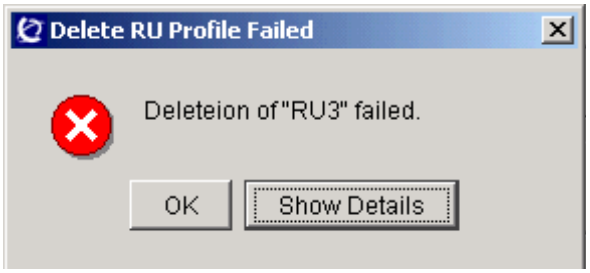
b Select one of the existing RU profiles in the list.



c Click the **Delete** button to remove the profile. At the prompt, click **Yes** to confirm the deletion.



Note: An error will occur if you try to delete an RU profile that used by an LBL.



7 If necessary, return to step 2 to repeat this procedure.

8 The procedure is complete.

Add a limited bandwidth link (LBL) zone

Purpose of this procedure

Use this procedure to define and add a limited bandwidth link (LBL) zone to the Gateway Controller (GWC) database. An LBL is a virtual representation of a link identified in the network that has restricted capacity and which warrants bandwidth management. An LBL zone is a type of a network service zone, like an IP-VPN network address translator (NAT) zone.

ATTENTION

If your network configuration includes the Policy Controller, all network zones must be configured identically: first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller. Once you add a new LBL zone to the CS 2000 system, you must immediately add it to the Policy Controller. Otherwise, the Network VCAC may not function properly.

For information on how to configure an LBL zone on the Policy Controller, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

If your network configuration does not include the Policy Controller (Network VCAC status is OFF), the following parameters must be defined:

- An LBL is configured to support a maximum count value representing the call set-up capacity through the link. Call set-up through an LBL causes a running total of bandwidth capacity used to be incremented. Call take-down causes the running total to be decremented. If a call set-up would cause the running total of capacity used to exceed the maximum capacity of the LBL, then the call attempt is rejected and routed to NBLN (network blocking load normal) treatment.

  Note: For additional information on VCAC and on the NBLN treatment datafill, refer to section Additional information on page 337.

- You must select a resource usage profile to be used for each LBL. Each resource usage entry has a set of values representing the bandwidth used per-call. These values depend on the codec and packetization rate used on the call. The resource usage entry assigned to an LBL defines the specific amount incremented to (or decremented from) the running total of used bandwidth capacity

when a call is set-up (or terminated). For more information, refer to procedure Configure resource usage data for limited bandwidth links (LBL) on page 323

This procedure includes the option to select a parent zone in the network hierarchy for the LBL zone you are configuring. A parent zone is defined as a zone that is closer to the network core (CS 2000) than the LBL zone you are adding. (Therefore, the LBL would be closer to the gateways at the edge of the network.) A parent zone can be an IP-VPN(NAT) zone, another LBL zone, or a composite NAT-LBL zone.

The system automatically assigns the zone identifier (ID) of an LBL. This ID incorporates the call agent ID assigned to the CS 2000.

This procedure also allows you to specify a zone ID for the LBL, instead of allowing the system to automatically assign the zone ID.

Note: You cannot change the zone ID after adding an LBL zone.

When to use this procedure

Use this procedure when you need to add one or more LBLs to the network. An LBL zone must be configured before any media gateways that use the LBL can be associated with a GWC.

Prerequisites and guidelines

The following prerequisites apply to this procedure:

- The call agent ID must be set for your CS 2000 before you add an LBL-type or a NAT-type zone. Refer to procedure Set the call agent identifier on page 67 for details.

  Note: Disregard this item if the call agent ID is already set.

- If your network does not include the Policy Controller and the Network VCAC status is OFF, you must add a resource usage profile before adding an LBL. Refer to procedure Configure resource usage data for limited bandwidth links (LBL) on page 323.
- If you need to select a parent zone for the LBL you are adding, then that zone must already be configured on the CS 2000. The parent zone can be an IP-VPN(NAT), an LBL, or a composite NAT-LBL zone.

The following guidelines apply to this procedure:

- LBL zones must be configured before any media gateways (MG) that use the LBL are associated with a GWC. Information on any

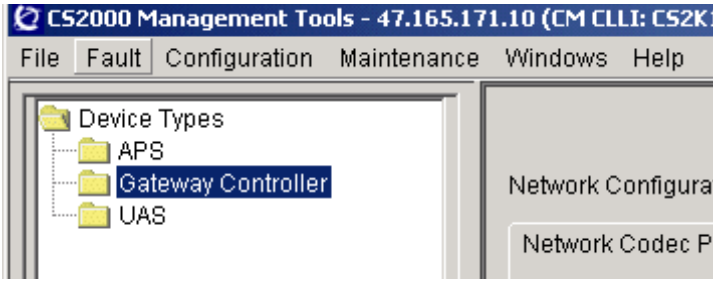
LBLs in the path of an MG is sent to the GWC when the MG is associated with the GWC.

- If two gateways are behind the same LBL, a call between the gateways does not use capacity over that LBL.
- The Integrated Access Cable solution uses DQoS and PEP Servers while the Integrated Access Wireline solution uses internet transparency (ITRANS) and NATs as media proxies. These two solutions are mutually exclusive as defined in the gateway profile service type. Therefore, DQoS and ITRANS cannot be defined together in a single GWC profile when associating a media gateway with a GWC.
- The maximum number of sequentially linked service zones in a network hierarchy is five.

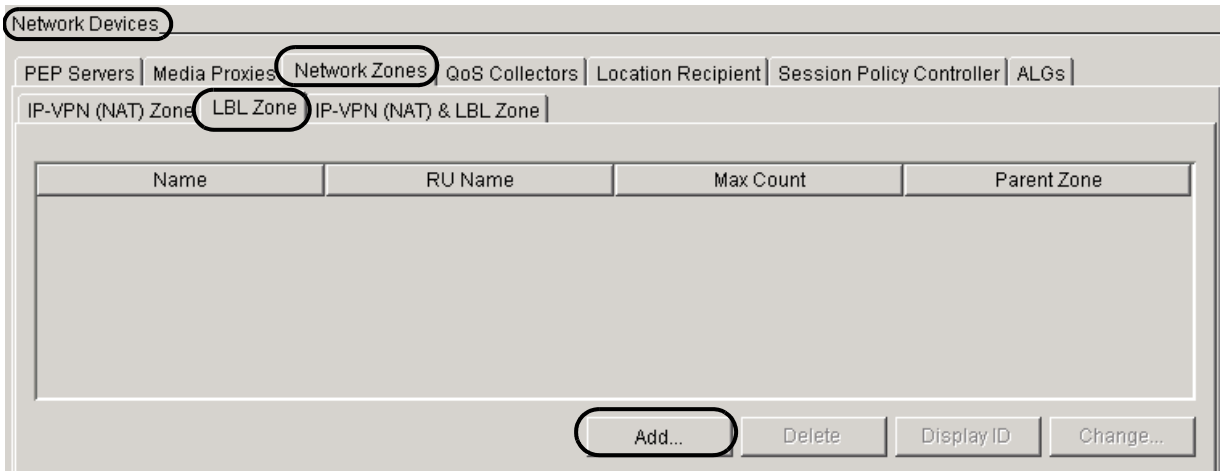
Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



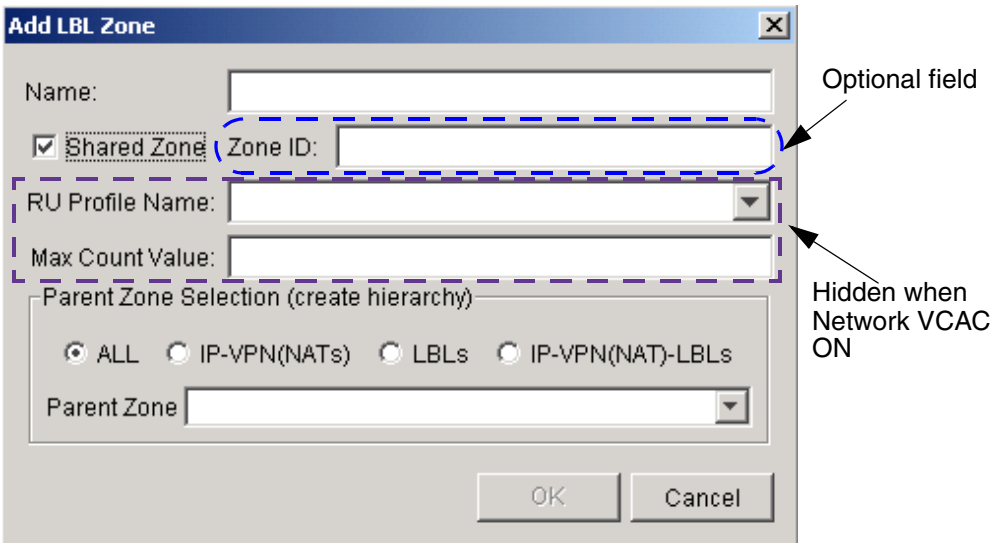
2 From the Network Devices panel, click the **Network Zones** tab, then click the **LBL Zone** tab to display the LBL pane.



3 Click the **Add** button to display the appropriate Add LBL Zone dialog box, depending on your network topology.

If your network configuration includes the Policy Controller (Network VCAC status: ON), the following fields are not displayed (hidden):

- RU Profile Name
- Max Count Value



4 At the Add LBL Zone dialog box, click in the Name: field and type a unique alphanumeric name for the LBL zone.

5 If you want the LBL zone to be shared, select the Shared Zone check box. Otherwise, continue with the next step.

When you select the Shared Zone check box, the dialog box extends to include the Zone ID: field. Assign the zone ID of the LBL.

The range of valid values is between 2 and 16777215 inclusive (1 is reserved). If necessary, contact your site system administrator to determine the zone ID you must use.

If the value entered is invalid, the text field is outlined in red and the OK button is disabled.

6 Use the following table to determine your next step.

If the Network VCAC status is	Do
OFF	go to step 7
ON	go to step 9

7 Click the RU Profile Name: drop-down menu to select a resource usage profile to be used for the new LBL.

Only the RU profiles already configured will appear in the drop-down list. To view the details of existing RU profiles, click the **VCAC Resource Usage** button under Network Configuration.

8 Click in the Max Count Value: field and type a non-negative integer value indicating the call set-up capacity through the link.

The call set-up capacity must be compared to the contents of the RU profile selected in the previous step.

9 Use the following table to determine your next step.

If the new LBL	Do
has a parent zone	go to step 10
does not have a parent zone	leave the Parent Zone: field blank or select <none>, and go to step 11

10 Select the parent zone for the new LBL using the following sub-steps.

Note: A parent zone is defined as a zone that is closer to the network core (the CS 2000) than the LBL zone you are adding.

a In the Parent Zone Selection area, select one of the radio buttons to choose the scope of your zone selection. The options are:

- ALL - includes all zones
- IP-VPN(NATs) - restricts the selection to IP-VPN(NAT) zones
- LBLs - restricts the selection to LBL zones
- IP-VPN(NAT)-LBLs - restricts the selection to composite IP-VPN(NAT) & LBL zones

b Click the Parent Zone: field and from the list in the drop-down menu, select a parent zone for the new LBL zone.

Note: If desired, first type text characters of a zone name in the field to fine tune your display. The system displays all NAT, LBL, or composite NAT-LBL zones with a name that matches any of the characters you type.

11 Click the **OK** button at the bottom of the dialog box to accept all the settings for the new LBL zone.

Note: If an error was made when adding the LBL zone, delete it from the network using procedure Delete a network service zone on page 359, then re-add the LBL zone using this procedure.

12 Confirm that the new LBL zone appears in list.

Note: If your network configuration includes the Policy Controller, you must now add this new zone to the Policy Controller using the same zone name, ID, and parent selection. If you did not assign the zone ID manually, obtain the ID assigned by the system using procedure View a network zone ID on page 355.

13 The procedure is complete.

Additional information

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 an 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 LBL.

NBLN datafill

To enable Network Blocking Normal Traffic (NBLN) treatment for VCAC, the following tables must be datafilled:

- Table Treatment Control (TMTCNTL) on page 338
- Table Treatment to Cause Map (TMTMAP) on page 339
- Table Flexible CAUSEMAP (FLXCMAP) on page 340

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.

ATTENTION

The datafill examples in the following sections are examples only. There are regulatory requirements for the behavior of signaling links and each operating company can have different requirements for the mapping of release codes to treatments, and for the management of their signaling network.

Table Treatment Control (TMTCNTL)

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.

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>
```

where

NBLN
is the assigned treatment

Y
indicates that the event must be logged

S
indicates that the tone is defined by Common Language Location Identifier (CLLI)

<tone>
is the preferred tone which is identified by the operating company 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.

Table Treatment to Cause Map (TMTMAP)

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 protocol. 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.

Table 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 operating company to identify a release cause that will map into their signaling network.

Examples of table TMTMAP datafill:

```
Q764 NBLN ALLBC ISUP NOLOCAL NORMUNSP LOCLNET Y

Q767 NBLN ALLBC ISUP 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 *Carrier VoIP 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 operating company 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 VCAC failures.

Table Flexible CAUSEMAP (FLXCMAP)

This table maps 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 *Carrier VoIP Networks Operational Configuration: Data Schema Reference*, NN10324-509.

Note 2: In multi-node scenarios, the operating company is responsible for configuring the signaling to ensure the NBLN treatment can reach the originator. If any node does not support 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.

Service limitations and restrictions

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

Lawful Intercept

For 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. VCAC does not give extra precedence to these calls over other voice traffic.

Examples of 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 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 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 re-connection can fail if other calls have consumed the bandwidth in the meantime. In this case, the party on hold drops to dial tone 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 VCAC actually blocks that party. The denied party hears NBLN treatment but existing conferees hear no indication that the joining attempt failed. If the 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 composite IP-VPN (NAT) and LBL zone

Purpose of this procedure

ATTENTION

Use this procedure only when your network configuration includes the Policy Controller and the Network VCAC status is ON. All network topology data must be configured identically: first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller. Once you add a new network zone to the CS 2000 system, you must immediately add it to the Policy Controller. Otherwise, the Network VCAC may not function properly.

For information on how to configure a composite zone on the Policy Controller, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

This procedure describes how to define and add a composite IP-VPN (NAT) and LBL network zone to the GWC database. A composite zone comprises the attributes of the following network zones:

- IP-VPN network address translator (NAT) zone
- limited bandwidth link (LBL) zone

Use this type of a network zone for gateways operating behind NATs and LBLs, but only when the Network VCAC status is ON. In this scenario, resource usage profile or max count information is not sent to the GWC; so, for internal counting, this composite zone is treated as an IP-VPN (NAT)-type zone.

Note: For information on an IP-VPN (NAT)-type zone, refer to procedure Add an IP-VPN (NAT) zone on page 317. For more information on an LBL-type zone, refer to procedure Add a limited bandwidth link (LBL) zone on page 331.

The system automatically assigns the zone identifier (ID) of the new zone. This ID incorporates the call agent ID assigned to the CS 2000.

This procedure also allows you to specify a zone ID for the new zone, instead of allowing the system to automatically assign it. Manually configuring a zone ID allows two or more CS 2000s to share the same zone.

Note: You cannot change the zone ID after adding a new zone.

This procedure includes the option to select a parent zone in the network hierarchy for zone you are configuring. A parent zone is defined as a zone that is closer to the network core (CS 2000) than the zone you are adding. (Therefore, the zone would be closer to the gateways at the edge of the network.) A parent zone can be an IP-VPN (NAT), an LBL, or a composite IP-VPN (NAT) and LBL zone.

When to use this procedure

Use this procedure when you need to add one or more composite IP-VPN (NAT) and LBL service zones to the network before associating gateways that use these zones with the GWC.

Prerequisites and guidelines

The following prerequisites apply to this procedure:

- The call agent ID must be set for your CS 2000 before you add a composite IP-VPN (NAT)-LBL zone. Refer to procedure Set the call agent identifier on page 67 for details.

  Note: Disregard this item if the call agent ID is already set.

- If you intend to configure a zone that is already configured on another CS 2000 (that is, a shared zone), you need to determine the zone ID of the zone on the other CS 2000. Refer to procedure View a network zone ID on page 355 for details.

The following guidelines apply to this procedure:

- Network service zones must be configured before any media gateways that use these services are associated to a GWC. The data for a zone will be sent down to the GWC when the zone is associated with a media gateway.
- Multiple NAT devices that all implement the same IP-VPN and share a single exit point should be configured as a single IP-VPN (NAT) zone.
- There is only one IP-VPN (NAT) exit point from a local network. If two gateways are behind the same IP-VPN (NAT) zone, they can setup a call without requiring a media proxy.
- The Integrated Access Cable solution uses DQoS and PEP servers while the Integrated Access Wireline solution uses ITRANS (internet transparency) and NATs as media proxies. These two solutions are mutually exclusive as defined in the gateway profile service type. In other words, DQOS and ITRANS cannot be defined

together in a single GWC profile when associating media gateways to a GWC.

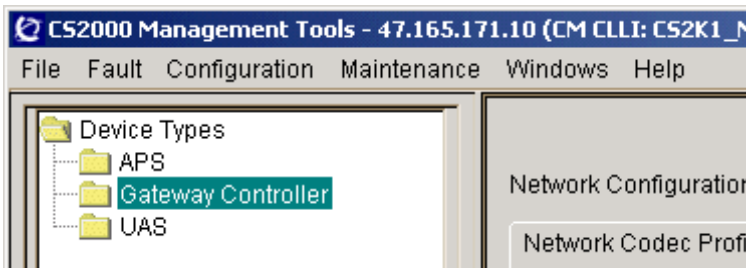
- The maximum number of sequentially linked zones in a network hierarchy is five.

Note: Media proxies are configured using the Multimedia Communications System (MCS) Manager application. Refer to the MCS documentation for details.

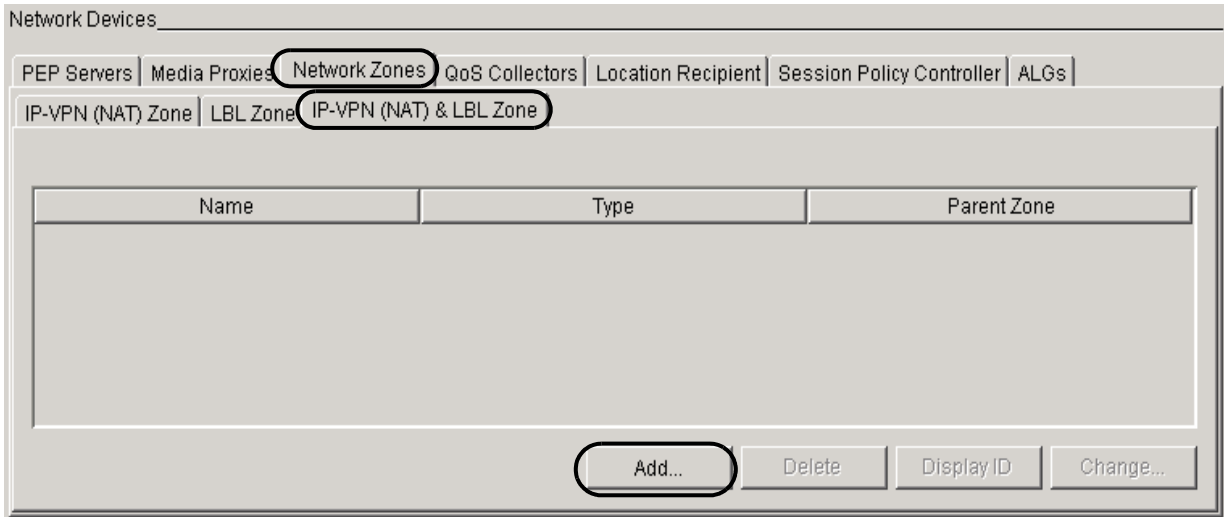
Action

At CS 2000 GWC Manager client

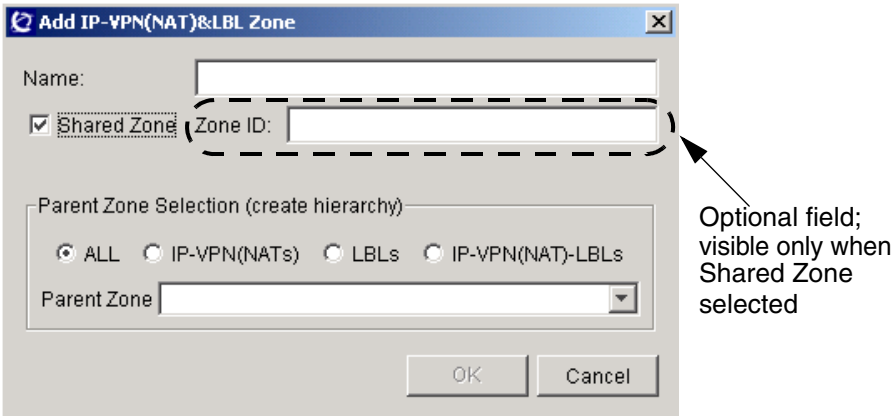
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Network Devices panel, click the **Network Zones** tab, then click the **IP-VPN (NAT) & LBL Zone** tab to display the IP-PVN (NAT) & LBL zone panel.



3 Click the **Add** button to display the Add IP-VPN (NAT) &L BL Zone dialog box.



4 Click in the Name: field and type a unique alphanumeric name for the composite IP-VPN (NAT) and LBL zone.

Note: If you intend to share this zone with another CS 2000, it is recommended that the name of the zone corresponds to the name used on the other CS 2000. However, this is not a requirement.

5 If you want the zone to be shared, complete the following sub-steps. Otherwise, continue with step 6.

Note 1: The zone ID of the shared zone is required for this procedure. Access the GWC Manager for a CS 2000 that is already configured with the zone you intend to share. Display and record the zone ID for that zone. Refer to procedure View a network zone ID on page 355 for details.

Note 2: If necessary, contact your site system administrator to identify the zone ID you must use.

a Select the Shared Zone check box. The dialog box extends to include the Zone ID: field.

b Assign the zone ID of the zone you intend to share with another CS 2000.

Note: The zone ID must match the existing ID for the zone already configured on another CS 2000.

The range of valid values is between 2 and 16777215 inclusive (1 is reserved). If necessary, contact your site system administrator to determine the zone ID you must use.

If the value entered is invalid, the text field is outlined in red and the OK button is disabled.

6 Use the following table to determine your next step.

If the new zone	Do
has a parent zone in the network	go to step step 7
does not have a parent zone in the network	leave the Parent Zone: field blank or select <none>, then go to step 8

7 Select a parent zone for the new zone using the following sub-steps.

Note: A parent zone is defined as a zone that is closer to the network core (the CS 2000) than the composite zone you are adding.

a In the Parent Zone Selection area, select one of the radio buttons to choose the scope of your zone selection. The options are:

- ALL - includes all zones
- IP-VPN(NATs) - restricts the selection to IP-VPN (NAT) zones
- LBLs - restricts the selection to LBL zones
- IP-VPN(NAT)-LBLs - restricts the selection to composite IP-VPN (NAT) and LBL zones

b Click the Parent Zone: field and from the list in the drop-down menu, select a parent zone for the new composite zone.

Note: If desired, first type text characters of a zone name in the field to fine tune your display. The system displays all IP-VPN (NAT), LBL, or composite NAT-LBL zones with a name that matches any of the characters you type.

8 Click the **OK** button at the bottom of the dialog box to accept all the settings for the new composite zone.

Note: If you did not assign the Zone ID manually, the system automatically assigns it. This ID incorporates the call agent ID assigned to the CS 2000.

If the name or the shared ID assigned is already in use, you will see an error message. If an error was made when adding the zone, delete it from the network using procedure Delete a network service zone on page 359. Then re-add the composite zone using this procedure.

9 Confirm that the new zone appears in the IP-VPN (NAT) & LBL Zone table.

Note: If your network configuration includes the Policy Controller, you must now add this new zone to the Policy Controller using the same zone name, ID, and parent selection. If you did not assign the zone ID manually, obtain the ID assigned by the system using procedure View a network zone ID on page 355.

10 The procedure is complete.

Change attributes of a network zone

Purpose of this procedure

ATTENTION

If your network configuration includes the Policy Controller, all IP-VPN (NAT), LBL, and composite IP-VPN (NAT)-LBL zones must be configured identically; first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller. Once you change any attribute of a network zone, you must immediately change it on the Policy Controller. Otherwise, the Network VCAC may not function properly.

For the Policy Controller configuration information, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

Use this procedure to change the attributes of one of the following existing network service zones defined for the CS 2000 system:

- IP -VPN network address translator (NAT) zone

  A NAT device is used to provide the gateways with a temporary public address.

- limited bandwidth link (LBL) zone

  An LBL is a virtual representation of a link identified in the network that has restricted capacity and which warrants bandwidth management.

- composite NAT and LBL zone

  A composite zone contains both NAT and LBL. Use this option only when your network configuration includes the Policy Controller, and the Network VCAC status is ON.

For information about the role of NAT devices, refer to procedure Add an IP-VPN (NAT) zone on page 317.

For more information on LBLs, refer to procedure Add a limited bandwidth link (LBL) zone on page 331.

In a network configuration that includes the Policy Controller (Network VCAC status: ON), the only attribute that you can change for any network zone is the parent zone setting.

In a network configuration without the Policy Controller (Network VCAC status: OFF), you can also change the resource usage (RU) profile and the Max Count value for an LBL zone.

When to use this procedure

Use this procedure when you need to change the attributes of a service zone in your network.

Prerequisites and guidelines

The following prerequisites apply to this procedure:

- You must already have a network zone configured.
- If you are changing the parent zone, the new parent zone must already be configured on the CS 2000.

The following guidelines apply to this procedure:

- You cannot change the name of an existing network zone.
- Whether or not the zone is shared cannot be changed.
- You may change the parent zone setting of an existing network zone even if a media gateway that uses this zone is associated with a GWC. The changes to the zone will be reflected on the GWC.
- For any network zone in a network with the Policy Controller, you can only change the parent zone setting.

ATTENTION

Do not attempt to remove the top-most IP-VPN (NAT) zone if it is associated with one of the following gateways:

- H.323 gateway

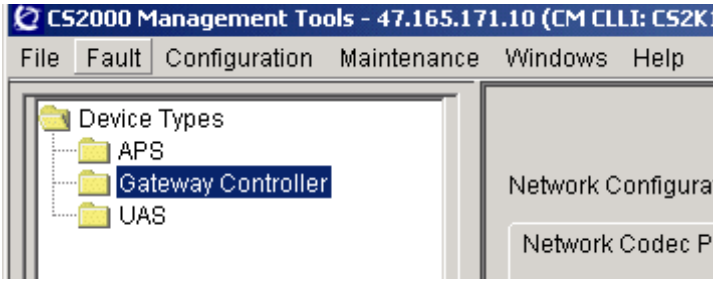
- any small line gateway configured with IP address other than 0.0.0.0

For these gateways, the IP address is not discovered; it is manually provisioned when associating the gateway with a GWC. Changing or removing the NAT zone would cause the gateway IP address to become invalid, since the gateway would now be in a different IP address space. For this reason, this operation is not allowed.

Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

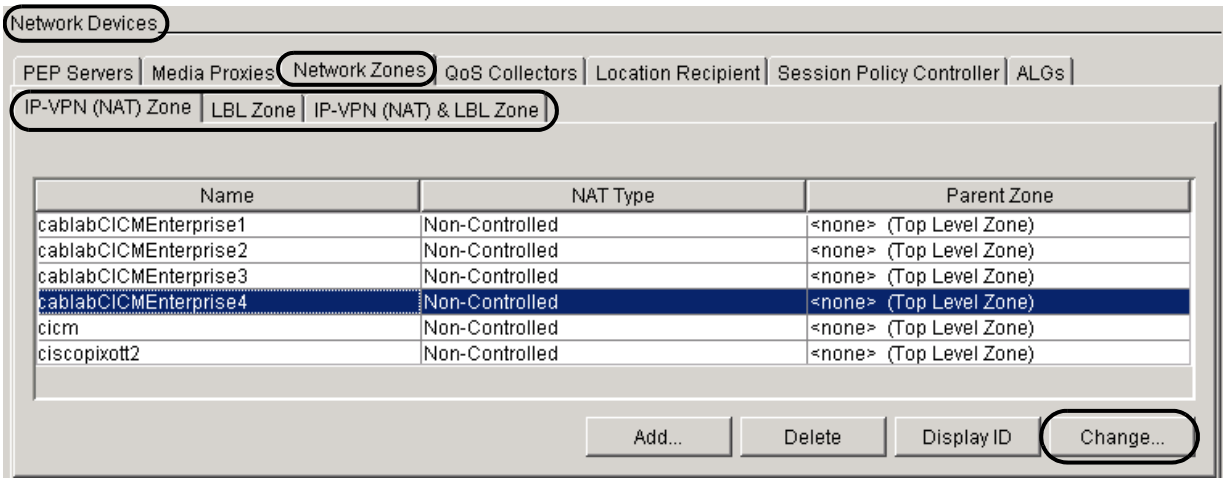


2 At the Network Devices panel click the **Network Zones** tab.

3 Click the appropriate tab to select the zone that you want to display; for example, **IP-VPN (NAT) Zone** tab.

4 At the selected zone panel, select the zone that you want to change.

Your selection is highlighted.



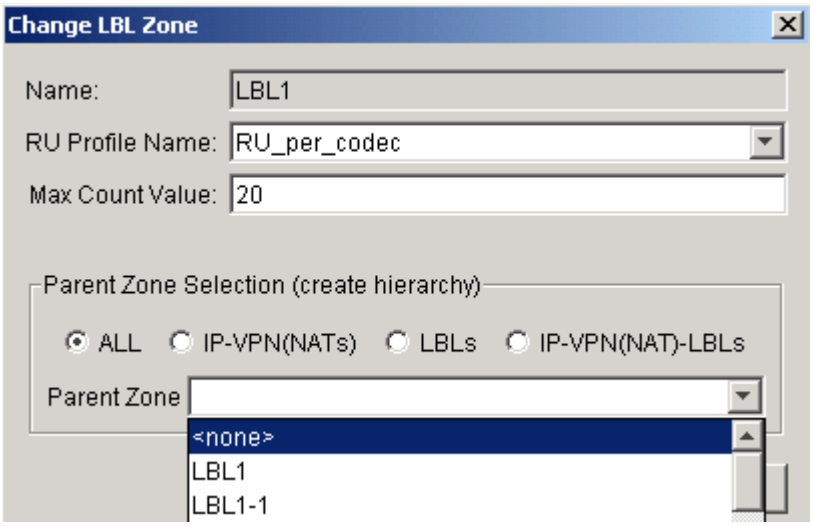
5 Click the **Change** button to display the appropriate Change <zone> Zone dialog box; for example, Change LBL Zone dialog box.

Use the following table to determine your next step.

If you are changing the attributes of	Do
an IP-VPN (NAT) or a composite IP-VPN(NAT) & LBL zone	go to step 7
an LBL zone, in a network with the Policy Controller (Network VCAC status: ON)	go to step 7
an LBL zone, in a network without the Policy Controller	go to step 6

6 At the displayed Change LBL Zone dialog box, change the applicable fields using the following sub-steps.

Note: The name of the LBL zone cannot be changed.



a In the RU Profile Name: field, click the drop-down menu to change the resource usage (RU) profile to be used for the selected LBL zone

Only RU profiles already configured will appear in the drop-down list. To view the details of existing RU profiles, click the **VCAC Resource Usage** button under Network Configuration.

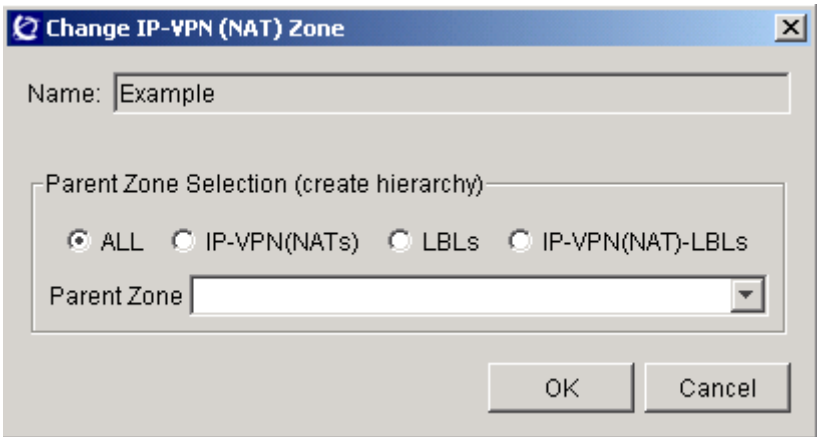
b In the Max Count Value: field, change the call set-up capacity through the link. The call set-up capacity must be compared against the contents of the RU profile selected in the previous step.

7 In the "Parent Zone Selection (create hierarchy)" section of the displayed <zone> Zone dialog box, change the parent zone setting to another zone or to <none>, using the following sub-steps.

Note 1: The following example shows the Change IP-VPN (NAT) Zone dialog box.

Note 2: The name of the zone cannot be changed.

Note 3: Whether or not the zone is shared cannot be changed.



a Select one of the radio buttons to choose the scope of your zone selection. The options are:

- ALL - includes all zones
- IP-VPN(NATs) - restricts the selection to IP-VPN (NAT) zones
- LBLs - restricts the selection to LBL zones
- IP-VPN(NAT)-LBLs - restricts the selection to composite NAT-LBL zones

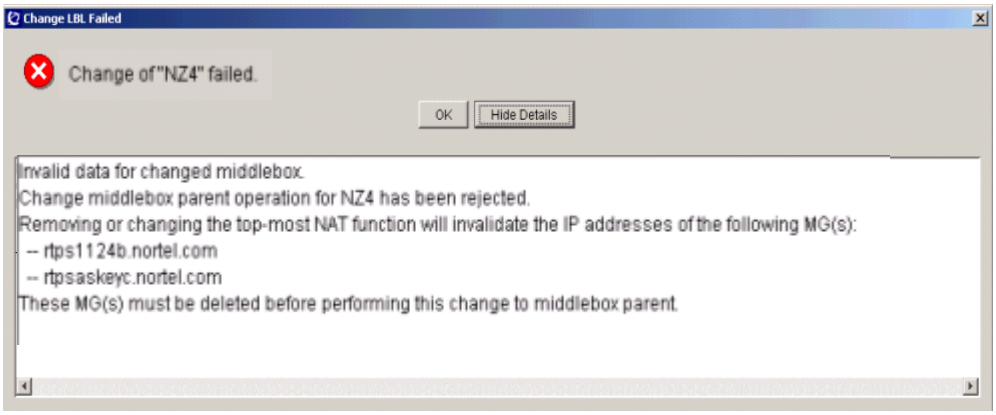
b Click in the Parent Zone field.

c If desired, type text characters of a zone name in the field to fine tune your display. The system displays all zones with a name that matches any of the characters you type.

d Select a new parent zone for the selected zone from the list in the drop-down menu.

8 Click the **OK** button at the bottom of the dialog box to accept the changes.

Note: If you attempted to remove the top-most IP-VPN (NAT) zone associated with an H.323 gateway or any small line gateway configured with IP address other than 0.0.0.0, the system displays the following error message.



You must remove and reconfigure the gateways indicated in this message, then complete this procedure again.

9 Confirm that the changed settings appear in the selected zone table.

10 The procedure is complete.

View a network zone ID

Purpose of this procedure

Use this procedure to display a zone ID of the selected network service zone. Each zone supports one of the following types of network services:

- network address translator (NAT) - used by a CS 2000 to communicate with gateways in the network
- limited bandwidth link (LBL) - used by a CS 2000 for virtual call admission control (VCAC) - in a network configuration that does not include the Policy Controller, the Network VCAC status is OFF
- composite NAT and LBL zone (for network sides that include both NATs and LBLs)

  Note: This option applies when your network configuration includes the Policy Controller and the Network VCAC status is ON.

When to use this procedure

Use this procedure when you need to view the zone ID of a selected network zone.

Prerequisites and guidelines

The following prerequisites and guidelines apply to this procedure:

- The LBL, NAT, or composite NAT-LBL zone must already exist in the CS 2000 network and must be configured using the CS 2000 GWC Manager.

  Note: For information on how to add an appropriate network service zone, refer to one of the following procedures:

  — Add a limited bandwidth link (LBL) zone on page 331

  — Add an IP-VPN (NAT) zone on page 317

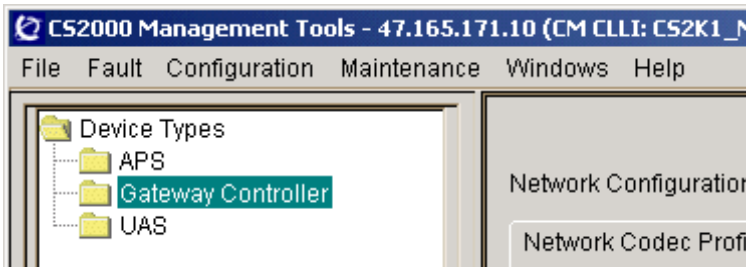
  — Add a composite IP-VPN (NAT) and LBL zone on page 343

- If you need to view a zone ID in order to configure another CS 2000 to share the same zone, you need to first perform the procedure Set the call agent identifier on page 67 for each CS 2000 in your network.

Action

At CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

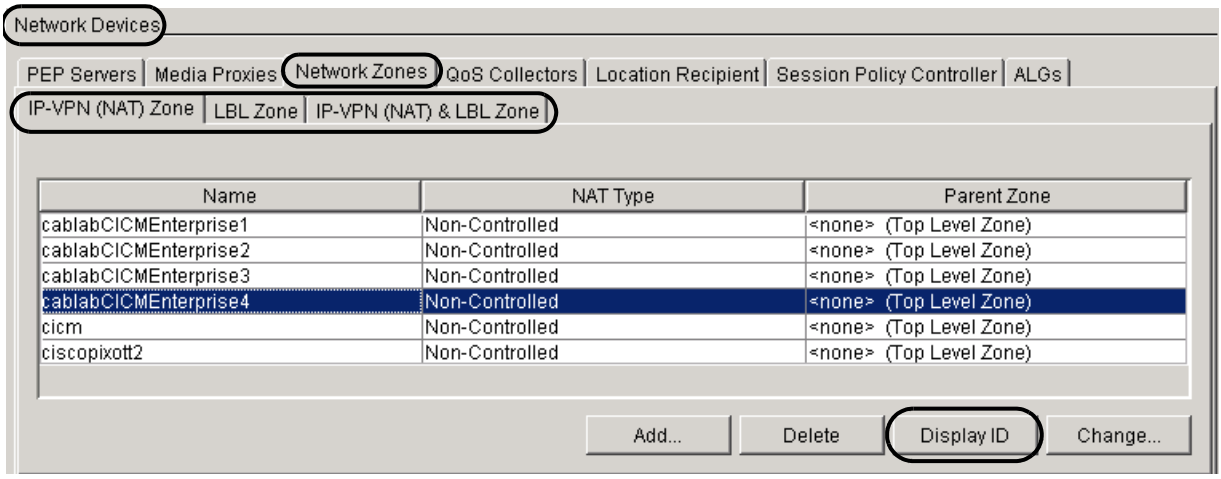


2 At the Network Devices panel click the **Network Zones** tab.

3 Click the appropriate tab to select the zone that you want to display; for example, **IP-VPN(NAT) Zone** tab.

4 At the selected zone pane, select one of the zones listed.

Your selection is highlighted.



5 Click the **Display ID** tab.

The system displays the zone ID for the zone selected in step 4, for example:

6 Click the **OK** button to close the Zone ID window.

7 The procedure is complete.

Delete a network service zone

Purpose of this procedure

ATTENTION

If your network configuration includes the Policy Controller, all IP-VPN (NAT), LBL, and composite IP-VPN (NAT) and LBL zones must be configured identically; first on the CS 2000 system through the GWC Manager or the OSSGate, then on the Policy Controller. Once you delete a network zone from the CS 2000 system, you must immediately delete it from the Policy Controller. Otherwise, the Network VCAC may not function properly.

For information on how to delete a zone from the Policy Controller, refer to the *Policy Controller Configuration Management* NTP, NN10432-511.

Use this procedure to delete one of the following network service zones from your network:

- IP-VPN network address translator (NAT) zone

  A NAT device is used to provide the gateways with a temporary public address.

- limited bandwidth link (LBL) zone

  An LBL is a virtual representation of a link identified in the network that has restricted capacity and which warrants bandwidth management.

- composite IP-VPN (NAT) and LBL zone

  A composite zone contains both NAT and LBL. Use this option only when your network configuration includes the Policy Controller, and the Network VCAC status is ON.

When to use this procedure

Use this procedure when you wish to remove one or more network zones from the network database.

Prerequisites and guidelines

The following prerequisites apply to this procedure:

- A network zone cannot be deleted if it is associated with a media gateway as an adjacent zone.

  Before attempting to delete a zone, remove all media gateway associations with it. Refer to procedure Disassociate a media gateway on page 305 to perform this activity.

- A zone cannot be deleted if it is configured as a parent zone for another network zone.

  Before attempting to delete a zone, ensure that it is not configured as a parent zone for another network zone. To change the parent zone setting of a selected network zone, refer to procedure Change attributes of a network zone on page 349.

The following guidelines apply when deleting a network zone.

If a network zone ID has been configured on more than one CS 2000 (that is, if the zone is shared), you must delete instances of the zone in the following order:

1. Delete the zone ID from all CS 2000s on which the zone ID was *manually* assigned during the network zone configuration (using the Shared Zone check box).

   If the zone is manually configured on more than one CS 2000, it does not matter which instance of the zone you remove first.

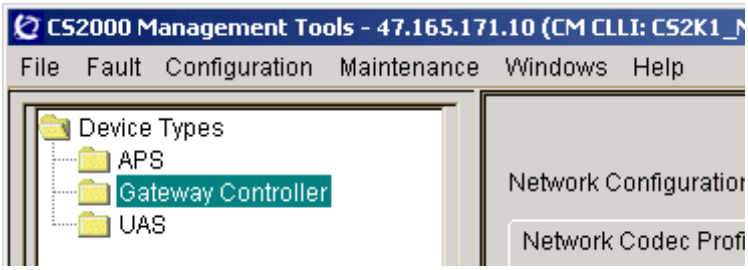
2. After all manually configured instances of the zone are removed, delete the zone ID from the CS 2000 on which the zone ID was automatically assigned by the system.

   This step refers to the CS 2000 on which the zone was originally configured.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

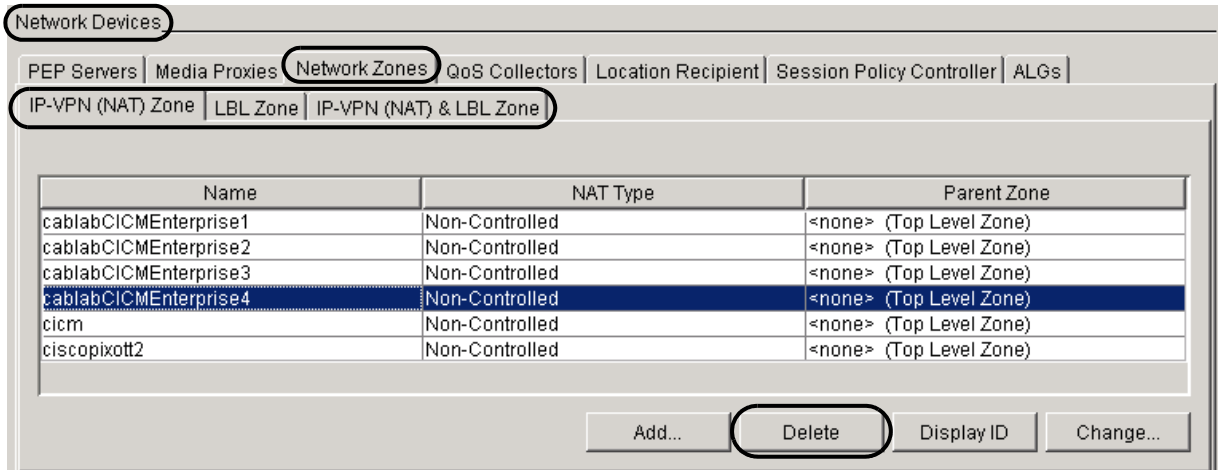


2 From the Network Devices panel click the **Network Zones** tab.

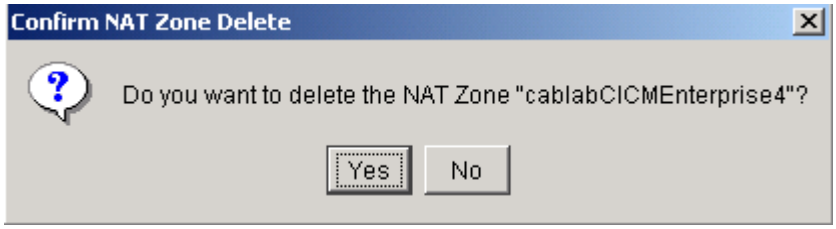
3 Click the appropriate tab to select the zone that you want to display; for example, **IP-VPN(NAT) Zone** tab.

4 Select the zone instance that you want to remove.

Your selection is highlighted.



5 Click the **Delete** button to delete the selected zone.



6 Click **Yes** to confirm the deletion.

The deletion will not work and the system will return an error message if any of the previously described prerequisites are not met. Refer to section Prerequisites and guidelines on page 360.

If you encounter errors in trying to remove a zone, contact your site system administrator.

7 Confirm that the selected network zone instance is removed from the appropriate zone display.

8 The procedure is complete.

Add a media proxy

Purpose of this procedure

Use this procedure to add one or more media proxies to perform network address translation (NAT) traversal. A media proxy device is used as an real-time internet protocol (RTP) portal to allow a gateway in one domain to communicate with another gateway in another domain. A pool of media proxies can be made available to perform the NAT traversal functions.

When to use this procedure

Use this procedure when you wish to add one or more media proxies to the network for use in performing NAT traversal.

Note: Starting in SN07, there is no longer a requirement to configure a media proxy for every GWC. Only those GWCs controlling endpoints outside the carrier's private network require media proxies. For example, only GWCs controlling MGCP integrated access devices (IAD), Centrex IP clients, H.323 GWs and SIP require a media proxy. GWCs controlling H.248 trunking gateways, MG 9000 gateways, universal audio servers (UAS) do not require a media proxy.

Prerequisites and guidelines

One or more physical NAT devices can be configured as a single logical NAT-type network zone for each media gateway.

The data for a NAT zone will be sent down to GWC when the zone is associated to a media gateway. The data for a media proxy will be sent down to the GWC when the media proxy is associated with a GWC. Media proxies are configured using the Multimedia Communications System (MCS) Manager application. Refer to the MCS documentation for details.

There is only one NAT exit point from a local network. If two gateways are behind the same NAT, then they can set up a call without requiring a media proxy.

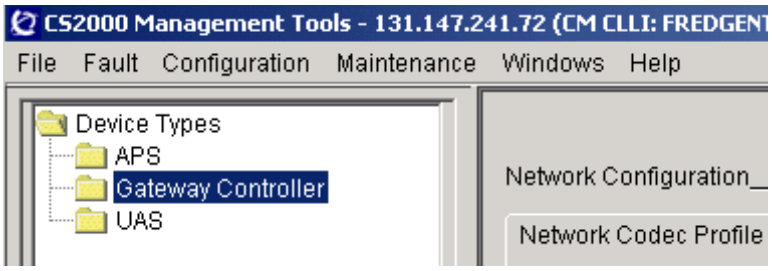
The Integrated Access Cable solution uses DQoS and PEP Servers while the Integrated Access Wireline solution uses internet transparency (ITRANS) and NAT-type network service zones as media proxies. These two solutions are mutually exclusive as defined in the gateway profile service type. In other words, DQOS and ITRANS cannot be defined together in a single GWC profile when associating media gateways to a GWC.

In the Carrier Centrex IP environment, an RTP Media Portal acts as a media proxy to bridge the RTP paths between endpoints for RTP media NAT traversal. The CS 2000 inserts the RTP Media Portal if the endpoints of the RTP media path are not in the same virtual private network (VPN). For example, calls between two enterprises, or calls from an enterprise H.323 gateway to a gateway on the carrier's packet network would require the insertion of a the RTP Media Portal.

Action

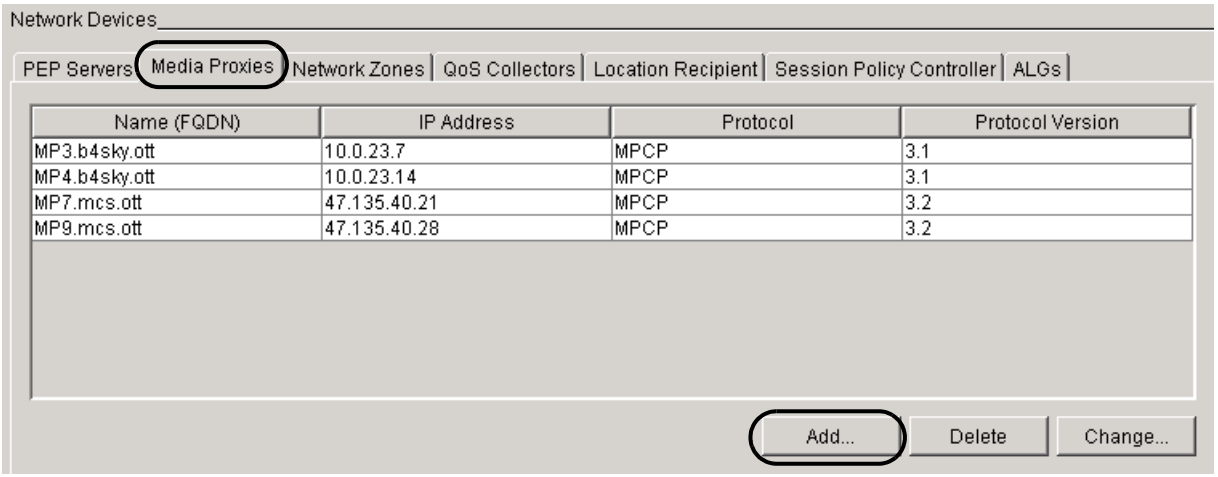
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

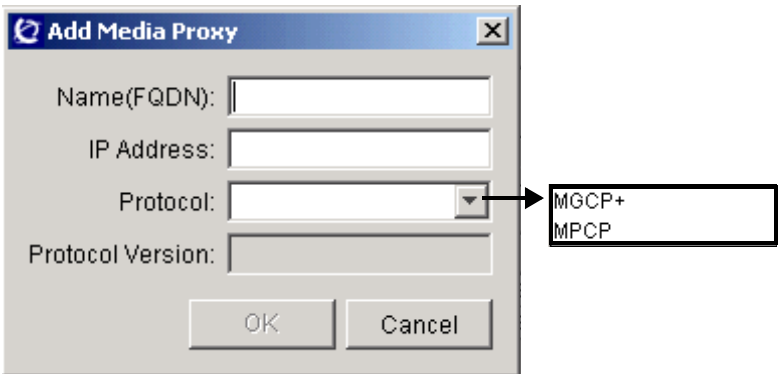


2 From the Network Devices panel click the **Media Proxies** tab to display the Media Proxies pane.

3 Click the **Add** button.



4 At the Add Media Proxy dialog box, enter the applicable configuration information, then click the **OK** button.



a In the Name (FQDN) field, type the network name of the proxy device in a fully qualified domain name (FQDN) format.

Use a domain name of the proxy device in the form of an absolute domain name including the host name of the device, suitable for lookup using Directory Name Service (DNS).

b In the IP Address field, type the IP address associated with the proxy device.

c In the Protocol field, select the connection control Protocol using the drop-down menu. MGCP+ version 2.0 and MPCP version 3.1 are supported.

Note: Support for MGCP+ version 2.0 is intended for the purpose of upgrading to SN07. Once your system is upgraded to SN07, use MPCP version 3.1.

The Protocol Version field is selected automatically based on the protocol chosen.

d Click the **OK** button.

Note: If you encounter errors in trying to add the proxy device, contact your site system administrator.

5 Verify that the new media proxy appears in the display.

6 The procedure is complete.

View media proxy configuration data for a GWC node

Purpose of this procedure

Use this procedure to view media proxy configuration data for a selected GWC node.

When to use this procedure

Use this procedure when you require specific configuration information about media proxies associated with a specific GWC node.

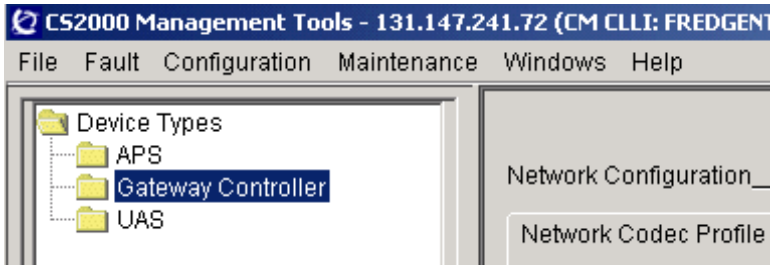
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

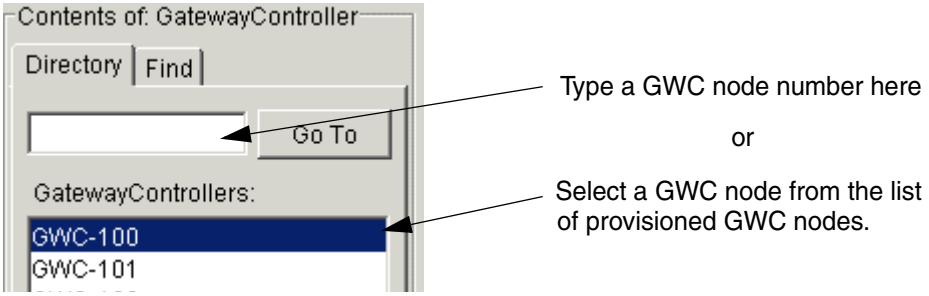
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



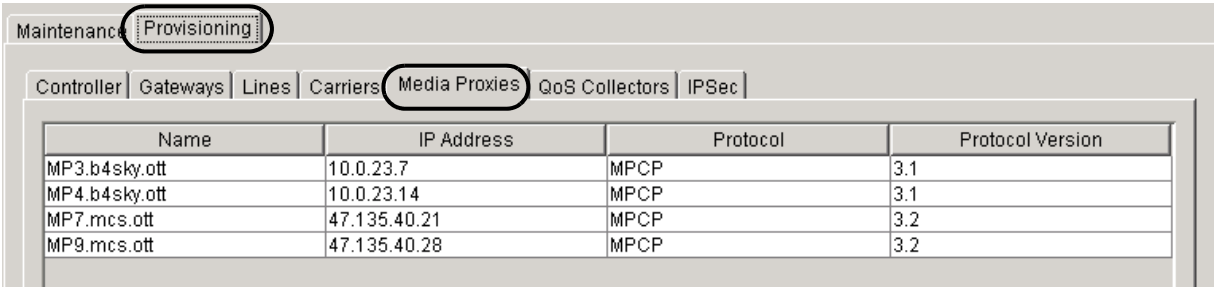
2 From the Contents of: Gateway Controller frame, select the GWC node that has a media proxy you wish to view.



3 Click the **Provisioning** tab in the GWC node view.

If necessary, click the **Controller** tab to view general node provisioning information for the GWC node.

4 Click the **Media Proxies** tab in the Provisioning panel to view information about media proxies associated with the selected GWC node.



5 The procedure is complete.

Modify a media proxy

Purpose of this procedure

Use this procedure to change the IP address or the control protocol version of a media proxy device already defined in the network.

A media proxy device acts as an RTP portal to allow a gateway in one domain to communicate with another gateway in another domain.

When to use this procedure

Use this procedure when you wish to change the IP address or the control protocol version of a media proxy in the network.

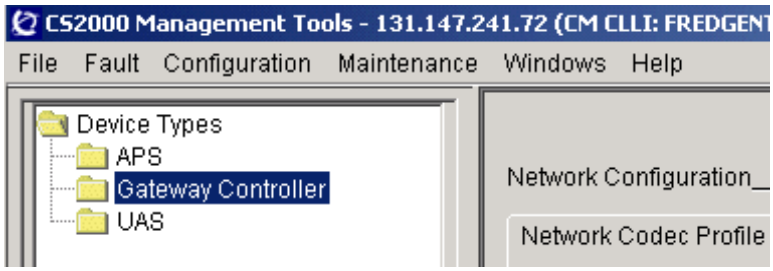
Prerequisites and guidelines

The media proxy you are changing must be configured with a valid IP address and control protocol.

Action

At the CS 2000 GWC Manager client workstation

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

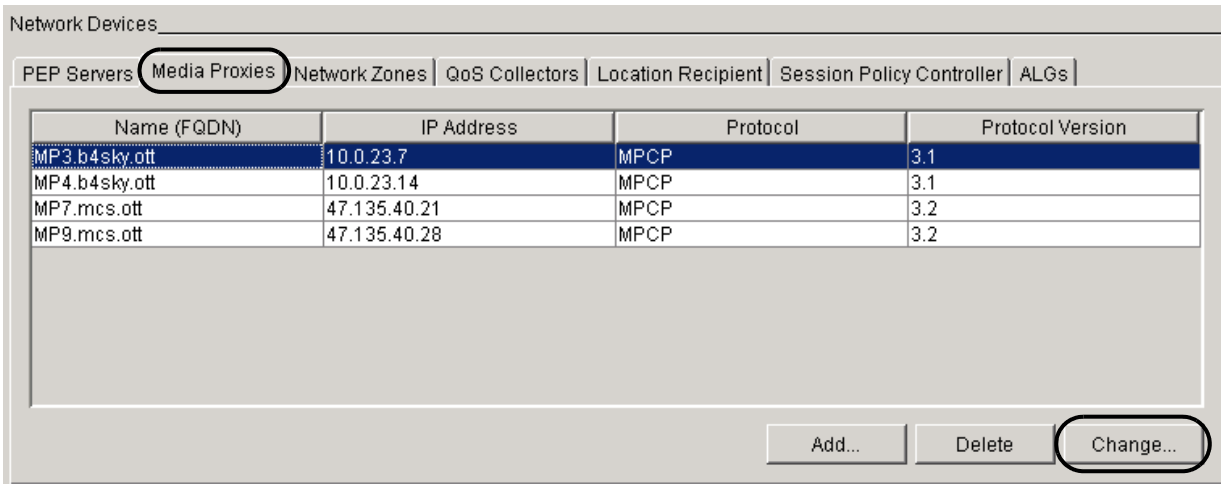


2 At the Network Devices panel, click the **Media Proxies** tab to display the Media Proxies pane.

3 Select the media proxy you wish to modify.

Your selection is highlighted.

4 Click the **Change** button to display the Change Media Proxy dialog box.



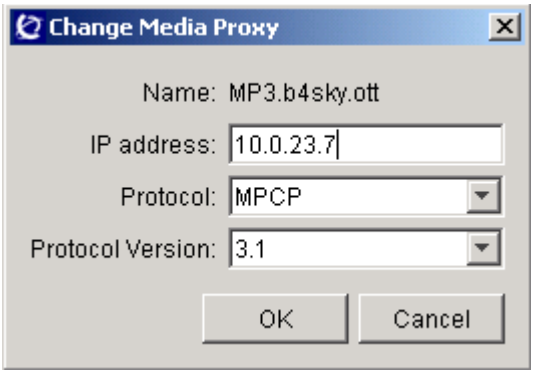
5 At the Change Media Proxy dialog box, enter the following data:

- In the IP address: field, type a new IP address.

  Note: Ensure that you are entering a valid IP address for the proxy device.

- In the Protocol: field, select a different control protocol using the drop-down menu.

  MGCP+ version 2.0 and MPCP version 3.1 are supported.



6 Click the **OK** button.

Note: If you encounter errors while attempting to change the proxy device, contact your site system administrator.

7 Verify that the changes are reflected in the Media Proxies display.

8 The procedure is complete.

Associate a media proxy with a GWC node

Purpose of this procedure

Use this procedure to associate a media proxy device, including an RTP Media Portal, to a selected GWC node. The action of associating a media proxy to a GWC node sends the datafill for the media proxy device to the GWC database.

In the Carrier Centrex IP environment, an RTP Media Portal acts as a media proxy to bridge the real-time protocol (RTP) paths between endpoints for RTP media network address translation (NAT) traversal. The CS 2000 inserts the RTP Media Portal if the endpoints of the RTP media path are not in the same virtual private network (VPN). For example, calls between two enterprises, or calls from an enterprise H.323 gateway to a gateway on the carrier's packet network would require the insertion of a the RTP Media Portal.

When to use this procedure

Use the procedure when you need to associate a media proxy with a selected GWC node.

Prerequisites and guidelines

The following prerequisites apply to associating media proxies with GWC nodes.

- You must add the media proxy to the network using procedure Add a media proxy on page 363 before you can associate the media proxy with a GWC node.
- Media proxies should be configured on the Multimedia Communications System (MCS) using the MCS Manager application before they are associated with the GWC. Refer to the MCS documentation for details.

The following guidelines apply to associating media proxies with GWC nodes.

- Using MGCP, a single media proxy can be associated with up to 5 GWC nodes.
- Using MPCP, a single media proxy can be associated with up to 20 GWC nodes.

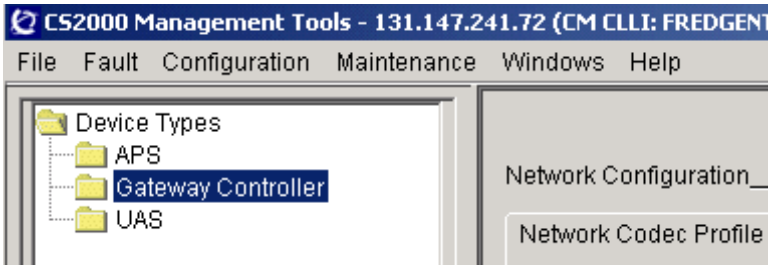
  Note: A media proxy that has reached its limit of associations to GWC nodes will not be available on the CS 2000 GWC Manager if you attempt to associate the media proxy to another GWC node.

- For both MGCP and MPCP, a maximum of 20 media proxies can be associated with a single GWC node.

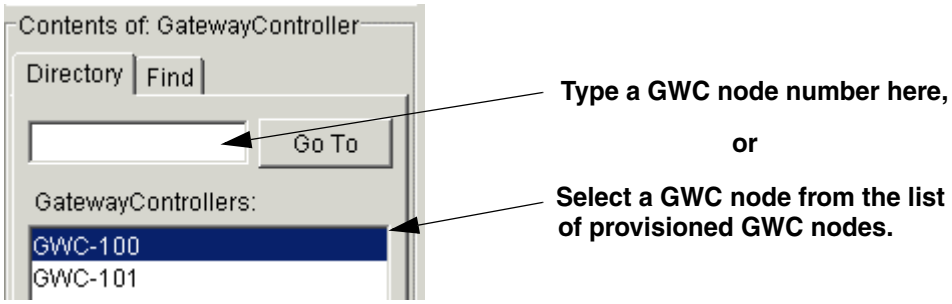
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate media proxy.

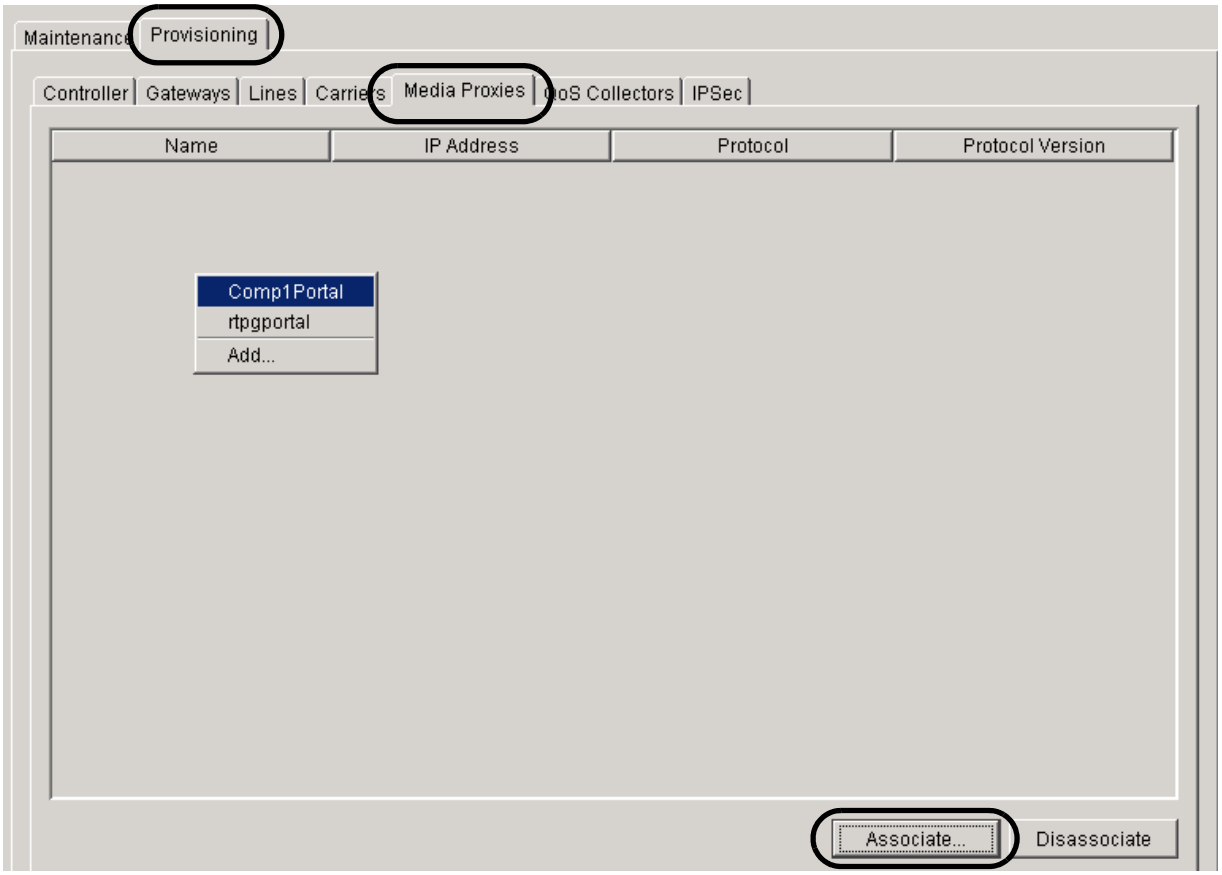


3 Click the **Provisioning** tab in the GWC node view.

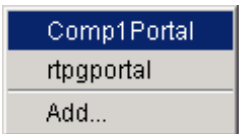
4 Click the **Media Proxies** tab in the Provisioning panel.

5 Note the name of any media proxies currently associated with the selected GWC node as shown in the following panel.

Note: A maximum of 20 media proxies can be associated to a single GWC node.



6 Click the **Associate** button in the lower part of the Media Proxies pane and refer to the following table to determine your next step.

If	Do
the system indicates that you have no media proxies configured in your network, as shown below: 	step 7
Or, if you wish to add a media proxy that is not yet configured in the network	
the system indicates that you do have media proxies configured in your network, as shown below: 	step 8

7 If no media proxy devices are available or if you wish to add a different media proxy that is not yet configured in the network, perform the following sub-steps:

a Click the **Add** button at the prompt.

b Complete the relevant steps in procedure Add a media proxy on page 363.

c Return to step 6 of this procedure and continue.

8 Select an media proxy from the list of available devices.

9 Verify that the media proxy device appears in the Media Proxies pane.

10 The procedure is complete.

Disassociate a media proxy from a GWC node

Purpose of this procedure

Use this procedure to disassociate a media proxy device from a selected GWC node. The action of disassociating a media proxy from a GWC node will remove the media proxy device datafill from the GWC database.

When to use this procedure

Use this procedure when you need to disassociate a media proxy from a GWC node.

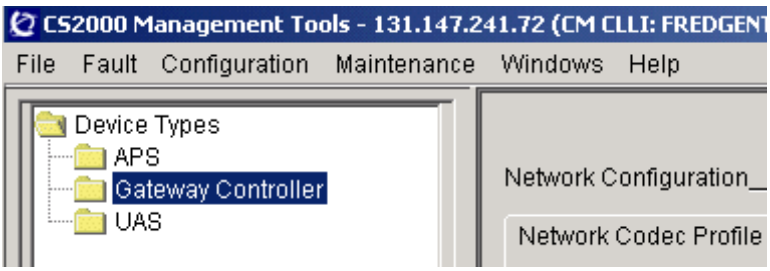
Prerequisites and guidelines

The media proxy must be associated with a GWC node before it can be disassociated.

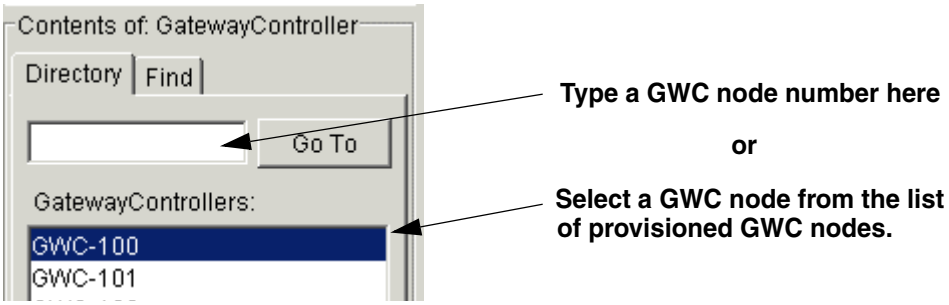
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to disassociate a media proxy from.



3 Click the **Provisioning** tab in the GWC node view.

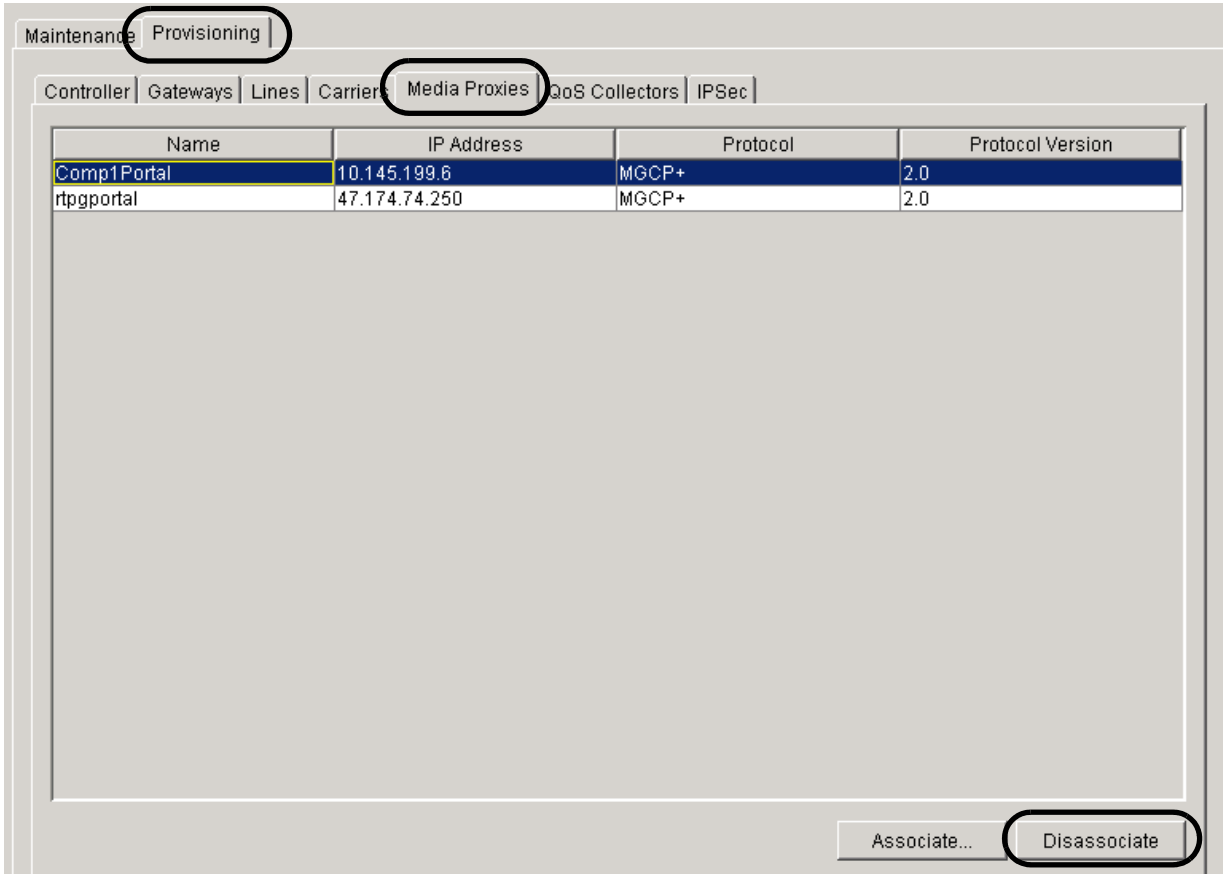
4 Click the **Media Proxies** tab in the Provisioning panel.

5 Select the media proxy you wish to disassociate from the list of media proxies currently associated with the GWC node. then

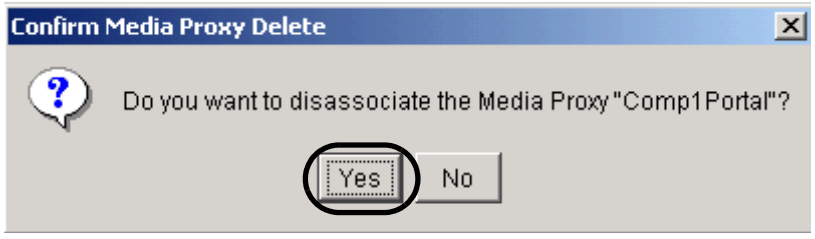
Your selection is highlighted.

Note: If you wish to disassociate multiple media proxies, they can only be disassociated one at a time.

6 Click the **Disassociate** button at the bottom of the screen.



7 Click **Yes** to confirm that you wish to disassociate the media proxy device from the selected GWC node.



8 Verify that the media proxy device is removed from the Media Proxies view.

9 The procedure is complete.

Delete a media proxy

Purpose of this procedure

Use this procedure to delete a media proxy from the network. A media proxy device acts as an RTP portal to allow a gateway in one domain to communicate with another gateway in another domain.

When to use this procedure

Use this procedure when you wish to remove one or more media proxies from your network.

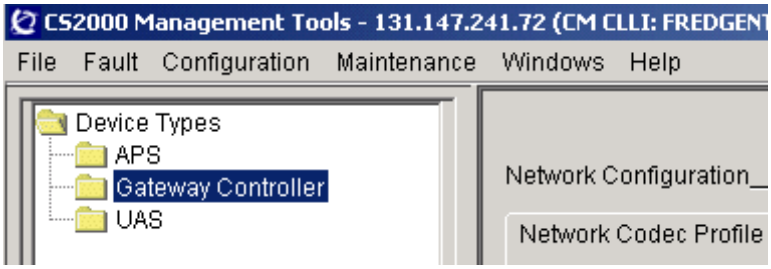
Prerequisites and guidelines

Before deleting a media proxy device, ensure that all GWC node associations with the device are removed. Refer to procedure Disassociate a media proxy from a GWC node on page 377.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

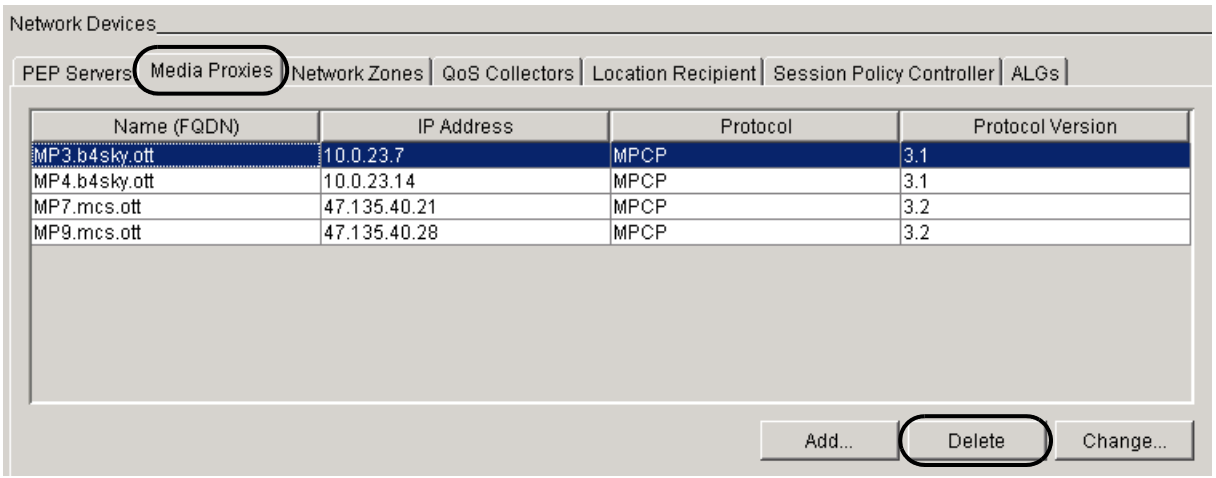


2 At the Network Devices panel, click the **Media Proxies** tab to display the Media Proxies pane.

3 Select the Proxy you wish to remove.

Your selection is highlighted.

4 Click the **Delete** button.



5 At the Confirm Media Proxy Delete dialog box, confirm that you want to delete the selected media proxy by clicking the **Yes** button.

Note 1: You cannot delete a media proxy device that is currently associated with a GWC node.

Note 2: If you encounter errors attempting to remove the proxy device, contact your site system administrator.

6 Verify that the media proxy is removed from the Media Proxies table.

7 The procedure is complete.

Add a quality of service (QoS) collector

Purpose of this procedure

Use this procedure to add a quality of service (QoS) collection device running a QoS collection application to the network. The QoS collector receives end-of-call quality of service statistics from GWCs that have QoS reporting configured and enabled.

Note: QoS is different from dynamic quality of service (DQoS), which relates to policy enforcement and dynamic bandwidth allocation provided in cable networks.

When to use this procedure

Use this procedure when you need to add one or more QoS collector devices to the network, which can be associated with GWC nodes for collecting QoS data.

Use this procedure before associating a specific QoS collector with a GWC node to manage a pool of QoS collector applications.

Prerequisites and guidelines

Only one QoS collection application can be configured on a CS 2000 Management Tools server.

QoS collection must also be enabled on the XA-Core. Refer to procedures in the *CS 2000 Configuration Management* NTP applicable to your solution.

For QoS reporting correlation to billing records, QoS reporting must also be enabled at table AMAOPT in the XA-Core using the MAPCI interface. Refer to procedure “Provisioning in support of QoS reporting” in the *CS 2000 Configuration Management* NTP applicable to your solution.

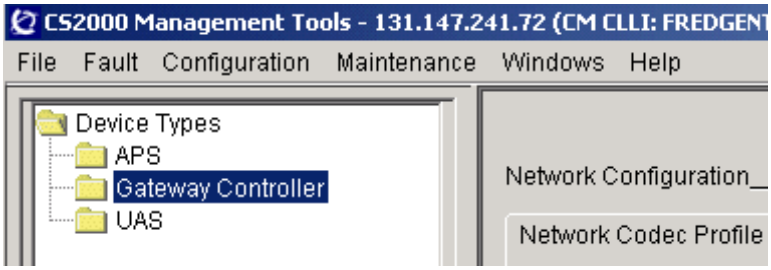
Note: QoS reporting is applicable to ATM and hybrid networks as well as to VoIP networks. Currently, QoS reporting has only been tested using gateways associated with GWC nodes in Carrier VoIP cable solutions.

If you would like to use QoS reporting in a non-cable solution, please contact your Nortel Networks account prime for more support information.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 At the Network Devices panel, click the **QoS Collectors** tab.

3 Click the **Add** button.

4 At the Add QoS Collector dialog box, type the following information:

a In the QoS Collector Name field, type the unique network name of an available, provisioned QoS collector server, preferably in FQDN format.

If necessary, contact your site system administrator for assistance with this task.

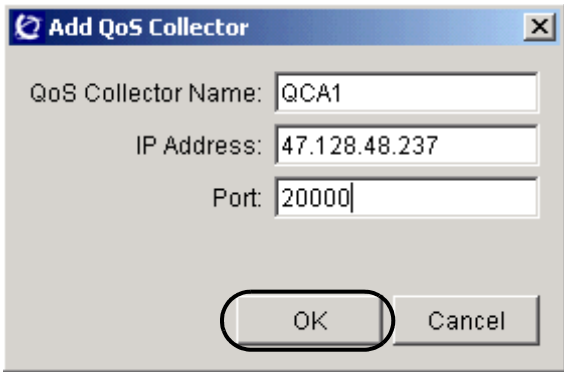
b In the IP Address field, type the IP address of the QoS collector.

c At the Port field, type the port number of the QOS collector. This value must be an integer from 20000 to 20004 inclusive.

Note 1: The QCA name and port number combination must be unique.

Note 2: A QoS collector IP address can have multiple port numbers associated with it. (The same port number can be assigned to different IP addresses.)

d Click the **OK** button.



5 Verify that the new QoS Collector appears in the list of QoS collectors.

6 The procedure is complete.

Associate a QoS collector with a GWC node

Purpose of this procedure

Use this procedure to associate a quality of service (QoS) collection device running a QoS collection application with one or more GWC nodes.

When to use this procedure

Use this procedure when you need to associate a QoS collector device with a GWC node so that QoS data can be collected from the gateways associated with the node.

Prerequisites and guidelines

The QoS collection device you intend to associate with a GWC node must already be configured and added to the CS 2000 network. Refer to procedure Add a quality of service (QoS) collector on page 383 for details.

A GWC node can be associated with a maximum of two QoS collectors.

If QoS reporting is enabled for all GWC nodes, QoS data is sent for all calls. If QoS reporting is enabled for only one or two GWC nodes involved in a call, QoS reports will only be sent for the call leg that includes any GWC nodes that have QoS reporting enabled.

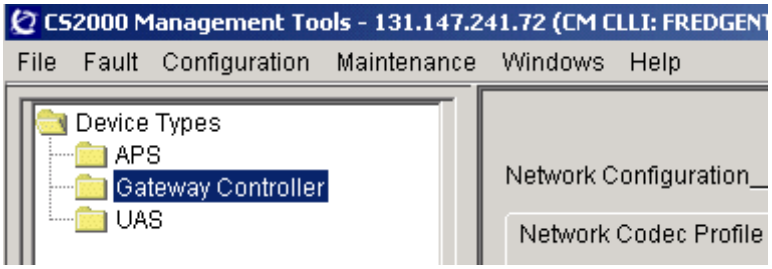
Note: QoS reporting is applicable to ATM and hybrid networks as well as to VoIP networks. Currently, QoS reporting has only been tested using gateways associated with GWCs in Carrier VoIP cable solutions.

If you would like to use QoS reporting in a non-cable solution, please contact your Nortel Networks account prime for more support information.

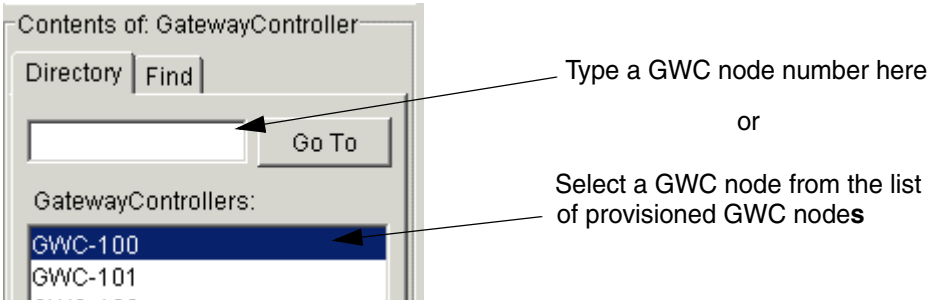
Action

At the CS 2000 GWC Manager client

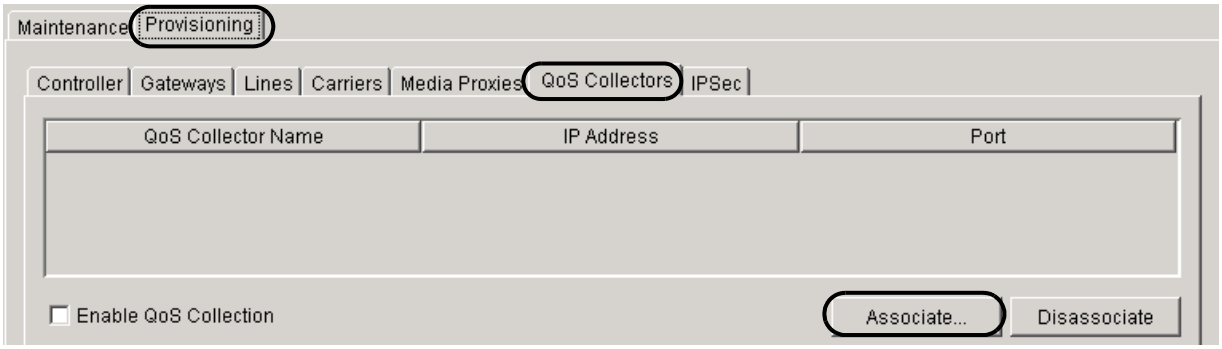
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node with which you wish to associate a QoS collector.



3 Click the **Provisioning** tab, then click the **QoS Collectors** tab.

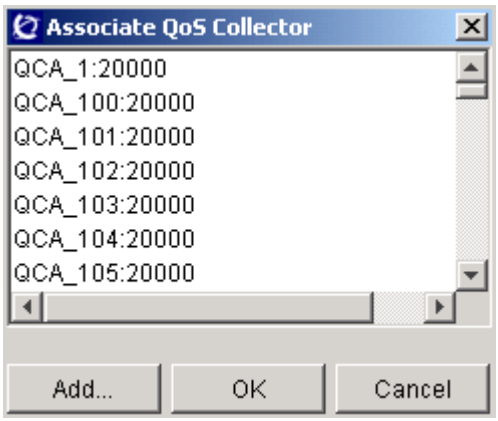


4 Click the **Associate** tab to display the Associate QoS Collector dialog box.

Note: If there are no QoS collectors configured and added to the network, the system displays an error message. Refer to procedure Add a quality of service (QoS) collector on page 383 to add a collector.

5 From the displayed list of QoS collectors in your network, select a collector to associate with the GWC node.

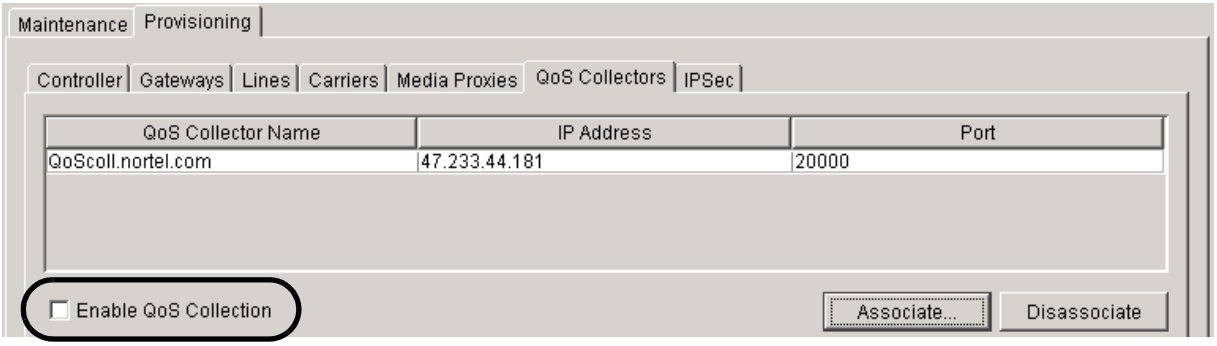
Note: If a particular collector has not yet been added to the network, click the **Add** button and refer to procedure to add a new collector.



6 Click the **OK** button to confirm your selection.

7 Confirm that your selection appears on the list of QoS collectors associated with the GWC node.

8 Select the Enable QoS Collection check box to enable QoS data reporting for this GWC node.



9 If you wish to associate another QoS collector with this GWC node, return to step 5.

10 The procedure is complete.

Enable or disable QoS reporting for a GWC node

Purpose of this procedure

Use this procedure to enable or disable quality of service (QoS) reporting for a GWC node.

When to use this procedure

Use this procedure when you need to start or stop recording QoS data for gateways associated with the node.

Prerequisites and guidelines

At least one QoS Collector must be associated with the GWC node. A maximum of two collectors are allowed. If no QoS Collector is associated with the node, refer to procedure Associate a QoS collector with a GWC node on page 387.

If QoS reporting is enabled for all GWC nodes, QoS data is reported for all calls. If QoS reporting is enabled for only one or two GWC nodes involved in a call, QoS data will be reported for the call leg that includes any GWC nodes that have QoS reporting enabled.

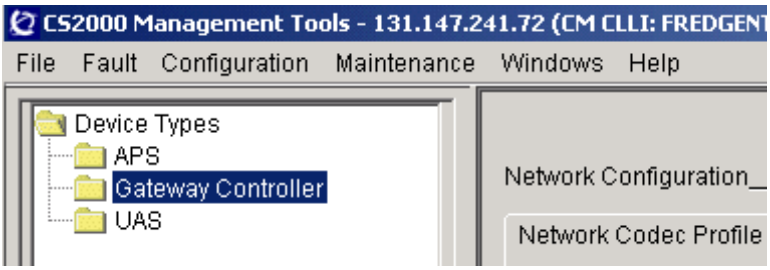
Note: QoS reporting is applicable to ATM and hybrid networks as well as to VoIP networks. Currently, QoS reporting has only been tested using gateways associated with GWCs in Carrier VoIP cable solutions.

If you would like to use QoS reporting in a non-cable solution, please contact your Nortel Networks account prime for more support information.

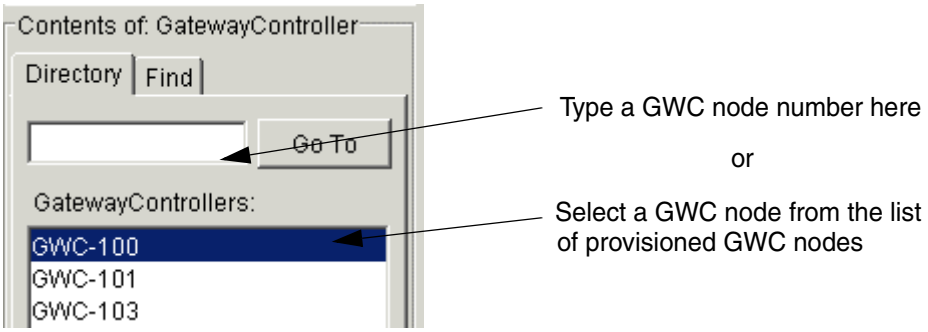
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node for which you wish to enable/disable QoS collection.



3 Click the **Provisioning** tab.

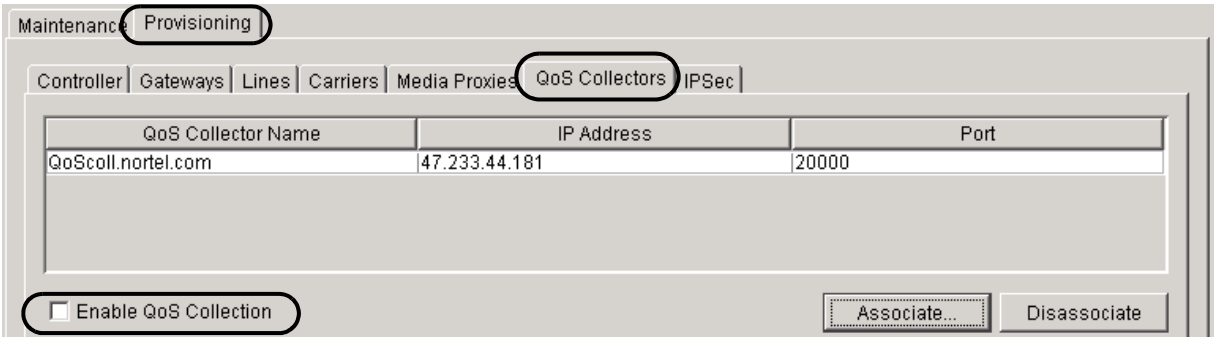
4 Click the **QoS Collectors** tab.

Note: At least one QoS Collector must be associated with this GWC node. A maximum of two collectors are permitted per node.

If no QoS Collector is associate with the node, complete procedure Associate a QoS collector with a GWC node on page 387.

5 Select the Enable QoS Collection check box to enable QoS data reporting for the GWC node.

If QoS collection is already enabled, de-select the Enable QoS Collection check box to disable QoS data reporting for the GWC node.



6 If you wish to enable/disable QoS reporting on another GWC node, return to step 2.

7 The procedure is complete.

View QoS collector configuration data for a GWC node

Purpose of this procedure

Use this procedure to view quality of service (QoS) collector data for a selected GWC node.

When to use this procedure

Use this procedure when you require specific information about the QoS collector associated with a specific GWC node.

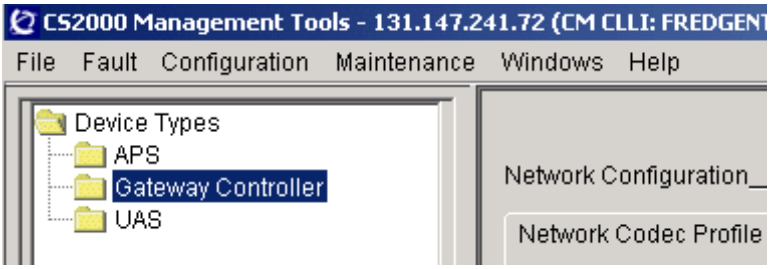
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

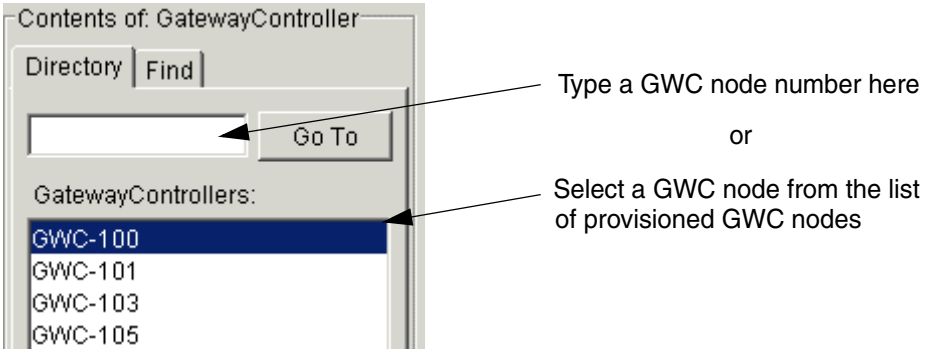
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

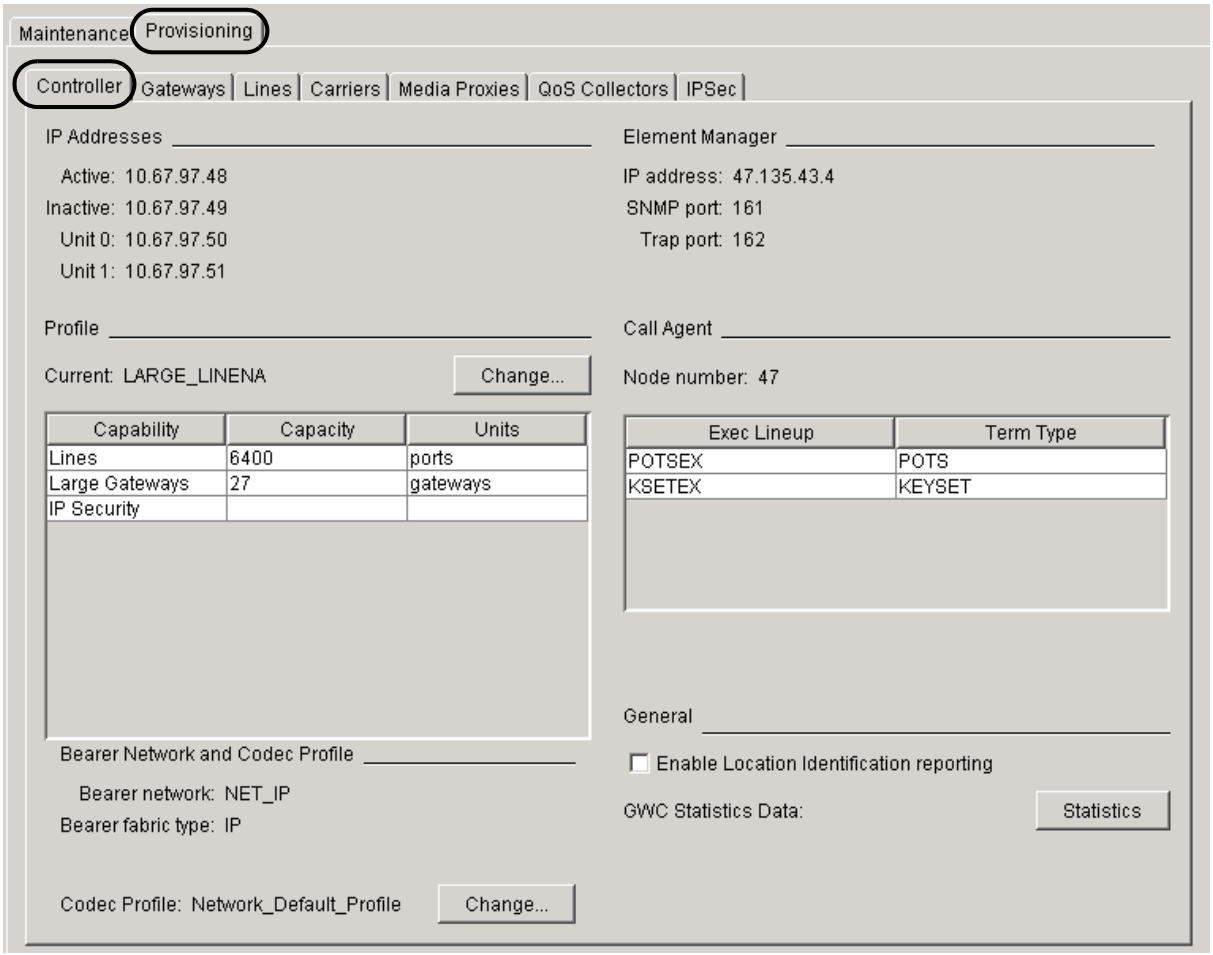


2 Select or type the name of the GWC node that has a QoS collector you wish to view.

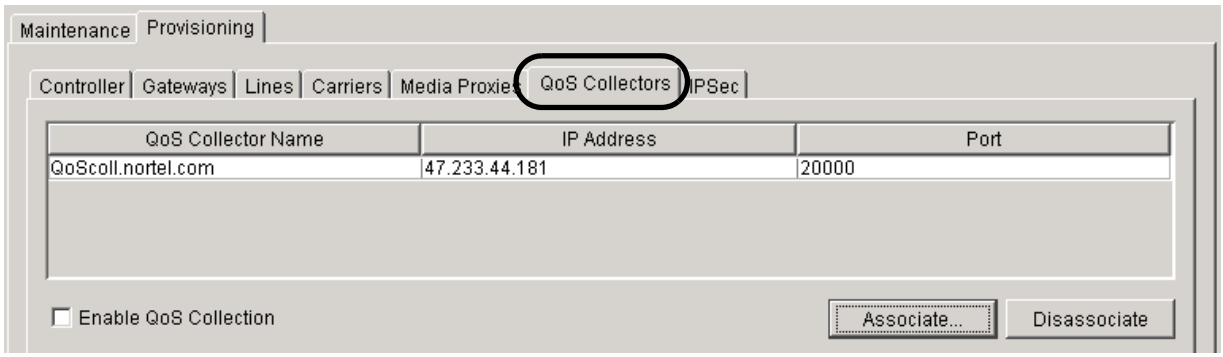


3 Click the **Provisioning** tab.

4 If desired, click the **Controller** tab to view general node provisioning information for the GWC node.



5 Click the **QoS Collectors** tab to view any QoS collector devices associated with the GWC node.



6 The procedure is complete.

Disassociate a QoS collector from a GWC node

Purpose of this procedure

Use this procedure to disassociate a quality of service (QoS) collection device running a QoS collection application from one or more GWC nodes.

When to use this procedure

Use this procedure when you need to disassociate a QoS collector device from a GWC node.

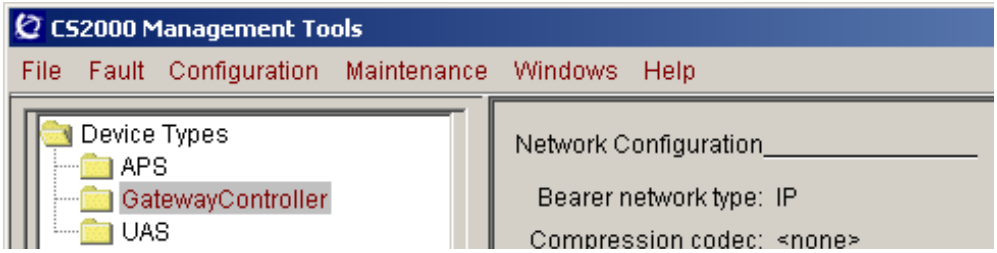
Prerequisites and guidelines

Prior to disassociating a QoS collector device from a GWC node, disable QoS collection for the node. Refer to procedure Enable or disable QoS reporting for a GWC node on page 391.

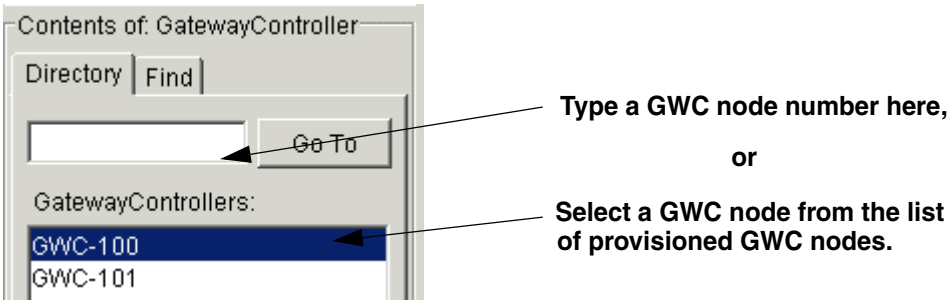
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node from which you wish to disassociate a QoS collector.



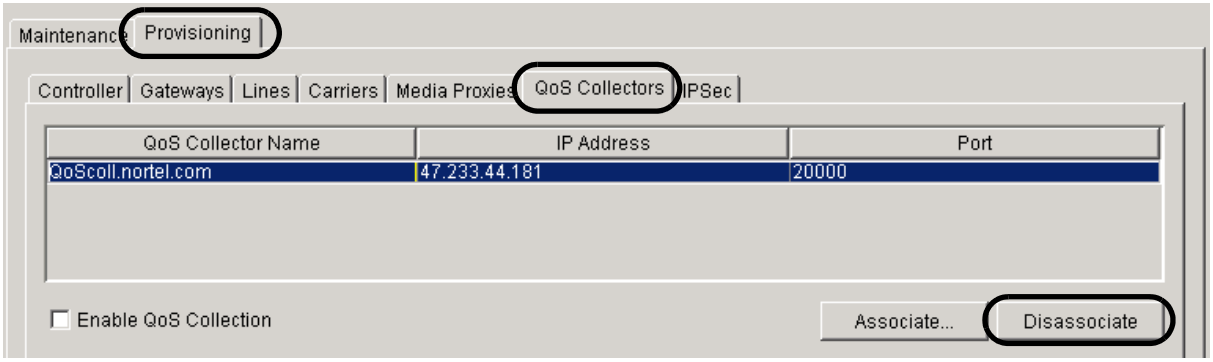
3 Click the **Provisioning** tab.

4 Click the **QoS Collectors** tab.

5 Select a QoS collector from the list.

Your selection is highlighted.

6 Click the **Disassociate** button.



7 Click the **Yes** button to confirm that you wish to disassociate the QoS collector from the GWC node.

8 Verify that the collector has been successfully removed from the list.

9 If you wish to disassociate another QoS collector from this GWC node, return to step 5.

10 The procedure is complete.

Delete a QoS collector

Purpose of this procedure

Use this procedure to remove a quality of service (QoS) collection device from the network.

When to use this procedure

Use this procedure when you need to remove one or more QoS collector devices from the network.

Prerequisites and guidelines

All QoS collectors may be deleted while QoS Reporting is enabled. This will cause the QCA state to change to “enabled pending”.

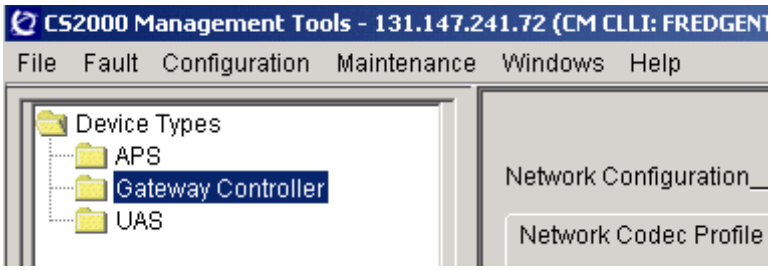
Note: When a QoS collector is deleted from the network database, any GWC node associations is automatically removed.

When deleting a QoS collector, a confirmation dialog box identifies any GWC nodes with which the collector was associated.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

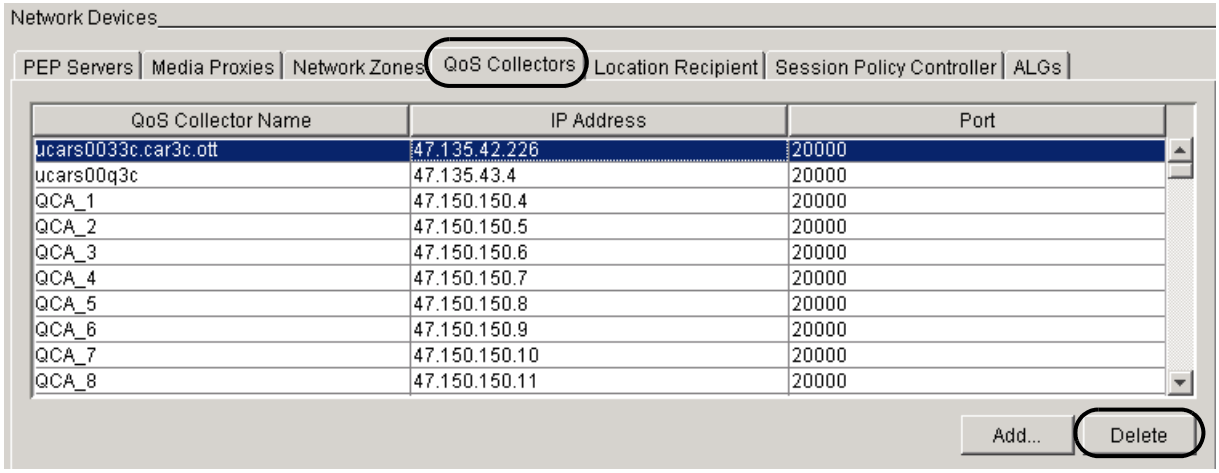


2 At the Network Devices panel, click the **QoS Collectors** tab.

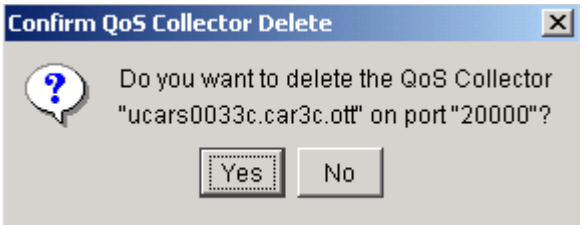
3 Select the QoS collector device to be deleted.

Your selection is highlighted.

4 Click the **Delete** button.



5 Click the **Yes** button to confirm the deletion.

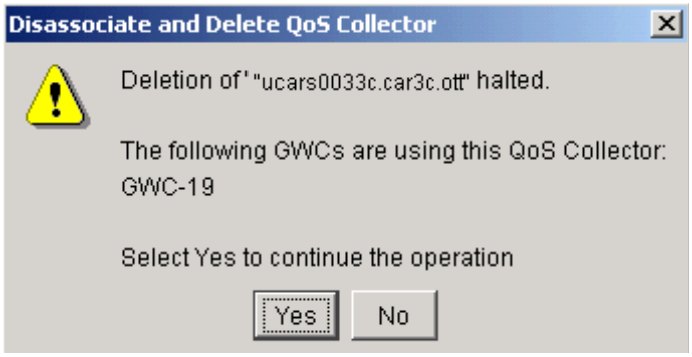


Note: If any GWC nodes are associated with the QoS collector being deleted, you will see a warning box notifying you of the GWC nodes that are using the QoS collector.

You can continue with the deletion by clicking **Yes**, but the QoS collector you are deleting will be removed from any GWC nodes with which it is currently associated. QoS collection for those nodes will be stopped.

To restart QoS collection for any GWC nodes, you must associate a different QoS collector with those GWC nodes.

6 If any GWC nodes are currently using the QoS collector, and you wish to continue the operation, click **Yes** at the Disassociate and Delete QoS Collector prompt.



7 Verify that the QoS Collector has been removed from the list of QoS collectors.

8 The procedure is complete.

Add a policy enforcement point (PEP) server

Purpose of this procedure

Use this procedure to add a policy enforcement point (PEP) server to the network.

A PEP server, also called a middlebox, is associated with small line gateways. The GWC communicates with the PEP server to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.

When to use this procedure

Use this procedure after initial network configuration has been completed and both a DQoS system policy and DQoS subscriber policy have been defined.

Prerequisites and guidelines

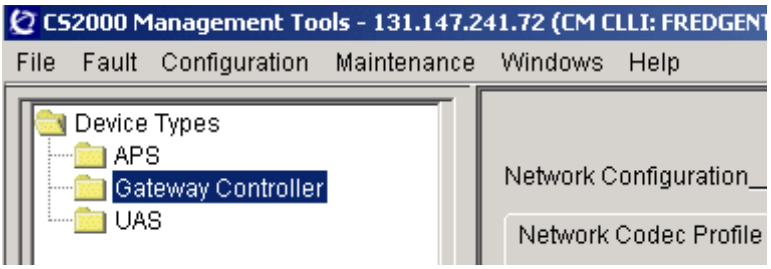
A PEP server must be installed on the network and configured for DNS lookup capability.

A valid PEP server name and IP address must be provided to successfully configure a PEP server in the network.

Action

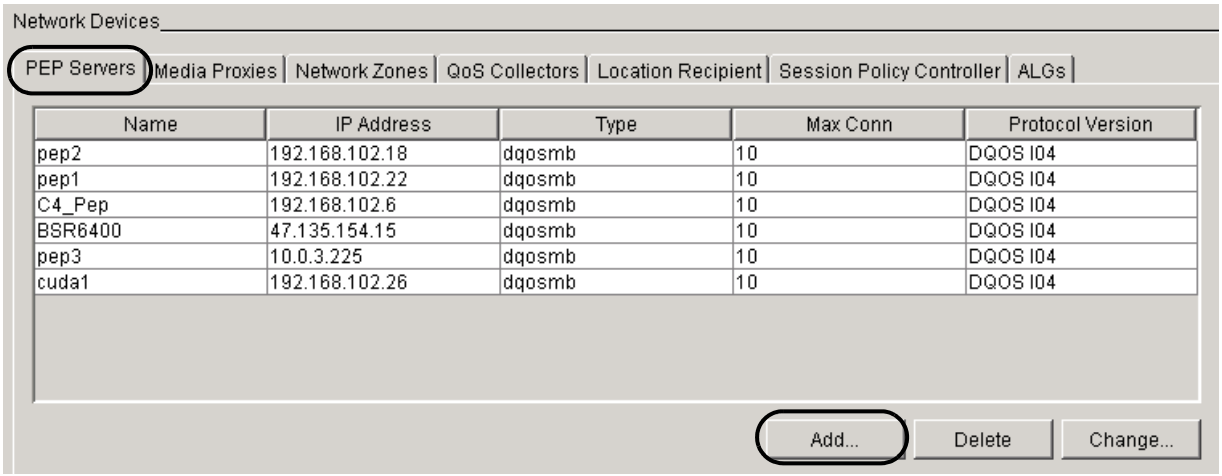
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

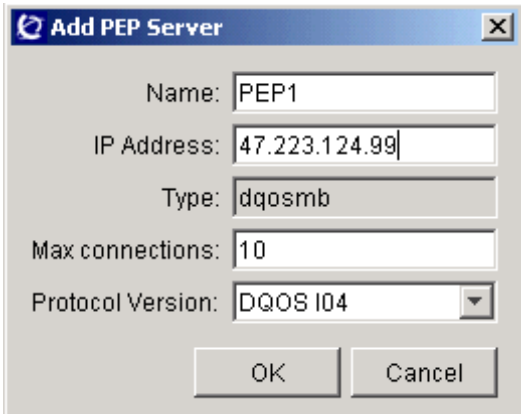


2 In the Network Devices area, click the **PEP Servers** tab.

3 Click the **Add** button to display the Add PEP Server dialog box



4 At the Add PEP Server dialog box, type the applicable configuration information as described below.



a In the Name field, type the network name of the server preferably in an fully qualified domain name (FQDN) format.

Use a server domain name in the form of an absolute domain name including the host name of the device, suitable for lookup using Directory Name Service (DNS).

b In the IP Address field, type the IP address of the server.

c Select the applicable protocol version.

The Type field is pre-defined to DQoS Middlebox (dqosmb).

The Max connections field is predefined at 10. This is the maximum number of Gateway Controllers with which PEP server can be associated.

d Click the **OK** button.

5 Verify that the server you added appears in the PEP Servers list.

6 The procedure is complete.

Associate a PEP server with a media gateway

Purpose of this procedure

Use this procedure to associate a media gateway with a policy enforcement point (PEP) server.

A PEP server, also called a middlebox, is associated with small line gateways. The GWC communicates with the PEP server to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.

When to use this procedure

Use this procedure when you wish to associate a media gateway on a specific GWC node with a PEP server for policy services

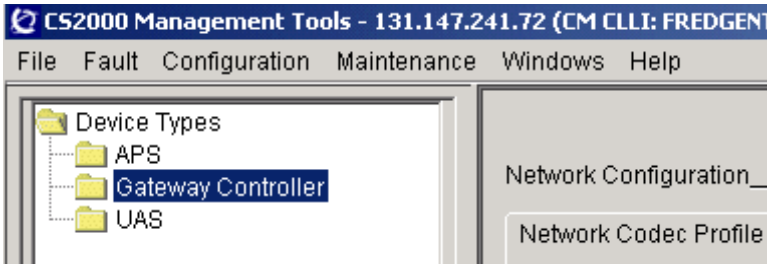
Prerequisites and guidelines

A PEP server must be installed and configured in the network.

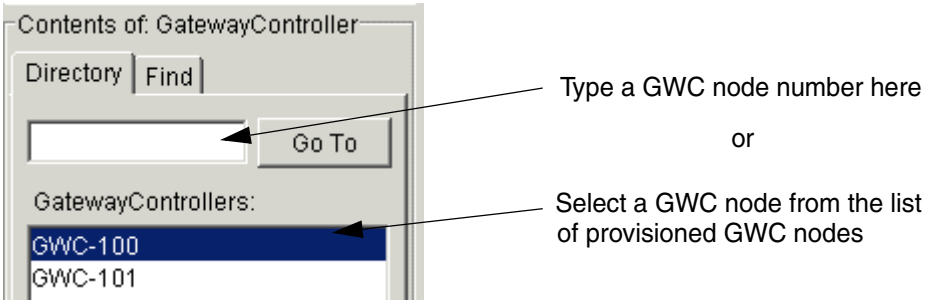
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab.

4 Click the **Gateways** tab.

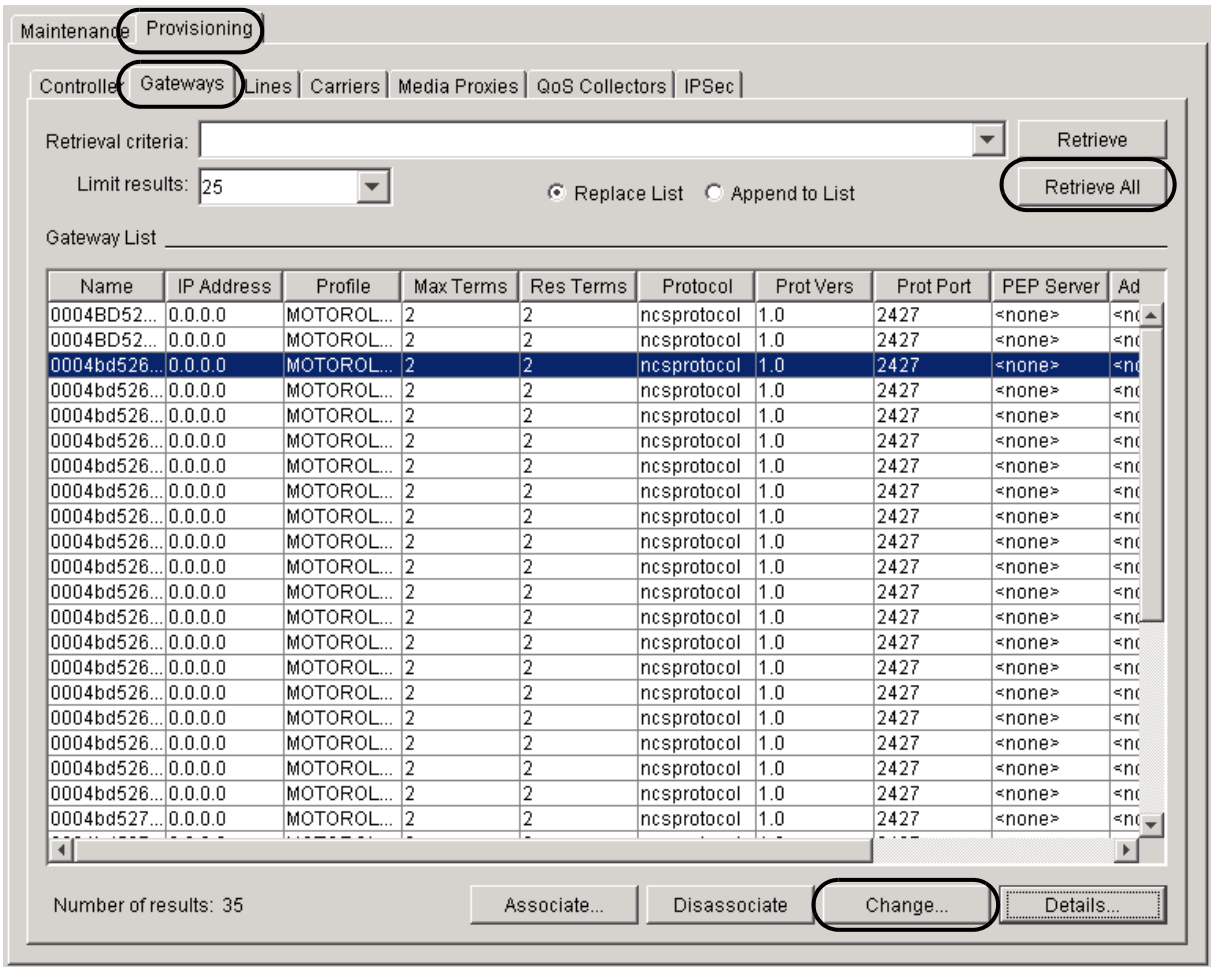
5 Click the **Retrieve All** button to display the media gateways associated with the GWC node.

6 Select a gateway from the list that you wish to associate with a PEP server.

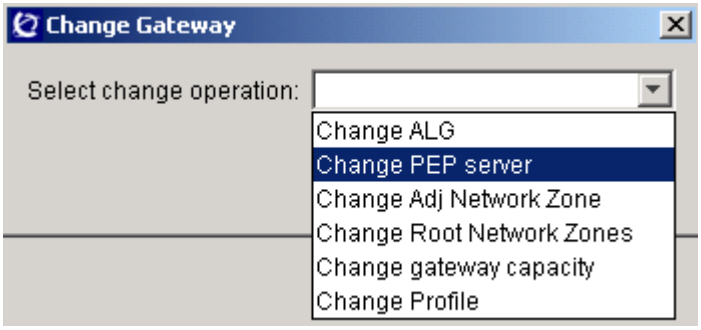
Your selection is highlighted.

7 Click the **Change** button at the bottom of the display.

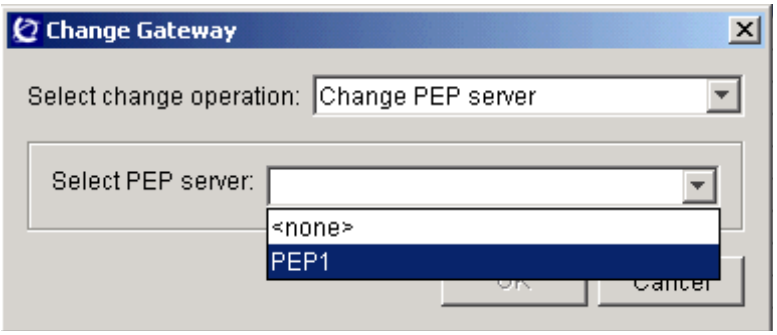
The Change Gateway dialog box is displayed.



8 Click the Select change operator drop-down menu and select **Change PEP Server**.

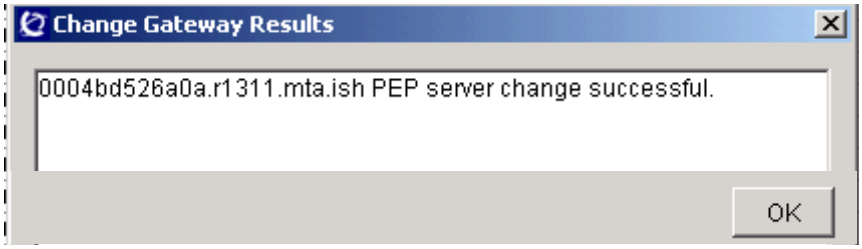


9 Click the Select PEP server drop-down menu and select an available PEP server.



10 Click the **OK** button to select the PEP server.

The Change Gateway Results dialog box is displayed.



11 Click the **OK** button to continue.

12 Repeat this procedure as required for other gateways with which you wish to associate a PEP server.

13 The procedure is complete.

Change the attributes of a PEP server

Purpose of this procedure

Use this procedure to change one of the following attributes of a policy enforcement point (PEP) server:

- IP address of the server
- The maximum number of connections supported by the server
- The version of dynamic quality of service (DQoS) protocol supported by the server

A PEP server, also called a middlebox, is used by small line gateways. The GWC communicates with the PEP server to provide DQoS and other policy services for the associated gateways.

When to use this procedure

Use this procedure when you need to change the one or more attributes of an associated PEP server.

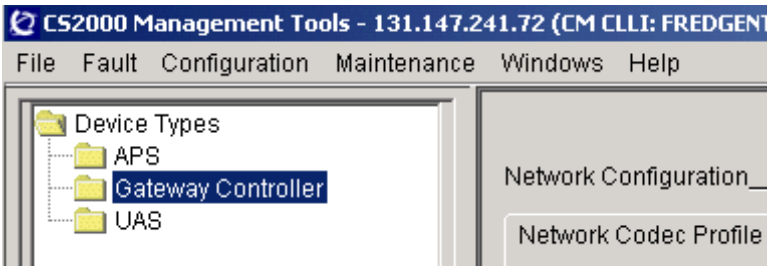
Prerequisites and guidelines

PEP servers must be installed on the network and configured for DNS lookup capability.

Action

At the CS 2000 GWC Manager client

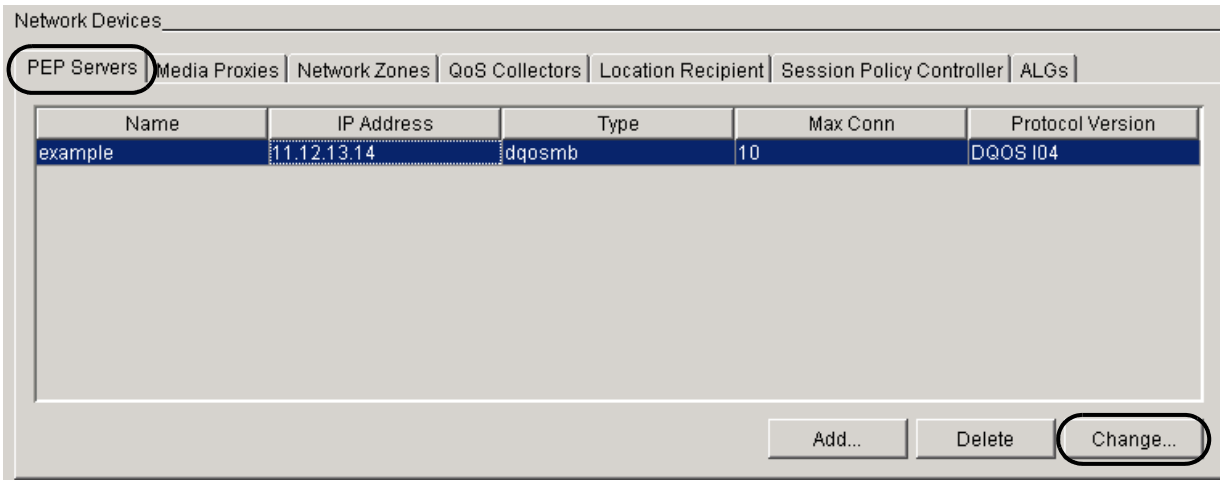
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

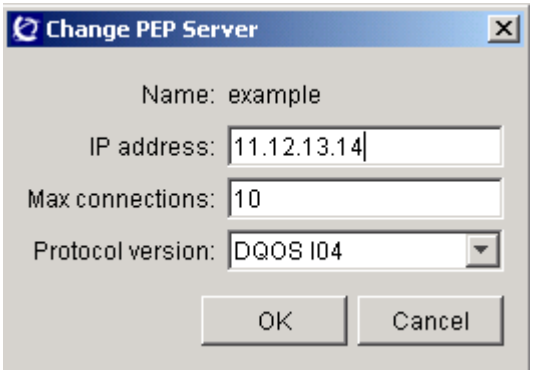


2 In the Network Devices section, click the **PEP Servers** tab.

3 Click the **Change** button.

The Change PEP Server dialog box is displayed





4 At the Change PEP Server dialog box, perform the following steps:

a Change any of the current settings in the following fields:

- In the IP address field, type a new IP address to be associated with the server.
- In the Max connections field, type a new value for the PEP server.

  A maximum of 10 connections is supported on a PEP server.
- Select a different version of the DQoS protocol for the server.

b Click the OK button.

5 Verify that the changes appear in the list of PEP servers.

6 The procedure is complete.

Disassociate a PEP server from a media gateway

Purpose of this procedure

Use this procedure to disassociate a policy enforcement point (PEP) server from a media gateway.

A PEP server, also called a middlebox, is associated with small line gateways. The GWC communicates with the PEP server to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.

When to use this procedure

Use this procedure when you want to disassociate a PEP server from a media gateway associated with a GWC node.

Prerequisites and guidelines

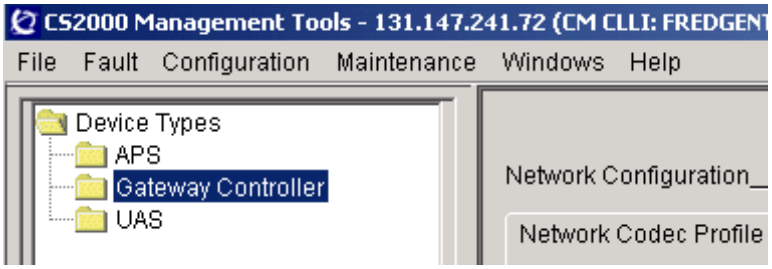
CAUTION
Possible service disruption
Disassociating a media gateway from its PEP server can affect call processing on the gateway.

There are no other prerequisites or guidelines for this procedure.

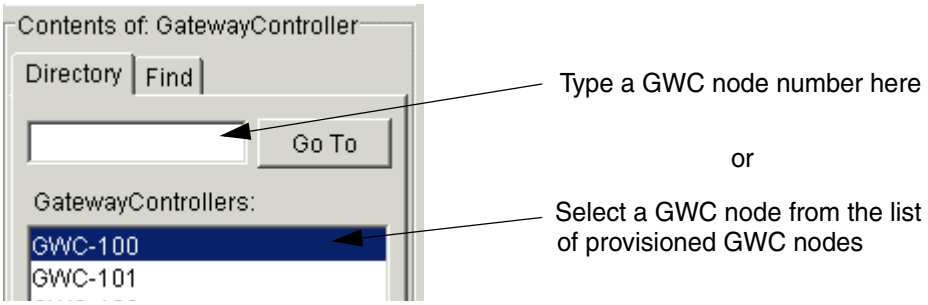
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Provisioning** tab, then click the **Gateways** tab.

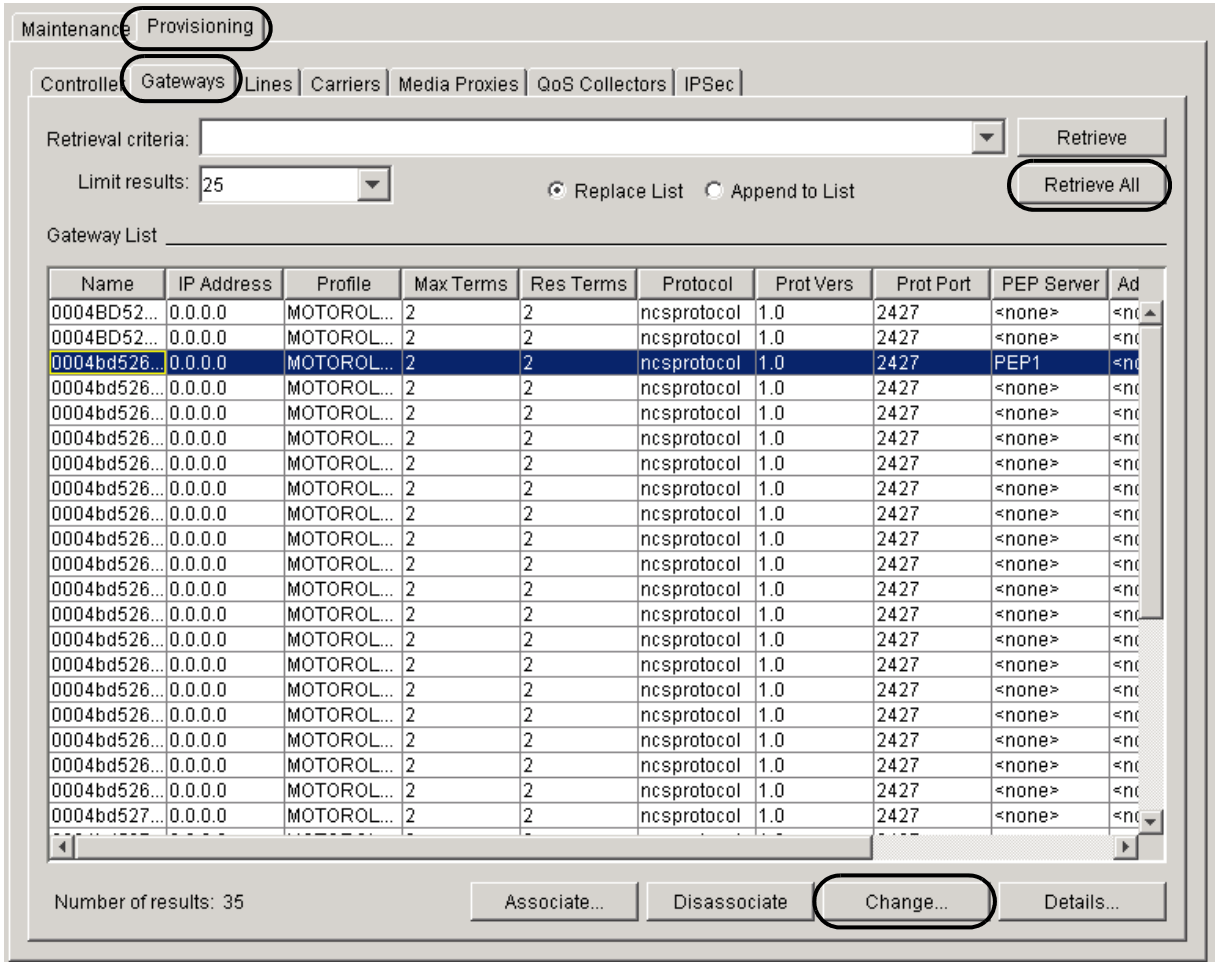
4 Click the **Retrieve All** button to view information about gateways associated with the selected GWC node.

5 Select a media gateway that has an associated PEP server that you wish to disassociate from the gateway.

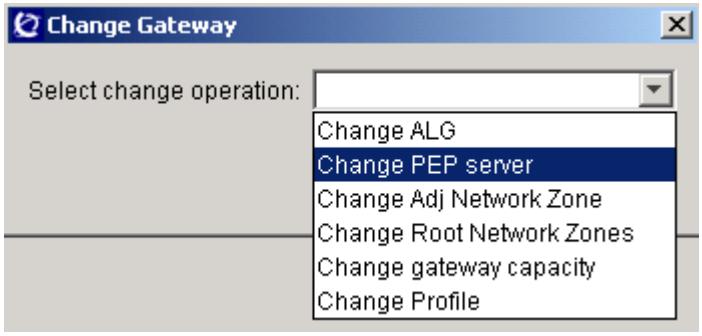
Your selection is highlighted.

6 Click the **Change** button at the bottom of the screen.

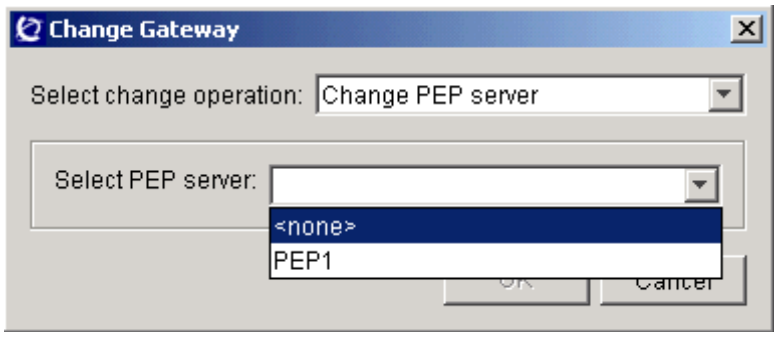
The Change Gateway dialog box is displayed.



7 Click the Select change operation: drop down menu and select **Change PEP Server**.

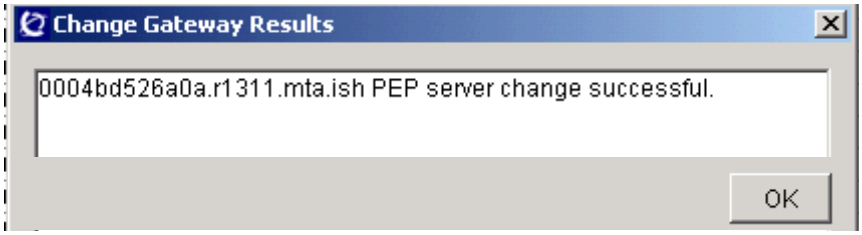


8 Click the Select PEP server: drop down menu and select **<none>**.



9 Click the **OK** button.

The Change Gateway Results dialog box is displayed.



10 Click the **OK** button to continue.

11 Verify that the PEP server is disassociated from the gateway.

Note: The display of media gateways may not indicate that the PEP server has been disassociated from the gateway. If necessary, repeat step 1 through step 4 of this procedure to verify that the change has occurred.

12 Repeat this procedure as required for other gateways from which you wish to disassociate a PEP server.

13 The procedure is complete.

Delete a PEP server

Purpose of this procedure

Use this procedure to delete a policy enforcement point (PEP) server from the network.

A PEP server, also called a middlebox, is associated with small line gateways. The GWC communicates with the PEP server to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.

When to use this procedure

Use this procedure whenever you need to remove a PEP server from the network.

Prerequisites and guidelines

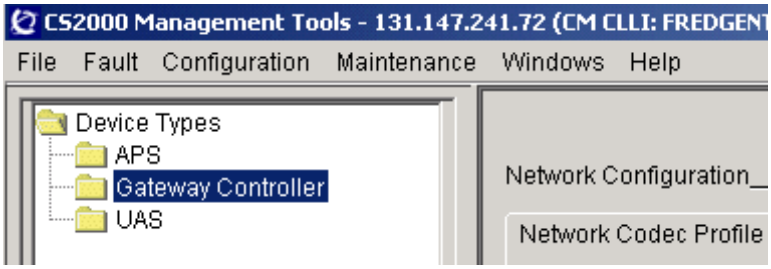
A PEP server must be installed on the network and configured for DNS lookup capability.

Note: You cannot remove a PEP server from the network while it is associated with a media gateway. You must first disassociate the PEP server from the gateway. Compete procedure Disassociate a PEP server from a media gateway on page 413 to accomplish this task.

Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

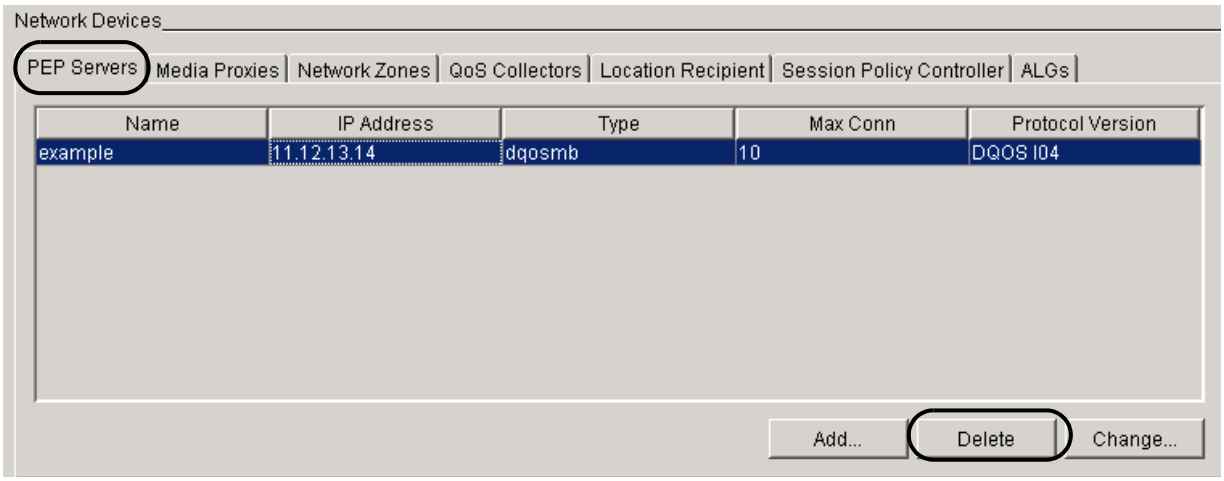


2 In the Network Devices section, click the **PEP Servers** tab.

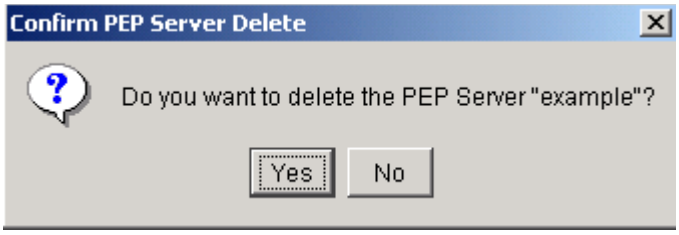
3 Select a PEP server from the list.

Your selection is highlighted.

4 Click the **Delete** button.



5 At the Confirm PEP Server Delete prompt, click **Yes**.



6 Verify that the PEP server is removed from the list.

7 The procedure is complete.

Add an application layer gateway to the network (cable market)

Purpose of this procedure

This procedure describes how to add an application layer gateway (ALG) to the network in a cable market solution.

An ALG is a type of middlebox associated with multimedia terminal adapter (MTA) small line gateways running network-based call signaling (NCS) protocol. An ALG is a virtual gateway residing on the third-party session border controller - a device located on the border between a cable provider network and a service provider network. The function of an ALG is to separate the cable provider IP address space from the service provider IP address space.

An ALG provides a network address translation (NAT) functionality. It provides a single IP address for a set of MTAs and maintains the mapping to the real MTA addresses. The real IP addresses of the gateways are not known to the Gateway Controller (GWC). The GWC communicates with MTAs through the ALG, using the single ALG IP address. This solution increases the security for the gateways, since ALG hides the real MTA IP addresses.

When to use this procedure

Use this procedure before associating MTAs to a GWC**.**

Prerequisites and guidelines

A valid ALG name and IP address must be provided to successfully configure an ALG in the network.

Use the following guidelines when adding an ALG to the network:

- You can provision and associate ALGs only with MTA small line gateways in a cable market solution.
- Each GWC can support up to 20 ALGs.
- You can associate ALGs only with gateways hosted by GWCs that are configured with the small line gateway profile.
- If you associate an ALG with a gateway, you cannot associate any of the following middleboxes with the same gateway:
  - DQoS policy enforcement point (PEP) server
  - limited bandwidth link (LBL)
  - IP-VPN network address translator (NAT)

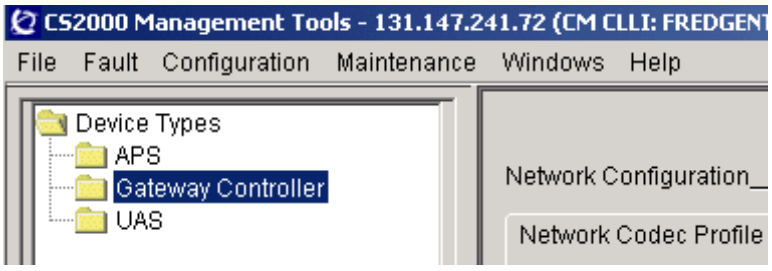
- If you associate an ALG with a gateway, IPSec between the GWC, ALG, and that gateway is not supported.
- If a redirecting media gateway controller (RMGC) is configured in the network, make sure that the Domain Servers IP addresses are configured correctly. When the ALG receives a message from the RMGC, the MTA gateway associated with this ALG must be able to resolve the fully qualified domain name (FQDN) included in that message through domain name service (DNS) queries.

Note: If required, refer to procedure Manually re-provision GWC cards on page 115 for how to verify and change basic GWC node configuration values, including Domain Servers IP addresses.

Action

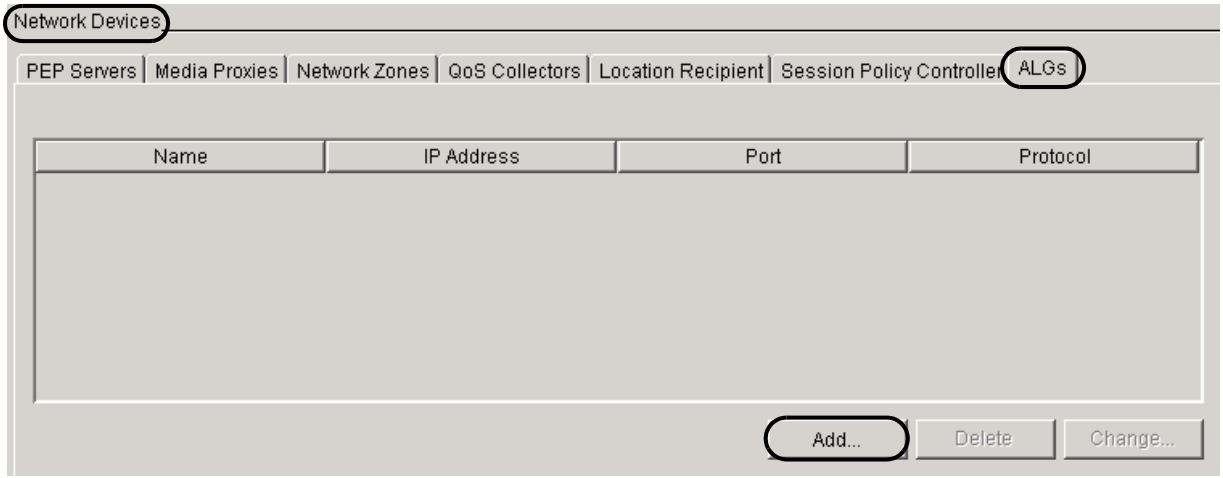
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

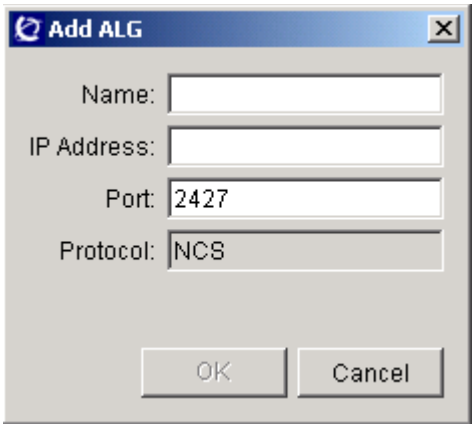


2 In the Network Devices area, click the **ALGs** tab.

3 Click the **Add** button to display the Add ALG dialog box.



4 At the Add ALG dialog box, type the applicable configuration information as described below.



a In the Name: field, type the network name of the ALG, preferably in an fully qualified domain name (FQDN) format.

Use an ALG domain name in the form of an absolute domain name including the host name of the device, suitable for lookup using Domain Name Service (DNS).

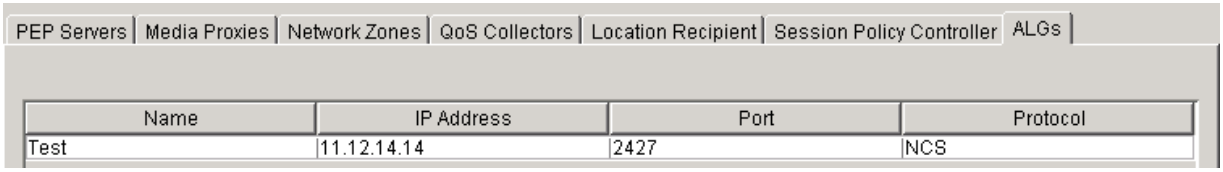
b In the IP Address: field, type the IP address of the ALG in the format of: <0-255>.<0-255>.<0-255>.<0-255>.

c The Port: field is pre-set to the NCS value of 2427. If you wish, you can delete this value and enter a new port number.

d The Protocol: field is predefined with the only valid value of NCS. You cannot change this field.

5 Click the **OK** button to apply the configuration values.

6 Verify that the ALG you added appears in the ALGs list.



7 The procedure is complete.

Change the attributes of an ALG

Purpose of this procedure

Use this procedure to change one of the following attributes of an application layer gateway (ALG):

- IP address of the ALG
- the port number

An ALG, a type of middlebox, is associated with multimedia terminal adapter (MTA) small line gateways. The GWC communicates with MTAs through the ALG, using the single ALG IP address.

When to use this procedure

Use this procedure when you need to change the IP address or the port number of an associated ALG.

Prerequisites and guidelines

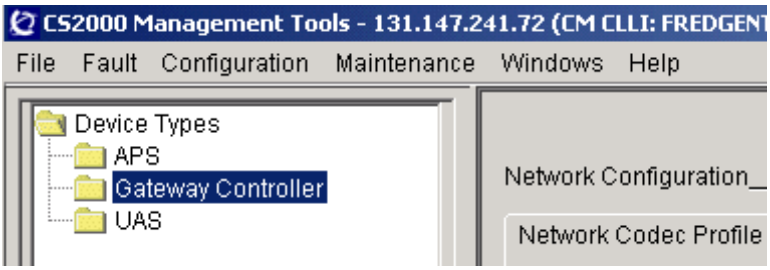
CAUTION
Possible service interruption
Changing ALG IP address or port of an ALG that has gateways associated with it can affect call processing on the gateway. Before proceeding, busy all lines configured on the gateway.

ALG must be installed and configured on the network.

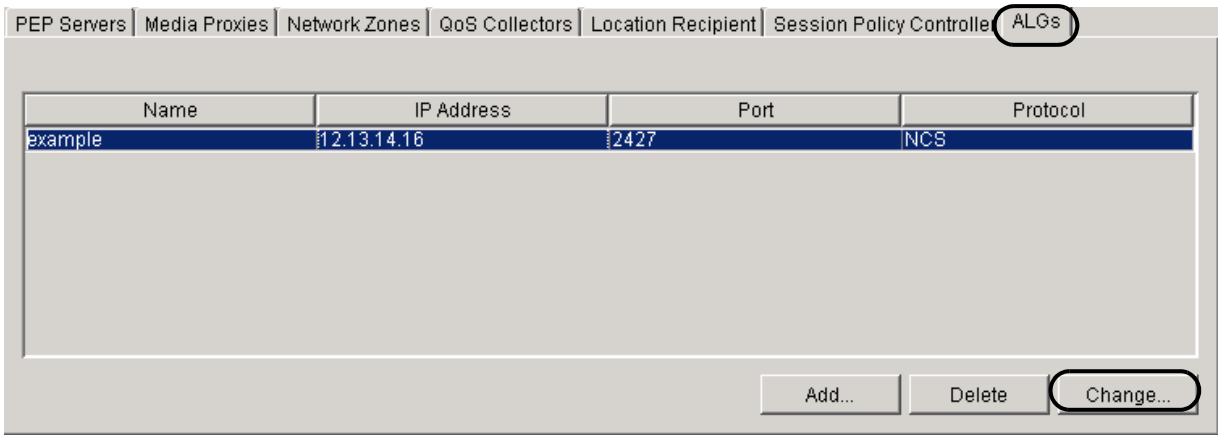
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

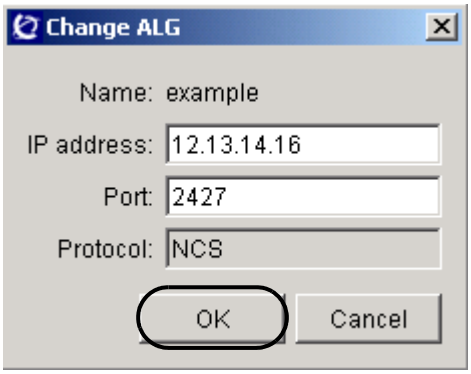


2 In the Network Devices section, click the **ALGs** tab and select the ALG that you want to change.



3 Click the **Change** button.

The Change ALG dialog box is displayed.



4 At the Change dialog box, enter the new data in one or both of the following fields:

- In the IP address: field, type a new IP address to be associated with this ALG.
- In the Port: field, enter the new port number.

Note: Do not change the Protocol: field. ALGs are only supported for NCS (1) protocol.

5 Click the **OK** button.

6 Verify that the changes appear in the list of ALGs.

7 The procedure is complete.

Associate an ALG with a media gateway

Purpose of this procedure

This procedure describes how to associate an application layer gateway (ALG) to a multimedia terminal adapter (MTA) gateway or gateways already associated with a specific Gateway Controller (GWC) node.

Note: You can also associate an ALG to the gateway during the process of associating the gateway with the GWC. Refer to procedure Associate a small line media gateway (cable market) on page 153.

When to use this procedure

Use this procedure when you wish to complete one of the following tasks:

- associate an ALG to a media gateway or gateways already associated with a specific GWC node
- change the ALG associated with a specific gateway or gateways

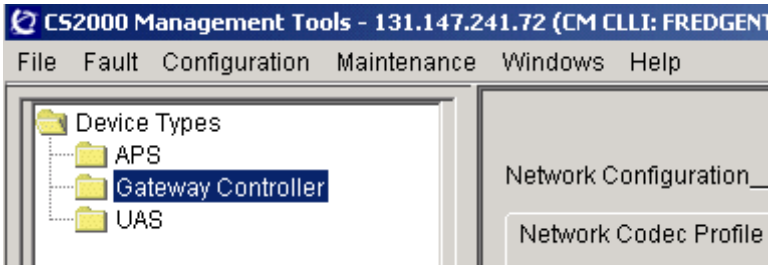
Prerequisites and guidelines

An ALG must be installed and configured in the network.

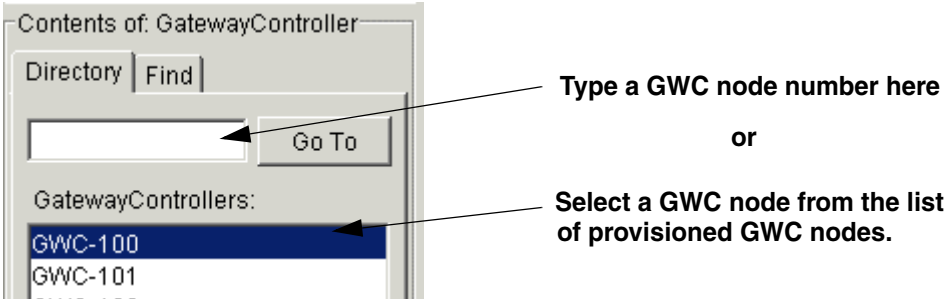
Action

At the CS 2000 GWC Manager client

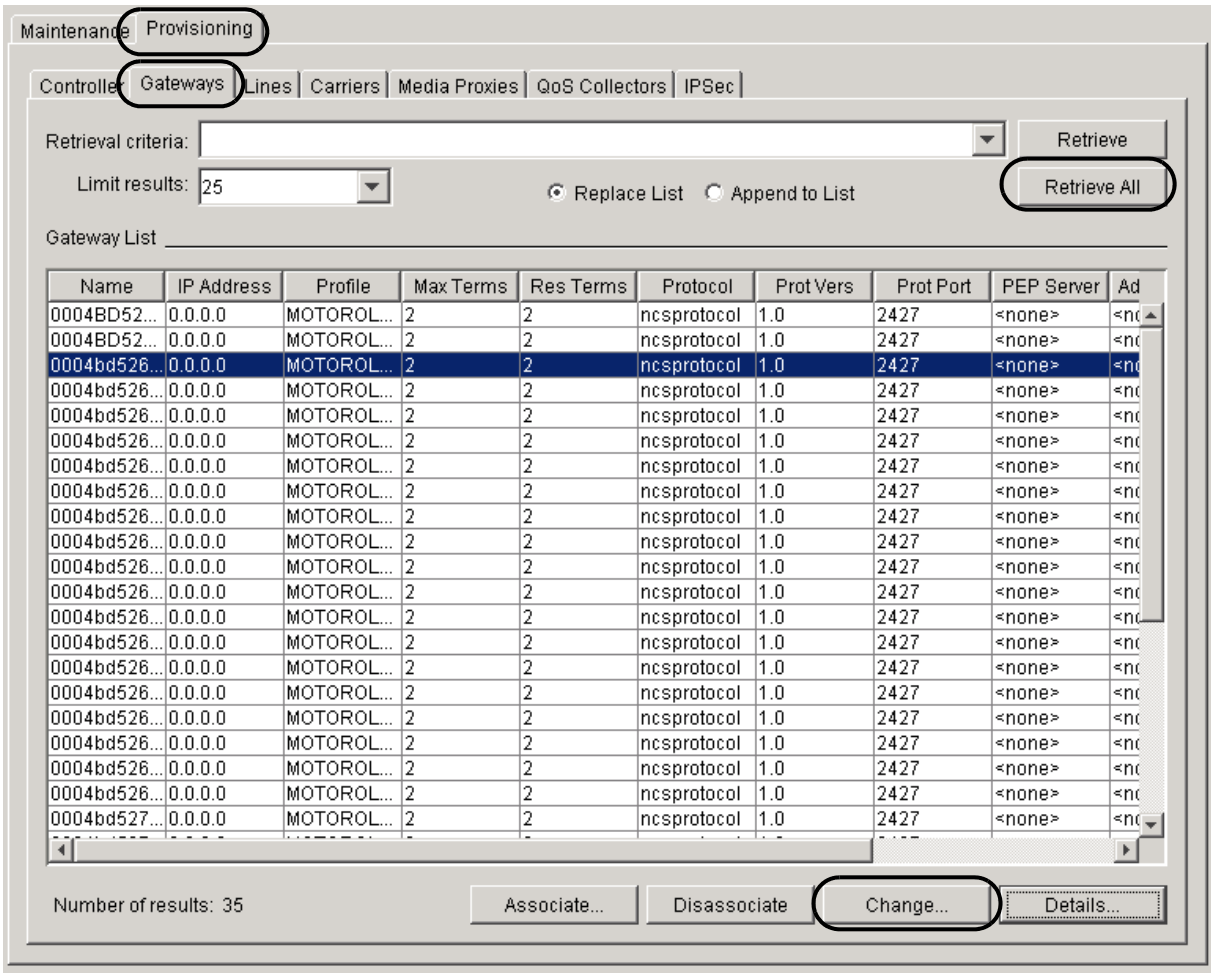
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Complete the following sub-steps to select the gateway or gateways that you wish to associate with an ALG, or for which you wish to change the associated ALG.



a Click the **Provisioning** tab, then the **Gateways** tab, then click the **Retrieve All** button to display the media gateways associated with the selected GWC node.

b From the Gateway List, select one or more gateways by clicking on the appropriate row.

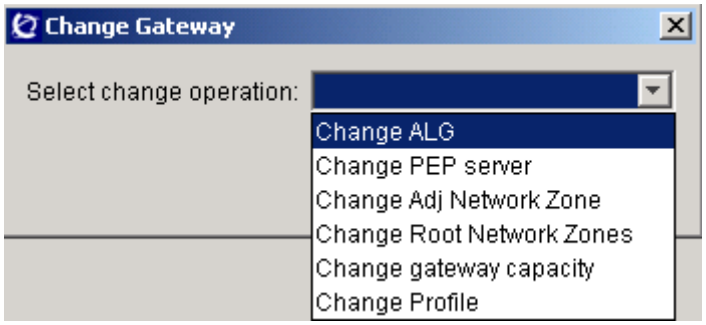
To select multiple gateways, hold down the Shift key and select each gateway entry.

Your selection is highlighted.

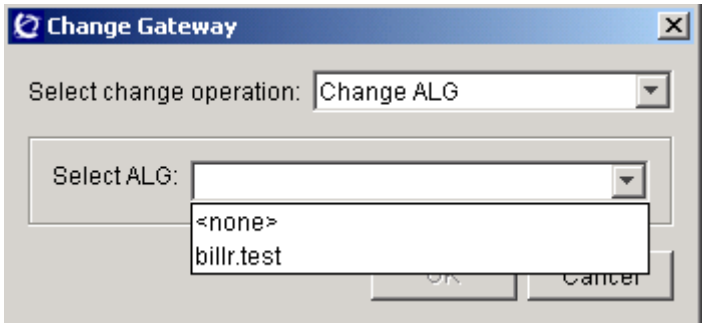
4 Click the **Change** button at the bottom of the display.

The Change Gateway dialog box is displayed.

5 Click the Select change operation: drop-down menu and select Change ALG option.

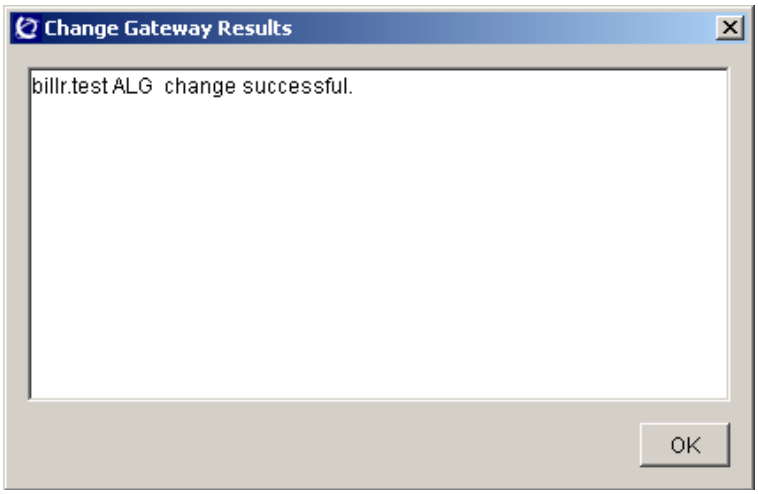


6 Click the Select ALG: drop-down menu and select one of the ALG names displayed.



7 Click the **OK** button to apply the ALG selection.

The Change Gateway Results dialog box is displayed



8 Click the **OK** button to continue.

9 Repeat this procedure as required for other gateways with which you wish to associate an ALG, or for which you want to change the associated ALG.

10 The procedure is complete.

Disassociate an ALG from a media gateway

Purpose of this procedure

This procedure describes how to disassociate an application layer gateway (ALG) from a media gateway or gateways.

An ALG, a type of middlebox, is associated with multimedia terminal adapter (MTA) small line gateways. The GWC communicates with MTAs through the ALG, using the single ALG IP address.

When to use this procedure

Use this procedure when you want to disassociate an ALG from a media gateway or gateways associated with a specific GWC node.

Prerequisites and guidelines

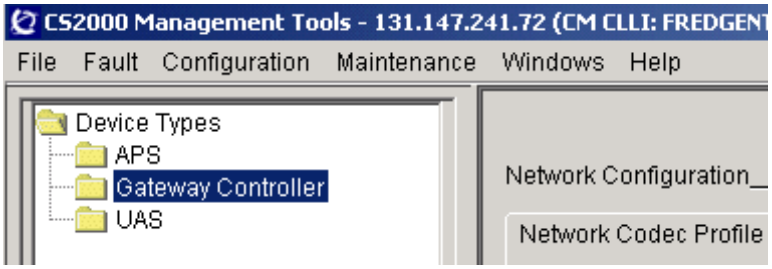
CAUTION
Possible service interruption
Disassociating a media gateway from its ALG can affect call processing on the gateway. Before proceeding, busy all lines configured on the gateway.

There are no other prerequisites or guidelines for this procedure.

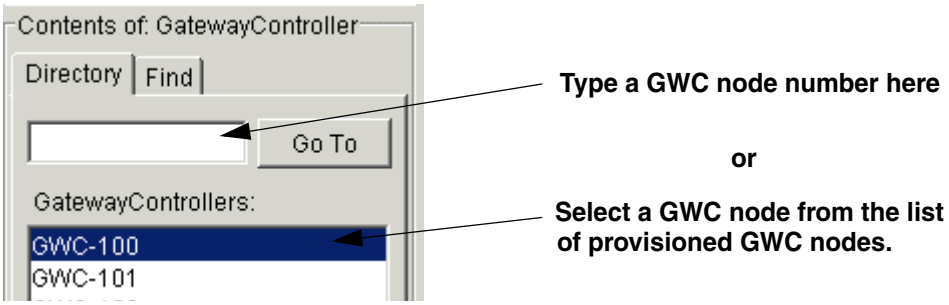
Action

At the CS 2000 GWC Manager client

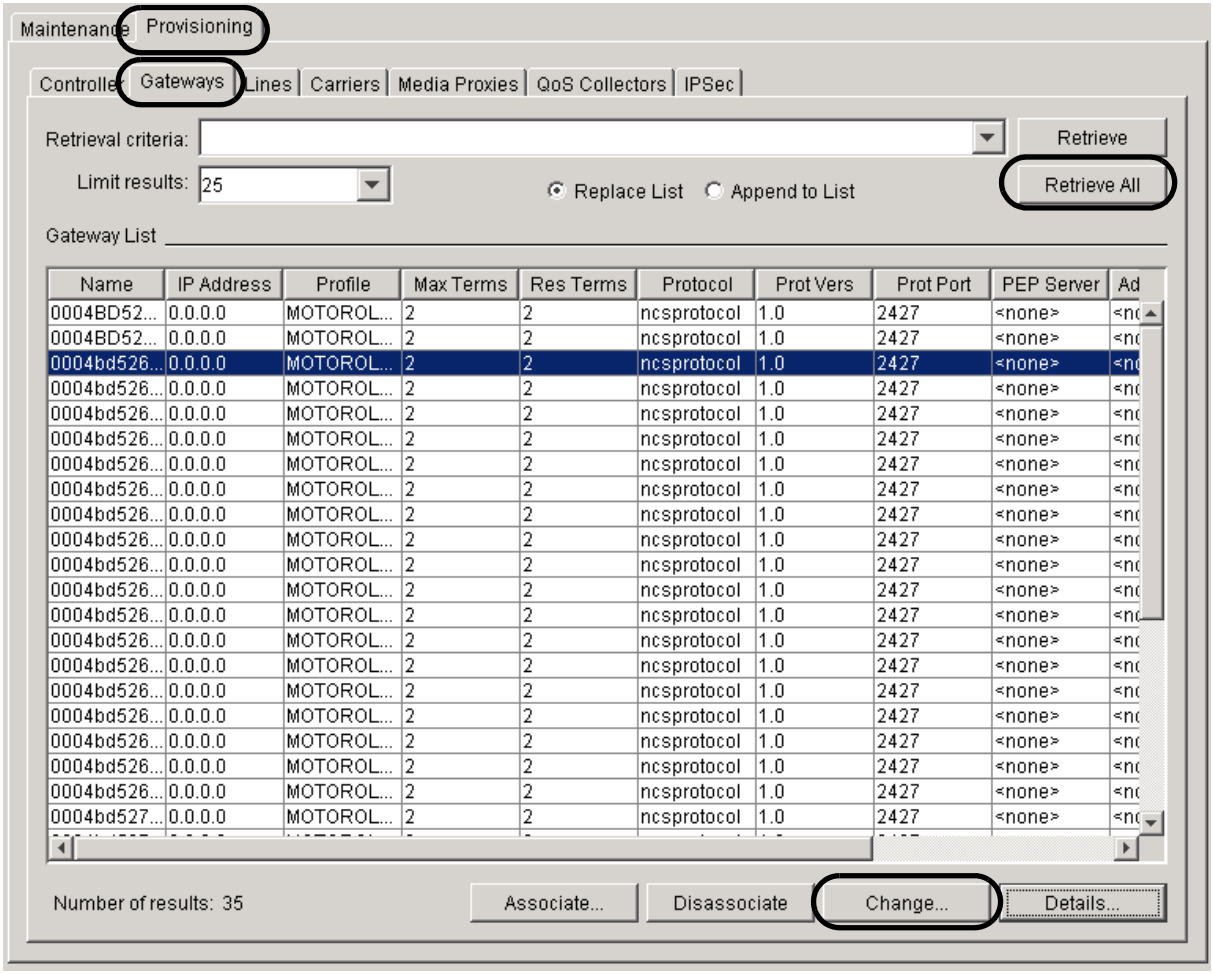
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Complete the following sub-steps to select the gateway gateways from which you wish to disassociate the ALG.



a Click the **Provisioning** tab, then the **Gateways** tab, then click the **Retrieve All** button to display the media gateways associated with the GWC node.

b From the Gateway List, select one or more gateways by clicking on the appropriate row.

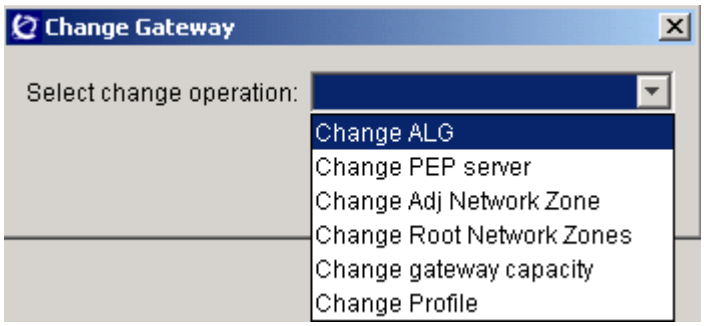
To select multiple gateways, hold down the Shift key and select each gateway entry.

Your selection is highlighted.

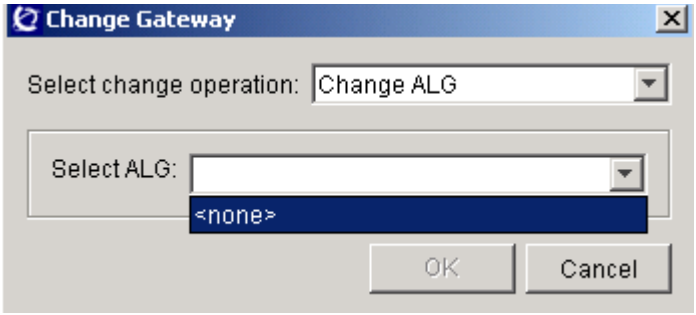
4 Click the **Change** button at the bottom of the screen.

The Change Gateway dialog box is displayed.

5 Click the Select change operation: drop-down menu and select the Change ALG option.

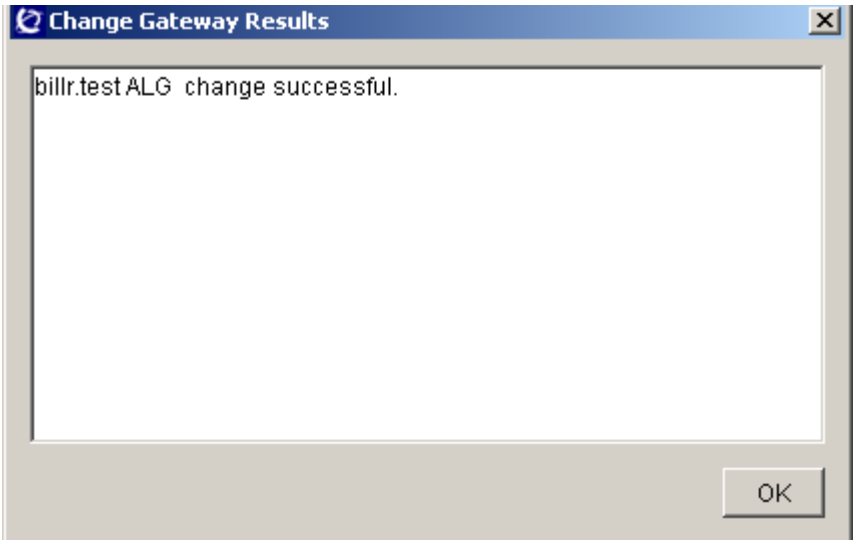


6 Click the Select ALG: drop down menu and select <none>.



7 Click the **OK** button.

The Change Gateway Results dialog box is displayed.



8 Click the **OK** button to continue.

9 Verify that the ALG is disassociated from the gateway.

Note: The display of media gateways may not indicate that the ALG has been disassociated from the gateway. If necessary, refresh the current display and verify that the word <none> appears under the ALG heading.

10 Repeat this procedure as required for other gateways from which you wish to disassociate an ALG.

11 The procedure is complete.

Delete an ALG

Purpose of this procedure

Use this procedure to delete an application layer gateway (ALG) from the network.

An ALG, a type of middlebox, is associated with multimedia terminal adapter (MTA) small line gateways. The GWC communicates with MTAs through the ALG, using the single ALG IP address.

When to use this procedure

Use this procedure whenever you need to remove an ALG from the network.

Prerequisites and guidelines

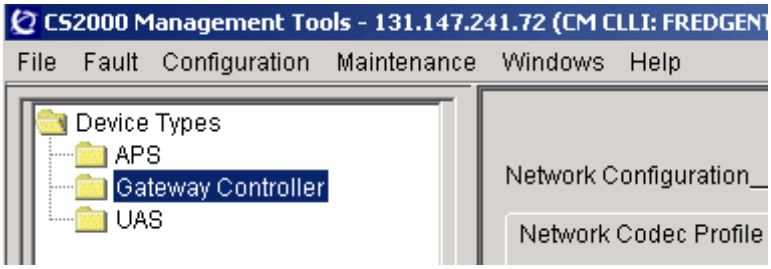
An ALG must be installed and configured on the network

Note: You cannot remove an ALG from the network while it is associated with a media gateway. You must first disassociate the ALG from the gateway. Refer to procedure Disassociate an ALG from a media gateway on page 431 to accomplish this task.

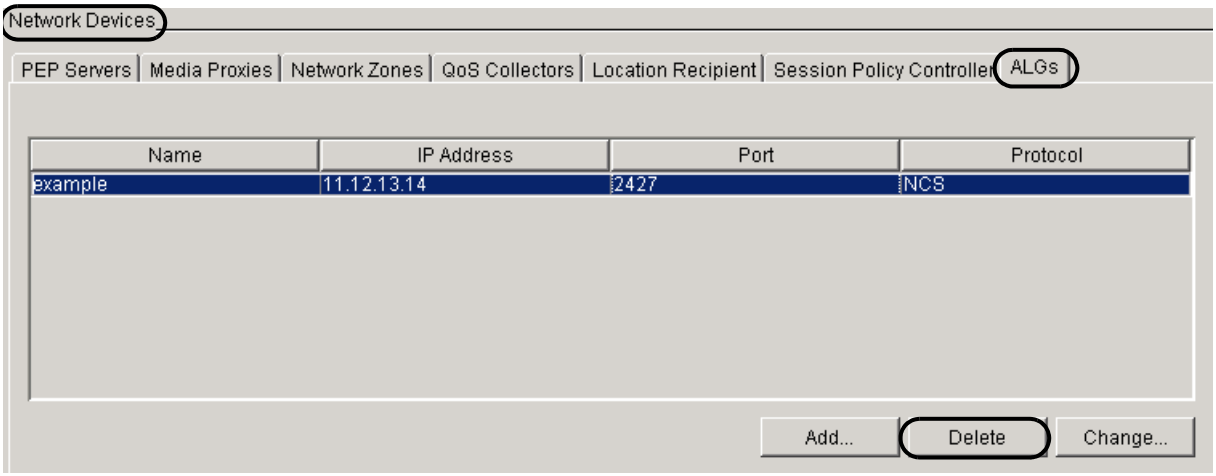
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

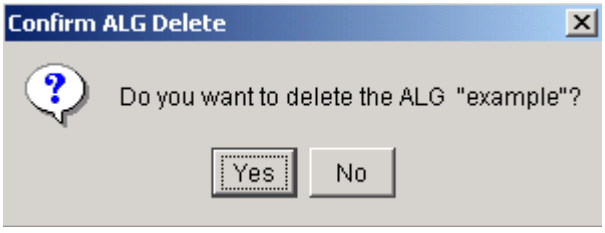


2 In the Network Devices section, click the **ALGs** tab and select the ALG that you want to delete.



3 Click the **Delete** button.

4 At the Confirm ALG Delete prompt, click **Yes**.



5 Verify that the ALG is removed from the list.

6 The procedure is complete.

Add a V5 interface provisioning template

Purpose of this procedure

Use this procedure to create and datafill V5PROV table information relating to:

- which channel(s) on which link(s) are the signaling channel(s) on the V5 interface
- what type of signaling is sent over which link
- which channels are used for backup signaling

Table V5PROV is referenced by main CM table GPPTRNSL.

When to use this procedure

Use this procedure when creating a new V5.2 provisioning template.

Prerequisites and guidelines

Before adding a V5.2 provisioning template, ensure that the following information is in place:

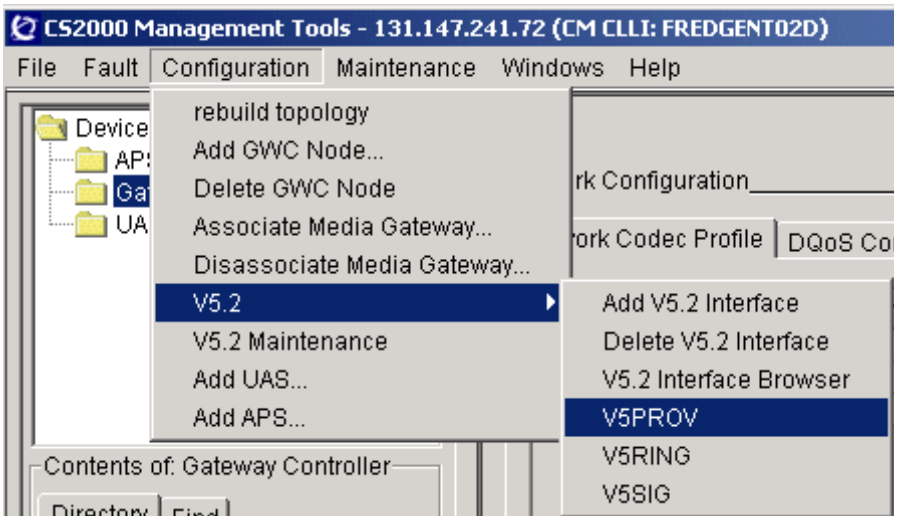
- You must know the V5 variant ID that is provisioned on the access node. This needs to match the V5PROV template as datafilled for the Interface (in table GPPTRNSL). Consult your site system administrator for details on how to acquire this information.
- The c-channel information in this profile must match the provisioning profile in the access node.

Tables V5RING and V5SIG must also be datafilled before the interface is fully provisioned.

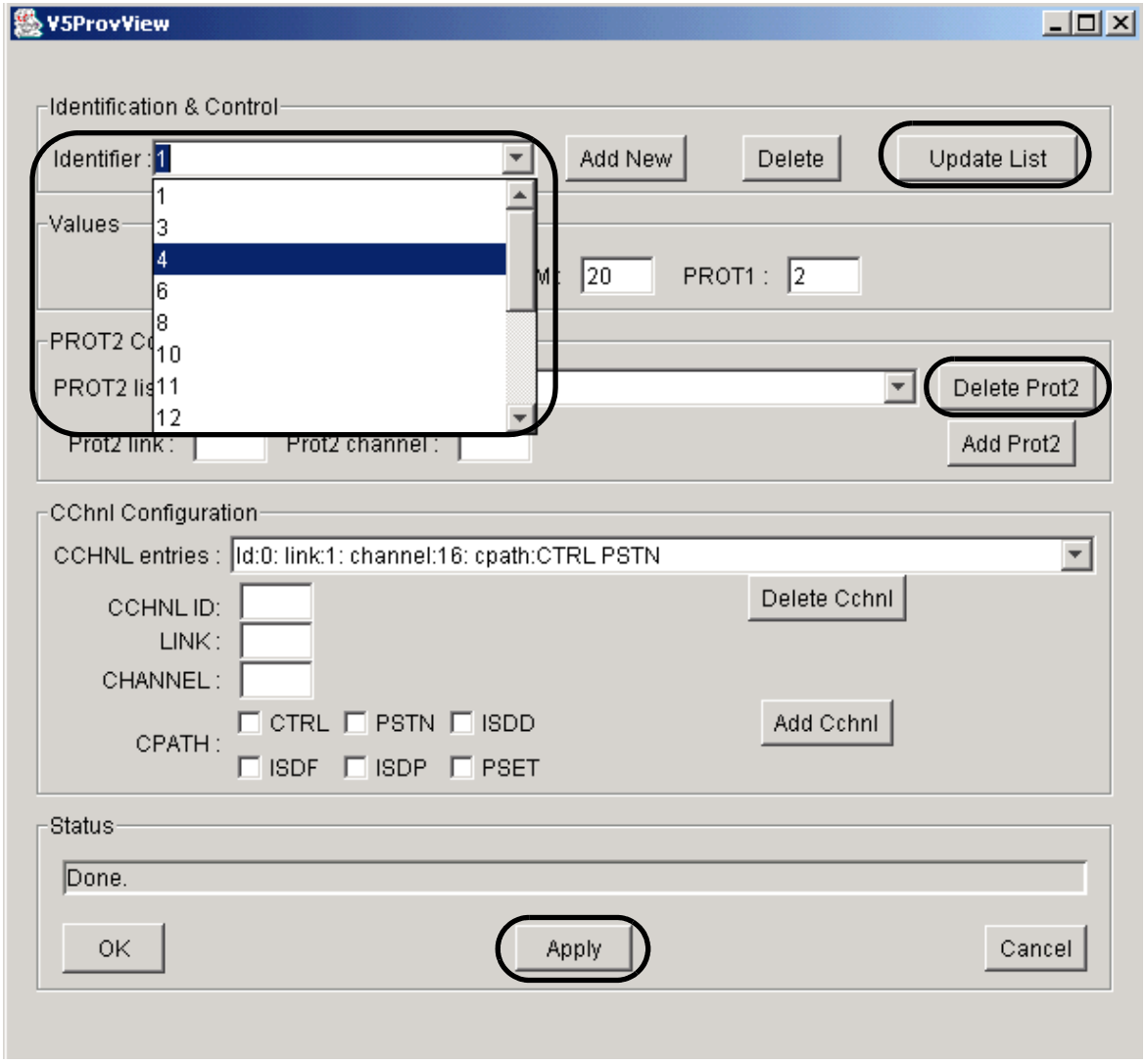
Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5PROV**.



2 Use the following provisioning view to select a provisioning template to modify by selecting its Identifier. If you cannot find the Identifier you are expecting, click the **Update List** button.



3 Use table V5 provisioning template values on page 442 to add values to the field entries:

- To add a new Prot2 link and channel, type the link and channel numbers into the Prot2 link and Prot2 channel data fields and click the **Add Prot2** button.

  Note: For a protected V5.2 interface with protection group 2, four C-channels are needed: primary link and secondary link, time slot 16, and two additional C-channels running active and standby c-path for the V5 PSTN protocol.

- To add a new C-channel configuration entry, type the CCHNL ID, LINK, CHANNEL entries in the appropriate data fields, check the appropriate CPATH check boxes that apply and click the **Add Cchnl** button.

4 Click the **Apply** button when you are finished adding templates.

5 Click the **OK** button to close the V5 provisioning view window.

6 The procedure is complete.

V5 provisioning template values (Sheet 1 of 2)

Field	Description
Identifier:	V5 provisioning variant ID. The operating company defines the different V5 provisioning IDs; use a numeric value from 0 to 127.
TBCC	Two bearer channel control timers. Set the timers to between 500 and 1500 ms; use a numeric value between 5 and 15 (5 =500 ms).
LKMJALM	Link manager alarm: threshold level of V5.2 link failure before the link triggers a major alarm. The value is the percentage of fault links that must be exceeded to generate the alarm; use a numeric value between 0 and 100.
PROT1	Protection link 1. Secondary link protection group 1 switches to this link if the primary C-channel link fails; use a numeric value from 1 to 16. Note: For a protected V5.2 interface with protection group 1, two C-channels are needed: primary link and secondary link, time slot 16. For an unprotected V5.2 interface, only one C-channel is needed: primary link, time slot 16.

V5 provisioning template values (Sheet 2 of 2)

Field	Description
Add Prot2 Delete Prot2 Buttons	Click the Add Prot2 button to add protection group 2. Click the Delete Prot2 button to remove it. Note: For a protected V5.2 interface with protection group 2, four C-channels are needed: primary link and secondary link, time slot 16, and two additional C-channels running active and standby c-path for the V5 PSTN protocol.
PROT2 list:	Protection link 2. Standby link and C-channel for protection group 2. First entry is the link, the second entry is the channel.
Prot2 link:	Link for standby link for protection group 2.
Prot2 channel:	Channel for standby link for protection group 2.
CCHNL entries:	C-channel link information; a maximum of 43 multiples of fields: CCHNL ID, LINK, CHANNEL, CPATH.
CCHNL ID:	Control channel ID number. An internal C-channel ID number; a numeric value, from 0 to 9, of provisioning channel IDs.
LINK:	The V5.2 link number that the C-channel resides on; a numeric value between 1 and 16.
CHANNEL	C-channel number or physical channel that the C-channel is on. Table control only accepts channel 16 for CNTRL. Use channel 31 after channels 15 and 16 have been used.
CPATH	Type of C-path control messages carried on the C-channel.
CTRL	Control channel messages.
PSTN	Public switched telephone network control messages.
ISDD	ISDN D-channel control messages; not currently supported.
ISDF	ISDN F-channel control messages; not currently supported.
ISDP	ISDN-P-channel control messages; not currently supported.
PSET	Proprietary phone signaling (EBS); not currently supported.

Add V5.2 interfaces

Purpose of this procedure

Use this procedure to do the following:

- add and datafill a V5.2 Interface
- map a bundle of up to 16 E1 carriers to the interface
- assign a ring plan, provisioning profile and signaling profile

When to use this procedure

Use this procedure when you are adding V5.2 interfaces and associating physical E1 links to a specific interface.

Prerequisites and guidelines

Prerequisites

Before adding V5.2 interfaces, ensure that the following prerequisites are in place:

- A GWC node must be provisioned with a V52Trunk profile using procedure Add and configure a GWC node on page 123. The gateways associated with that GWC must use the Megaco (H.248) signaling protocol.

  Note: Starting in SN06, ASPEN protocol will no longer be supported. Only H.248 /Megaco signaling will be supported, but ASPEN protocol will not be removed and can co-exist with H.248 protocol on the GWC. However, H.248 and ASPEN protocol can not co-exist on one VSP card or on one V5.2 Interface. All carrier links forming a V5.2 interface must be running the same protocol. Therefore, all gateways associated with a V5.2 interface must also be running the same protocol. Refer to the upgrades documentation for your solution to determine protocol conversion procedures.

- Carrier links must follow the naming convention for the protocol that the Gateway they are associated with is running, this is currently either ASPEN or MEGACO.

  Refer to the procedure Add carriers to a GWC on page 201 for the naming convention used for various carriers and their applicable supported protocols.

- You must know the V5 Interface ID and the GWC node ID. Your site system administrator should have this information.
- You must know the V5 variant ID that is provisioned on the access node. The profile associated with this variant ID on the access node

must match the V5PROV template as datafilled for the V5 Interface. Consult your site system administrator for details on how to acquire this information.

- The PVG nodes are already provisioned and available.
- The E1 carriers must be provisioned and in service on the PVG.
- You must know the gateway name and carrier name of the E1 links which connect to access nodes (ANs). You must also know the AN to which each E1 link connects.
- The XA-Core SOC option for V5.2 services must be turned on.
- You must know the location information contained within the XA Core table SITE. This information is provisioned as the AMCNO key component of table GPPTRNSL.

Guidelines

A single GWC node can support the following V5.2-related resources:

- 6384 V5.2 line endpoints
- 53 protected V5 interfaces in table GPPTRNSL
- 128 E1 links
- 256 C-Channels

When adding an interface, the following guidelines apply:

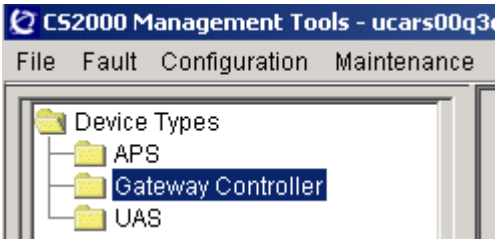
- One interface can not be spread over more than one GWC
- One interface can be spread over one or more gateways
- Links of several interfaces can be defined on one gateway

Note: It is recommended that you spread every interface evenly over two gateways (VSP cards in different PVG shelves). Refer to your the Network Engineering Guidelines for your solution.

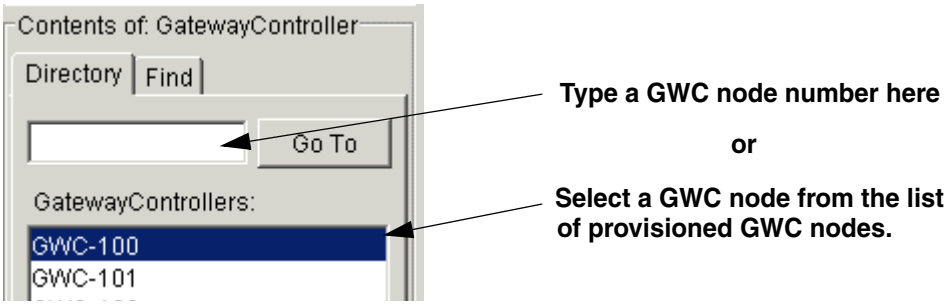
Action

At the CS 2000 GWC Manager client

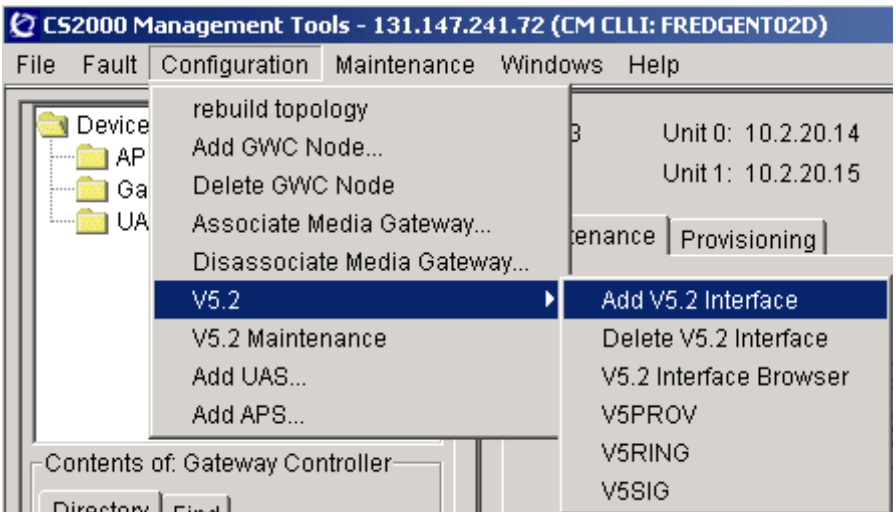
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to provision a V5.2 interface on.

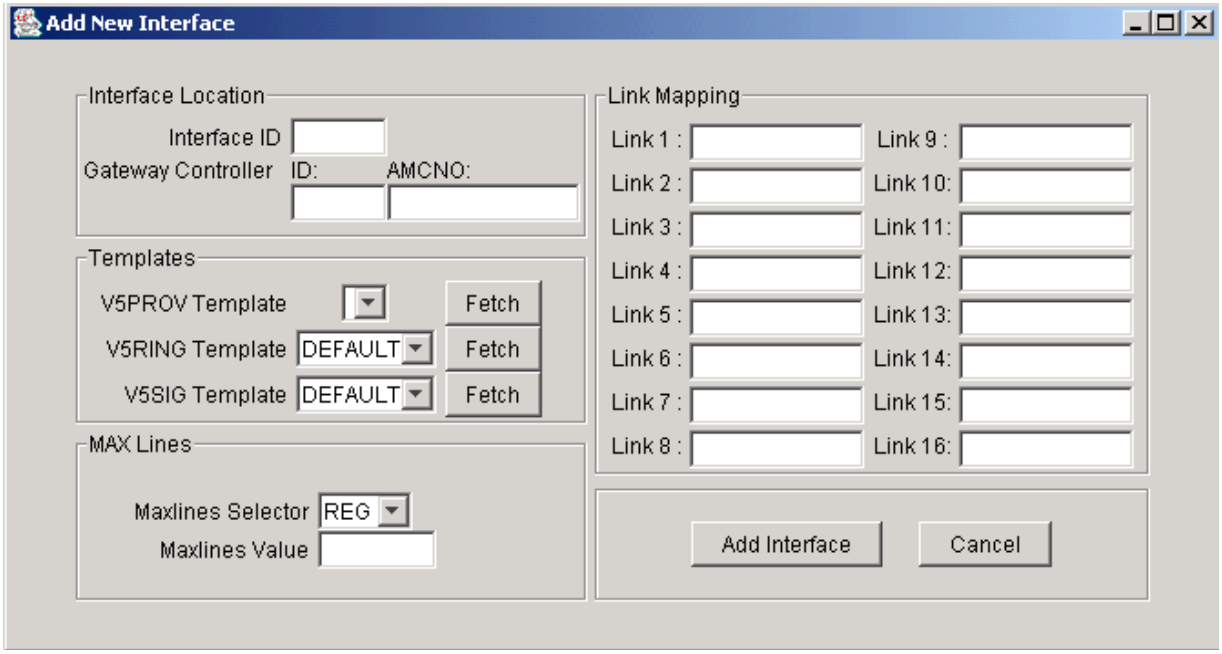


3 Click the **Configuration** menu, select **V5.2,** and then **Add V5.2 Interface**.



4 Type the interface attributes in each of the fields as needed.

Use table V5.2 interface attributes on page 448 to assist you with entering valid attributes.



5 Click **Add Interface** when you are done.

6 Click **OK** at the Adding V5.2 Interface confirmation box.

7 The procedure is complete.

V5.2 interface attributes (Sheet 1 of 2)

Field	Description
Interface ID	The V5.2 interface identifier tuple is a unique number between 0 and 16777215. It is unique between the local exchange and the access node. Up to 53 interfaces can be configured per GWC node.
Gateway Controller ID	Type the GWC number in the range of 1-255.
AMCNO	AN (access node) location, a unique line identifier.
V5PROV Template	Click on the drop-down menu button to obtain a list of up to 127 definable provisioning profiles. (The profile number needs to match the variant ID as provisioned in the access node.)

V5.2 interface attributes (Sheet 2 of 2)

Field	Description
V5RING Template	Click the **Fetch** button to obtain a list of available ringing profiles (up to 127 definable profiles) or select the DEFAULT template.
V5SIG Template	Click the **Fetch** button to obtain a list of available signaling profiles (up to 127 definable profiles). Do not use the DEFAULT template as this will generate error messages from the XA-Core.
MAX Lines Selector	REG (regular) lines or PRIM (primary) lines; only REG lines are supported.
MAX Lines	Maximum number of lines assigned to the interface from 1 to 2048, based on the capacity of the AN.
Link Mapping	V5 link-to-carrier mapping fields (up to 16 for each interface) ***Note:*** Carrier links must follow the naming convention for the protocol of the Gateway with which they are associated. This is currently either ASPEN or MEGACO. Refer to the procedure Add carriers to a GWC on page 201 for the naming convention used for various carriers and their applicable supported protocols. ASPEN format carrier links are named as follows: <Gateway Name>.E1_<xxxx> Where Gateway Name is the provisioned name of a PVG gateway, and <xxxx> is a combined shelf slot and E1 number. MEGACO format carrier links are named as follows: <Gateway Name>/E1/<yy>/<zz> Where Gateway Name is the provisioned name of a suitable Gateway, <yy> is a shelf slot number, and <zz> is an E1 number.

Add a V5 ring template

Purpose of this procedure

Use this procedure to create V5 ring templates for the V5RING table which contains information relating to mappings between ringing cadences and ringing types. Table V5RING is referenced by the main CM table GPPTRNSL.

When to use this procedure

Use this procedure when a new V5.2 interface is being provisioned.

Prerequisites and guidelines

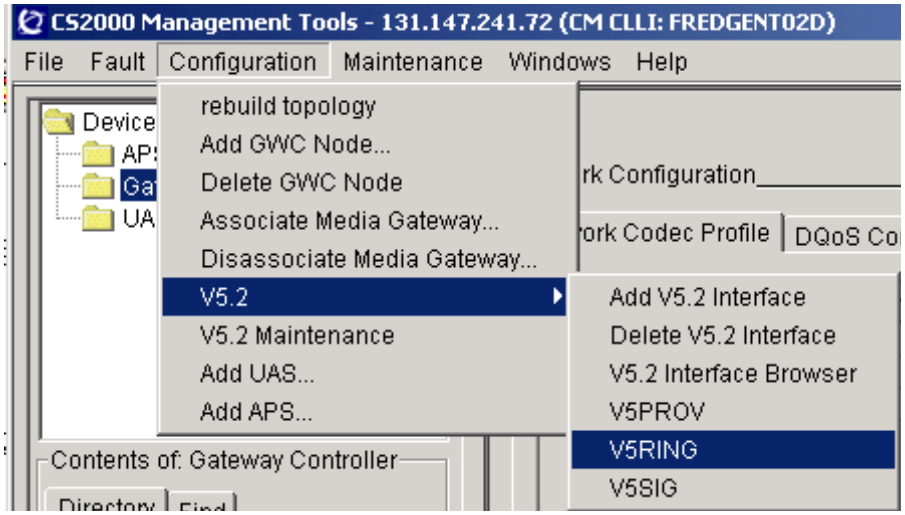
Tables V5PROV and V5SIG must also be datafilled before the interface is fully provisioned.

A default profile, identified as DEFAULT, is always provided in the template.

Action

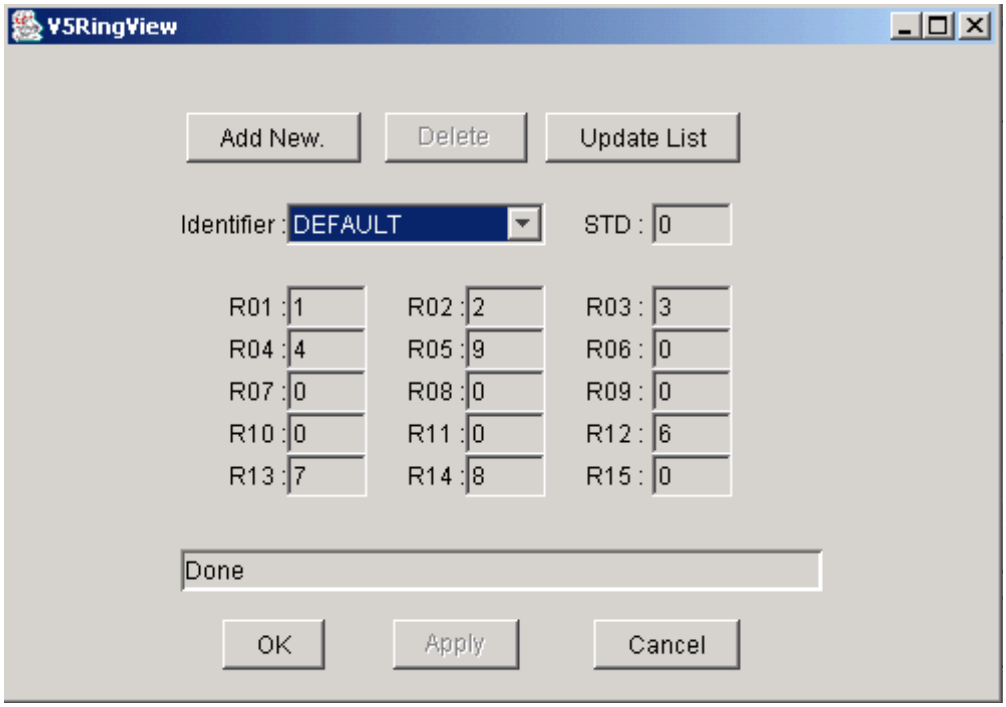
At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5RING**.



2 Use table V5.2 ring template attributes on page 453 to enter all of the ring attributes for a V5.2 ring template.

Set up a new template by adding an Identifier. Click the **Add New** button and complete the appropriate data fields.



3 Click the **Apply** button when you are finished adding ring templates.

4 Click the **OK** button to close the V5 ring view window.

5 The procedure is complete.

V5.2 ring template attributes (Sheet 1 of 2)

Field	Description
Identifier:	The V5 ring mapping ID. The operating company can define up to 127 different V5 ring mapping profile IDs; use an alphanumeric string up to16 characters that uniquely identifies the ring character to ring type mapping set.
STD	Standard Ring; a number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 0.
R01	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 1. XPM Ring Char 1 is commonly used for Distinctive Ringing 1.
R02	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 2. XPM Ring Char 2 is commonly used for Distinctive Ringing 2.
R03	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 3. XPM Ring Char 3 is commonly used for Distinctive Ringing 3.
R04	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 4. XPM Ring Char 4 is commonly used for Distinctive Ringing 4 and Automatic Recall.
R05	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 5. XPM Ring Char 5 is commonly used for Distinctive Ringing 5.
R06	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 6. No known service matching.
R07	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 7. No known service matching.
R08	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 8. No known service matching.
R09	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 9. No known service matching.
R10	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 10. No known service matching.

V5.2 ring template attributes (Sheet 2 of 2)

Field	Description
R11	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 11. No known service matching.
R12	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 12. Ring Char 12 is most commonly used for Distinctive Ringing 6 and Teen Service SDN1.
R13	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 13. Ring Char 13 is most commonly used for Distinctive Ringing 7 and Teen Service SDN2.
R14	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 04. Ring Char 14 is most commonly used for Distinctive Ringing 8 and Teen Service SDN3.
R15	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 15. No known service matching.

Add a V5 signaling template

Purpose of this procedure

Use this procedure to create and datafill V5SIG table information relating to signaling characteristics. Table V5SIG allows a set of signaling characteristics to be defined as a signaling profile. There is a default profile provisioned on any switch. These characteristics include (but are not limited to) line attenuation, End-Of-Call signaling support and suppression indication. Table V5SIG is referenced by main CM table GPPTRNSL.

When to use this procedure

Use this procedure when provisioning a new V5.2 interface.

Prerequisites and guidelines

Tables V5PROV and V5RING must also be datafilled before the interface is fully provisioned.

Note: For V52, a line attenuation value of V5_DIGITAL is not currently supported.

CAUTION

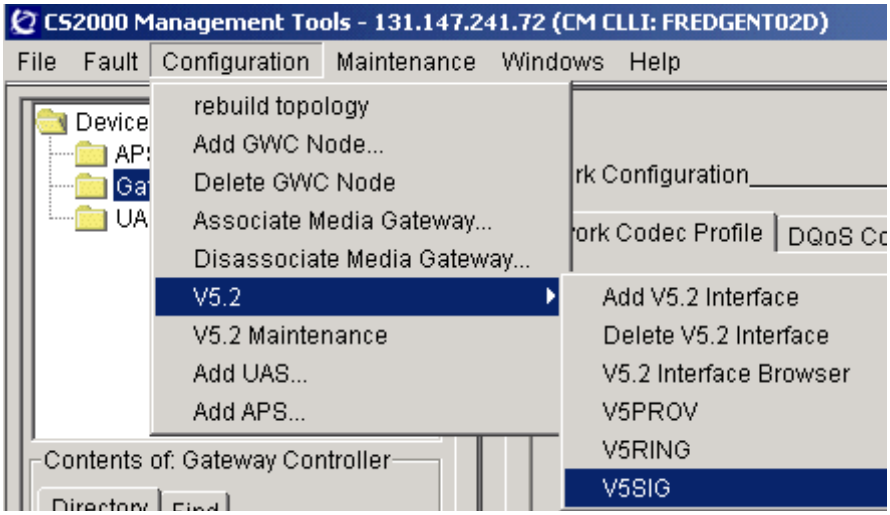
The DEFAULT template for the V5SIG table is not a valid option to select. If used, an error message will be returned from the XA-Core.

This procedure assumes that you are already logged into the CS 2000 GWC Manager and that you know the V5 Interface ID and the GWC node ID. Consult your site system administrator for details on how to acquire this information.

Action

At the CS 2000 GWC Manager client

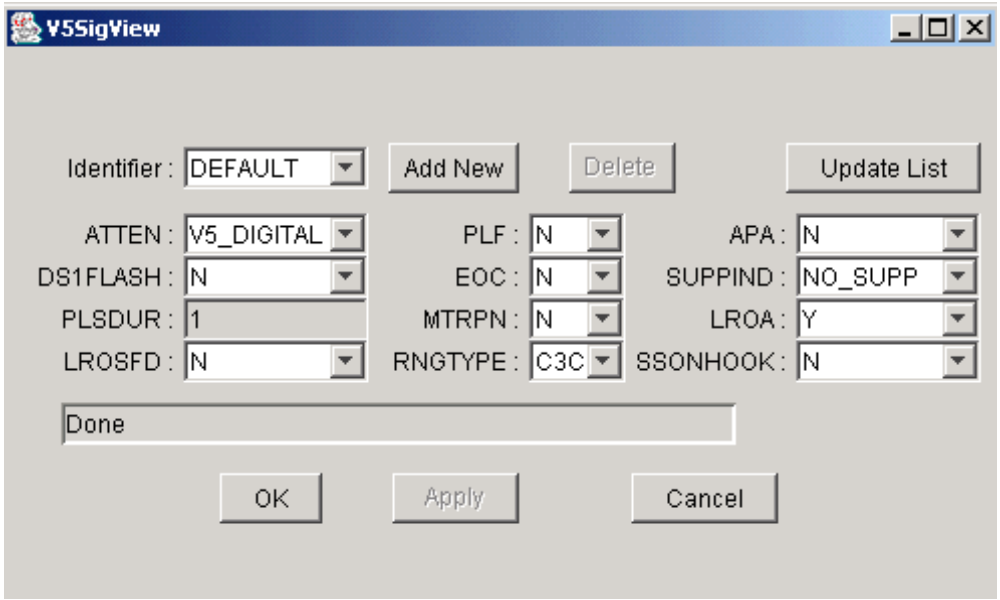
1 Click on the **Configuration** menu, select **V5.2,** and **V5SIG**.



2 Datafill all of the signaling attributes for the desired V5.2 interface.

Refer to table V5.2 interface signaling attributes on page 457 for descriptions of the V5.2 signaling attributes.

To add a new Identifier click the **Add New** button and complete the appropriate data fields.



3 Click the **Apply** button when you are done adding the sig template(s).

4 Click the **OK** button to close the V5 sig view window.

5 The procedure is complete.

V5.2 interface signaling attributes (Sheet 1 of 3)

Field	Description
Identifier	The V5 sig profile ID. The operating company can define up to 127 different V5 signaling profile IDs; use an alphanumeric string of up to16 characters that uniquely identifies the ring character to ring type mapping set.
ATTEN:	Line attenuation field; possible values are: • V5_NONE-no additional attenuation is inserted • V5-DIGITAL-not currently supported • V5-ANALOG-attenuation is added at the access node (AN) line card
PLF:	Parked Line Feed fictionalizing; Enter Y if the battery signal should be sent from the local exchange to an access node when the line enters the lock or blocked state. The reduced battery signal allows the access node to save power. The default is N (No).
APA:	Accelerated Port Alignment: Enter Y to allow the alignment of port states without supply block and unblock messages for each port. Default is N (No).
DS1FLASH:	Digit 1 register recall. Enter Y to use digit 1 to represent recall during an active call (that is, not during digit collection). The default is N (No).
EOC:	End of Call Signaling. Enter Y to use a signaling sequence that sends a V5.2 ‘pulse signal no battery’ message from the local exchange to the access node. This message indicates to the subscriber that the call has ended or failed. The end of call signaling feature provides the CPE with an indication of call completion. The default value is N (No).

V5.2 interface signaling attributes (Sheet 2 of 3)

Field	Description
SUPPIND:	Field Suppression Indication; possible values are: • NO_SUPP - No suppression is allowed. • LE_SUPP - Only a new message generated from the local exchange (LE) shall terminate the pulses being sent out from a user port. An example of a condition involving LE_SUPP would be to initiate a disconnect signal before pulsing has completed. • TE_SUPP - Only a new condition from terminal endpoint (TE) shall terminate the pulses being sent out from a user port. An example involving TE_SUPP would be to perform an on-hook before pulsing has completed. • LE_TE_SUPP - Either messages from the LE or new conditions from TE shall terminate the pulses being sent out from a user port.
PLSDUR:	Pulse Duration; When available for datafill, the value of this field reflects the length of the pulse defined in the Access Node. Enter a value between 0 and 31. The default value is 1.
MTRPN:	Meter Pulse Notification; supported. If the MTRPN field of V5SIG datafilled to Y, pulse notification will be enabled. Datafilling this field to FALSE will indicate that the V5.2 interface will not enable pulse notification.
LROA:	Line Reversal On Answer. Enter Y to indicate that each V5.2 virtual line in the office receives line reversal on seizure and forward disconnect. Enter N to indicate that V5.2 virtual lines in the office do not receive line reversal on seizure and forward disconnect. (If the entry is N, operating company personnel cannot provision fields LROSFD or RNGTYPE on a V5.2 line. Enter CHKLN in indicate V5.2 virtual lines in the office receive line reversal on answer. The line reversal depends on the LROA line option on each line.
SSONHOOK:	Signal SS: On-hook message flag; Enter a value of Y to allow or N to disallow.

V5.2 interface signaling attributes (Sheet 3 of 3)

Field	Description
LROSFD:	If the entry in the field LROA is Y or CHKLN, enter data for field LROSFD to indicate if the office requires line reversal on seizure and forward disconnect signal. Enter Y to indicate all V5.2 virtual lines in the office have line reversal. Enter N to indicated all V5.2 virtual lines in the office do not have line reversal.
RNGTYPE:	Ring Type; possible values for V5SIG table field RNGTYPE are: • C3C - The default ring type • C3D - Japanese ringing type • C6F - Portuguese ringing type

View V5.2 interface properties

Purpose of this procedure

Use this procedure to view provisioning details about the V5.2 interface.

When to use this procedure

Use this procedure when you need to view provisioning datafill about the interface and its carrier mapping.

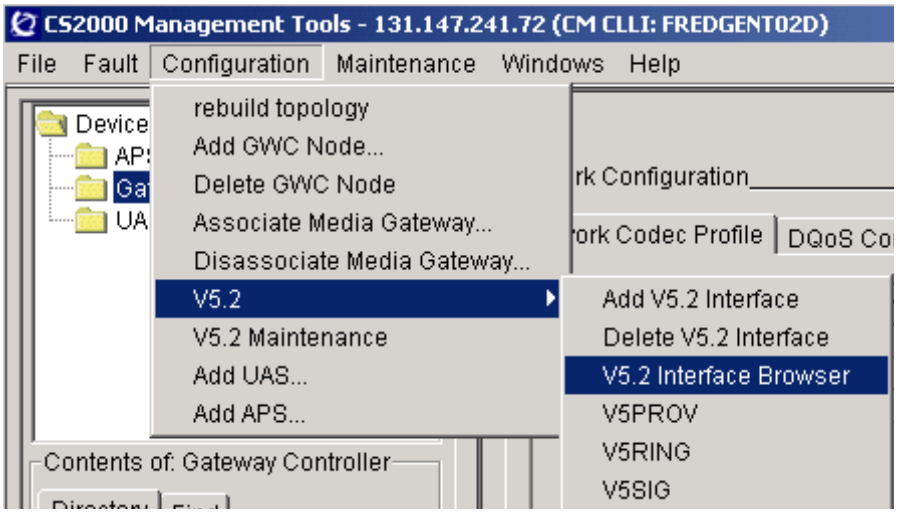
Prerequisites and guidelines

A V5.2 interface must be provisioned using the CS 2000 GWC Manager.

Action

At the CS 2000 GWC Manager client

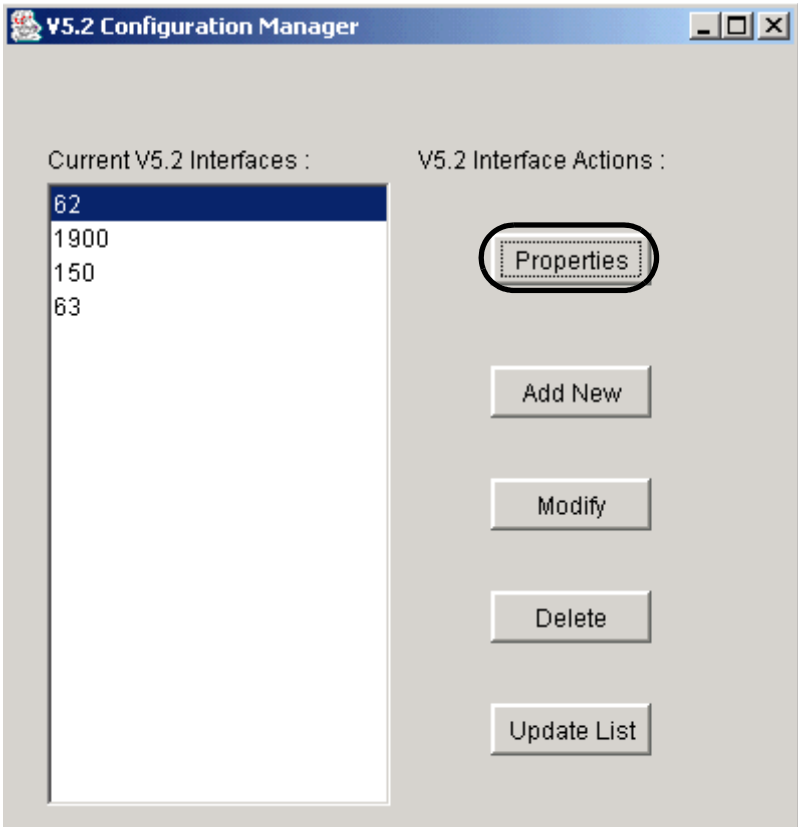
1 Click on the **Configuration** menu, select **V5.2,** and then **V5.2 Interface Browser**.



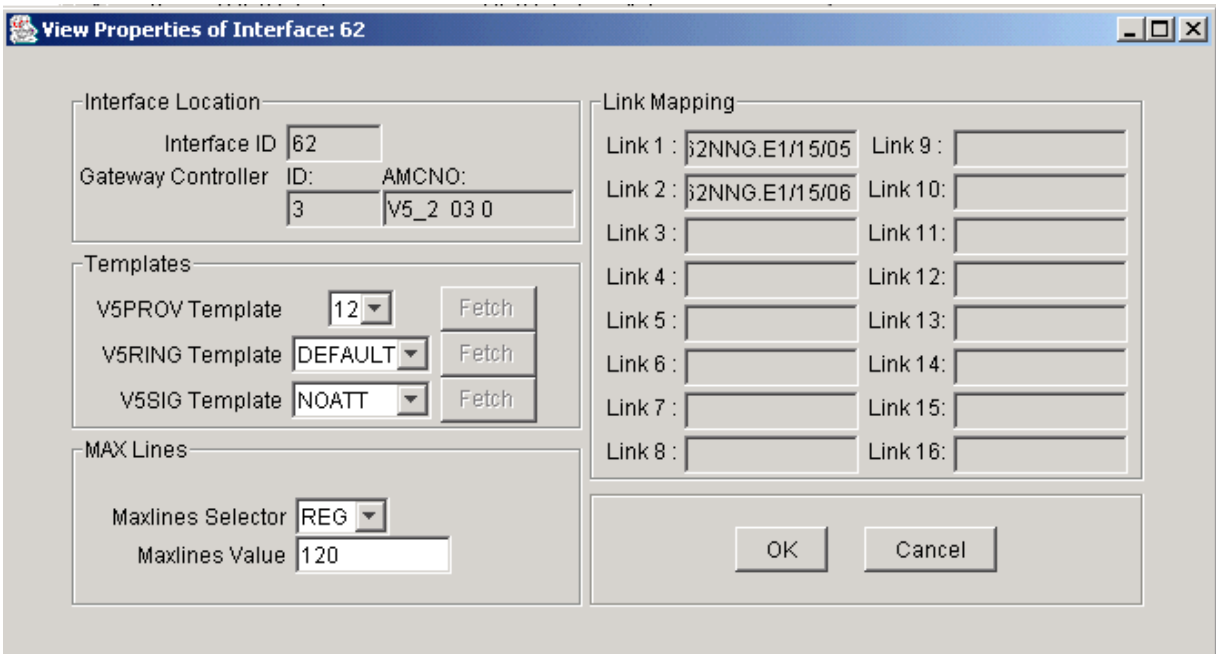
2 At the V5.2 Configuration Manger dialog box select the interface you wish to review.

Your selection is highlighted.

3 Click the **Properties** button.



4 Review the fields of the properties box. Refer to table V5.2 interface properties on page 463 for a description of the various fields.



5 The procedure is complete.

V5.2 interface properties (Sheet 1 of 2)

Field	Description
Interface ID	The V5.2 interface identifier tuple is a unique number between 0 and 16777215. It is unique between the local exchange and the access node.
Gateway Controller ID	Type the GWC number in the range of 1-255.
AMCNO	AN (access node) location, a unique line identifier.
V5PROV Template	The V5PROV provisioning profile selected for this interface.
V5RING Template	The V5RING provisioning profile selected for this interface.
V5SIG Template	The V5SIG provisioning profile selected for this interface.
MAX Lines Selector	REG (regular) lines or PRIM (primary) lines; only REG lines are supported.

V5.2 interface properties (Sheet 2 of 2)

Field	Description
MAX Lines	Maximum number of lines assigned to the interface from 1 to 2048, based on the capacity of the AN.
Link Mapping	V5 link-to-carrier mapping fields (up to 16 for each interface) ***Note:*** Carrier links must follow the naming convention for the protocol that the Gateway they are associated with is running. The protocol may be either ASPEN or MEGACO. Refer to procedure Add carriers to a GWC on page 201 for the naming convention used for various carriers and their applicable supported protocols.

View a V5 interface provisioning template

Purpose of this procedure

Use this procedure to view the details about a datafilled V5 interface provisioning template.

When to use this procedure

Use this procedure when you need to review certain provisioning template details are needed for review.

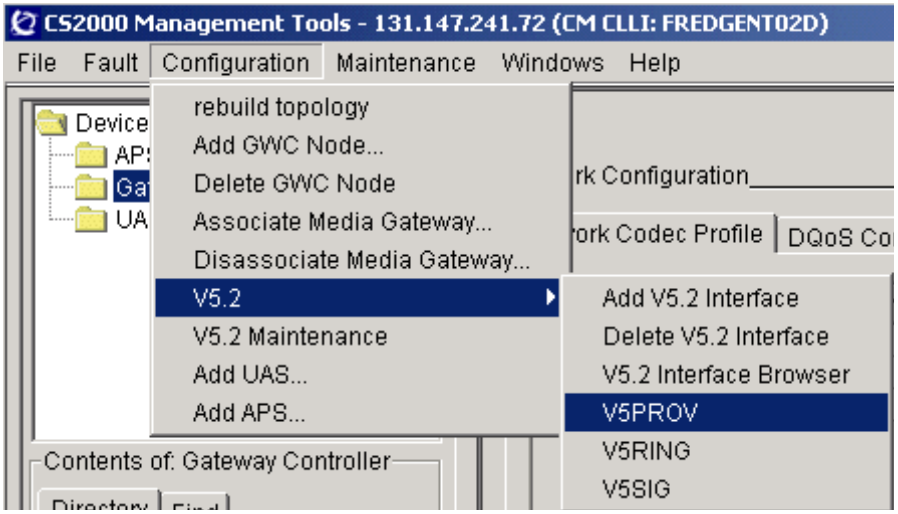
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

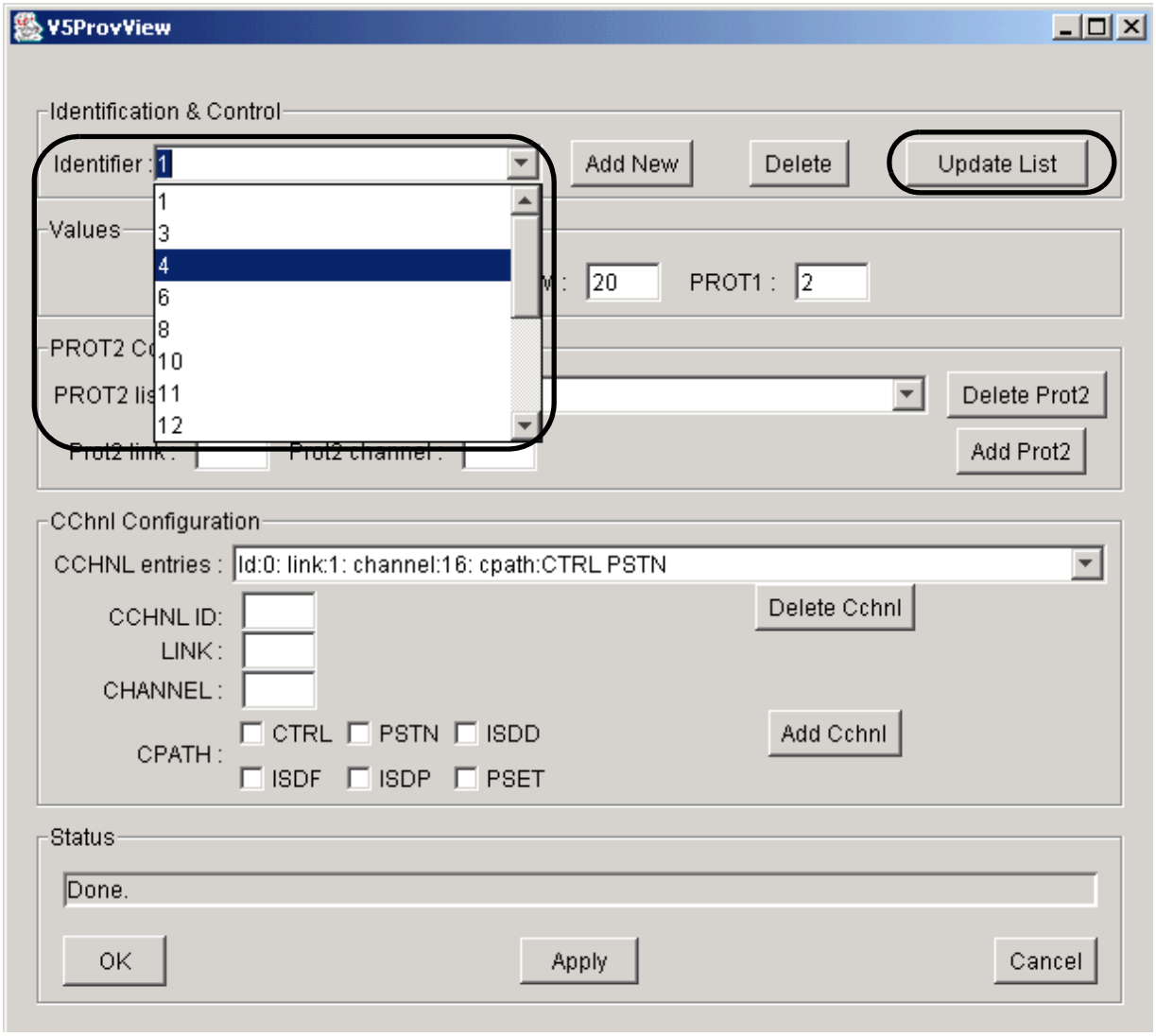
Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5PROV**.



2 Use the following provisioning view to select a provisioning template to review by selecting its Identifier. If you cannot find the Identifier you are expecting, click the **Update List** button.



3 Use table V5 Interface provisioning template on page 467 to determine the meaning and value of the field entries.

4 Click **OK** or **Cancel** when you are finished.

5 The procedure is complete.

V5 Interface provisioning template (Sheet 1 of 2)

Field	Description
Identifier:	V5 provisioning variant ID. The operating company defines the different V5 provisioning ID; use a numeric value from 0 to 128.
TBCC	Two bearer channel control timers. Set the timers to between 500 and 1500 ms; use a numeric value between 5 and 15 (5 =500 ms).
LKMJALM	Link manager alarm. Threshold level of V5.2 link failure before the link triggers a major alarm. The value is the percentage of fault links that must be exceeded to generate the alarm; use a numeric value between 0 and 100.
PROT1	Protection link 1. Secondary link protection group 1 switches to this link if the primary C-channel link fails; use a numeric value from 1 to 16.
PROT2 list:	Protection link 2. Standby link and C-channel for protection group 2. First entry is the link, the second entry is the channel.
Prot2 link:	Link for standby link for protection group 2
Prot2 channel:	Channel for standby link for protection group 2.
CCHNL entries:	C-channel link information; a maximum of 43 multiples of fields: CCHNL ID, LINK, CHANNEL, CPATH.
CCHNL ID:	Control channel ID number. An internal C-channel ID number; a numeric value, from 0 to 9, of provisioning channel IDs.
LINK:	The V5.2 link number that the C-channel resides on; a numeric value between 1 and 16.
CHANNEL	C-channel number or physical channel that the C-channel is on. Table control only accepts channel 16 for CNTRL. Use channel 31 after channels 15 and 16 have been used.

V5 Interface provisioning template (Sheet 2 of 2)

Field	Description
CPATH	Type of C-path control messages carried on the C-channel.
CTRL	Control channel messages.
PSTN	Public switched telephone network control messages.
ISDD	ISDN D-channel control messages; not currently supported.
ISDF	ISDN F-channel control messages; not currently supported.
ISDP	ISDN-P-channel control messages; not currently supported.
PSET	Proprietary phone signaling (EBS); not currently supported.

View V5 ring template

Purpose of this procedure

Use this procedure to view details about an existing V5 ring template.

When to use this procedure

Use this procedure whenever ring template details need to be for reviewed.

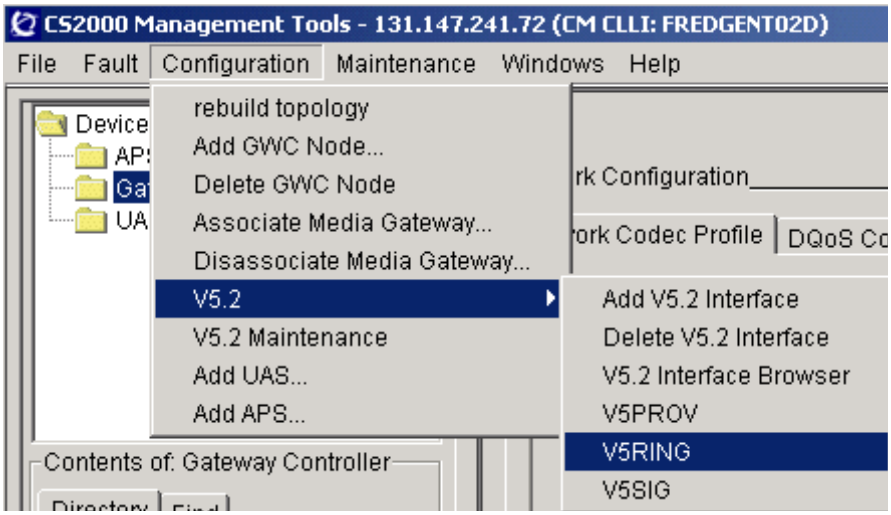
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

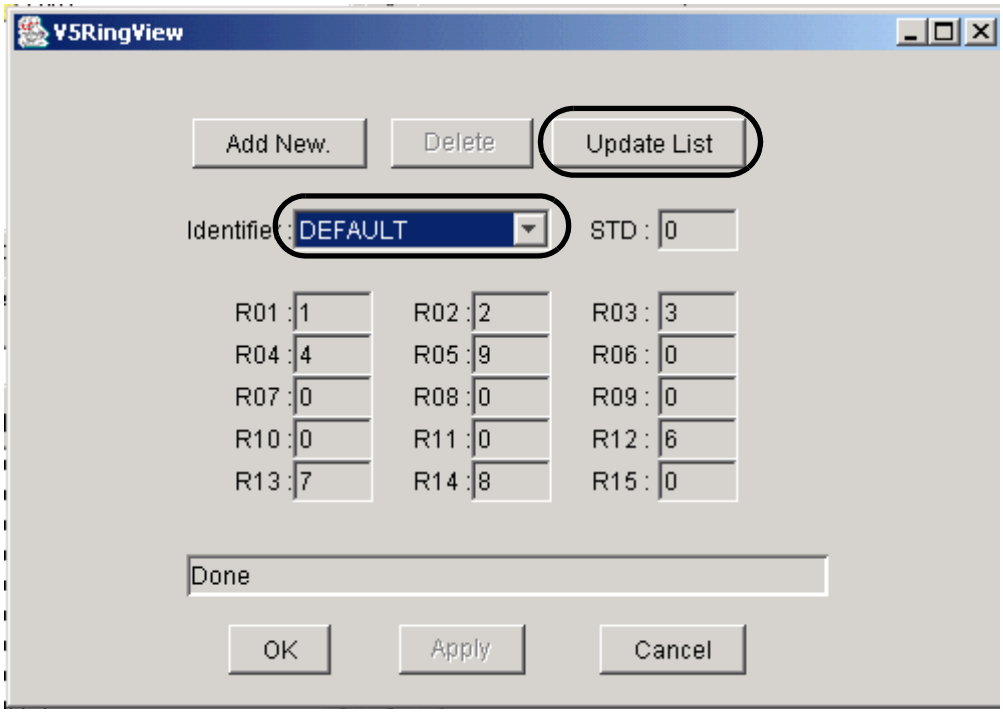
Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5RING**.



2 At the V5RingView dialog box, select a ring template Identifier to review using the drop-down menu. If the identifier is not available, click the **Update List** button.



3 Use table V5.2 ring template attributes on page 471 to review the fields, terms and the descriptions.

4 Click the **OK** or **Cancel** button when you are done.

5 The procedure is complete.

V5.2 ring template attributes (Sheet 1 of 2)

Field	Description
Identifier:	The V5 ring mapping ID. The operating company defines the different V5 ring mapping IDs; use an alphanumeric string up to16 characters that uniquely identifies the ring character to ring type mapping set.
STD	Standard Ring; a number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 0.
R01	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 1. XPM Ring Char 1 is commonly used for Distinctive Ringing 1.
R02	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 2. XPM Ring Char 2 is commonly used for Distinctive Ringing 2.
R03	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 3. XPM Ring Char 3 is commonly used for Distinctive Ringing 3.
R04	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 4. XPM Ring Char 4 is commonly used for Distinctive Ringing 4 and Automatic Recall.
R05	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 5. XPM Ring Char 5 is commonly used for Distinctive Ringing 5.
R06	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 6. No known service matching.
R07	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 7. No known service matching.
R08	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 8. No known service matching.
R09	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 9. No known service matching.
R10	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 10. No known service matching.

V5.2 ring template attributes (Sheet 2 of 2)

Field	Description
R11	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 11. No known service matching.
R12	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 12. Ring Char 12 is most commonly used for Distinctive Ringing 6 and Teen Service SDN1.
R13	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 13. Ring Char 13 is most commonly used for Distinctive Ringing 7 and Teen Service SDN2.
R14	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 04. Ring Char 14 is most commonly used for Distinctive Ringing 8 and Teen Service SDN3.
R15	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 15. No known service matching.

View a V5 signaling template

Purpose of this procedure

Use this procedure to view the V5SIG table signaling attributes.

When to use this procedure

Use this procedure when you need to view certain signaling template details.

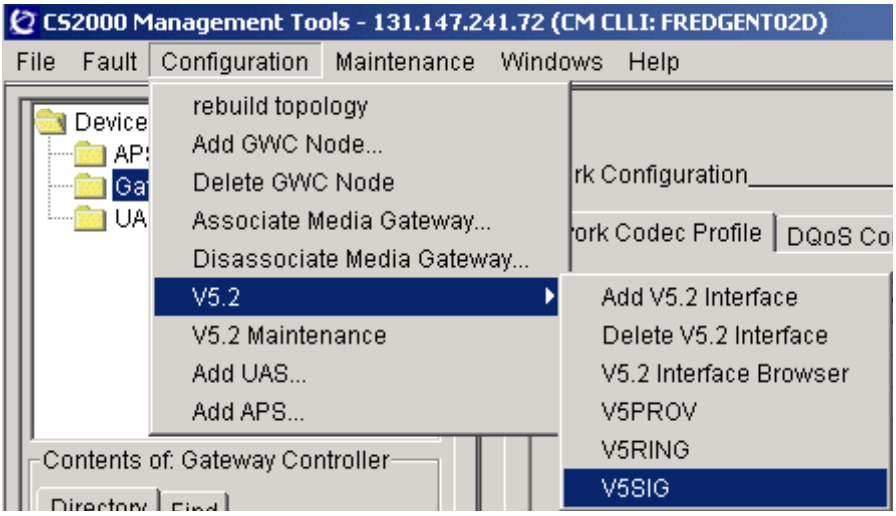
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

Action

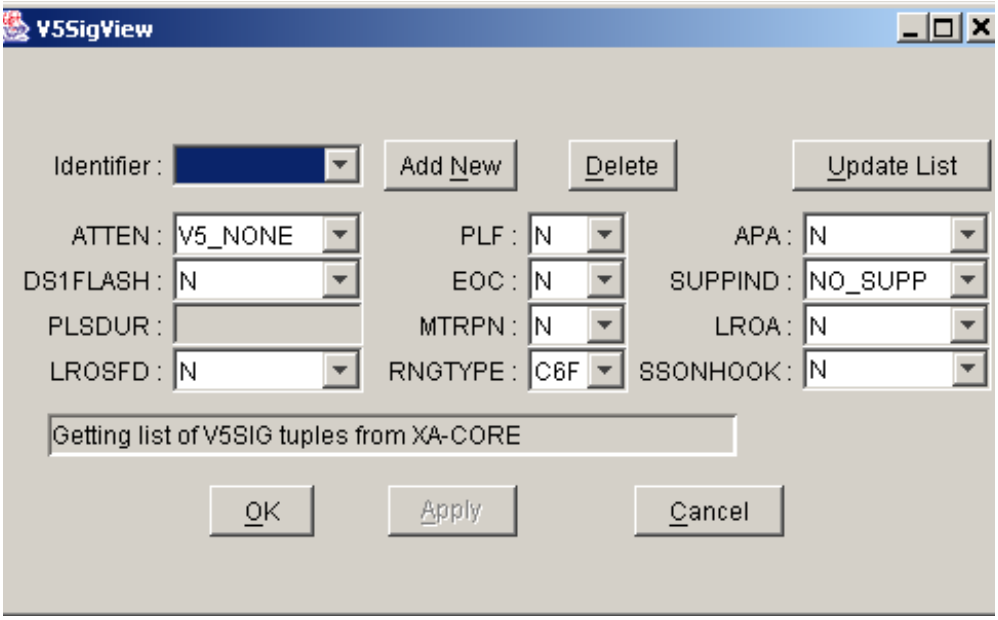
At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5.2SIG**.



2 Select the signaling template attributes to review using the Identifier drop-down menu.

Refer to table V5.2 signaling template attributes on page 474 to review the field definitions.



3 Click the **OK** or **Cancel** button when you are finished reviewing the sig template.

4 The procedure is complete.

V5.2 signaling template attributes (Sheet 1 of 3)

Field	Description
Identifier	The V5 sig profile ID. The operating company can define up to 127 different V5 signaling profile IDs; use an alphanumeric string of up to16 characters that uniquely identifies the ring character to ring type mapping set.
ATTEN:	Line attenuation field; possible values are: • V5_NONE-no additional attenuation is inserted • V5-DIGITAL-not currently supported • V5-ANALOG-attenuation is added at the access node (AN) line card.

V5.2 signaling template attributes (Sheet 2 of 3)

Field	Description
PLF:	Parked Line Feed fictionalizing; Enter Y if the battery signal should be sent from the local exchange to an access node when the line enters the lock or blocked state. The reduced battery signal allows the access node to save power. The default is N (No).
APA:	Accelerated Port Alignment: Enter Y to allow the alignment of port states without supply block and unblock messages for each port. Default is N (No).
DS1FLASH:	Digit 1 register recall. Enter Y to use digit 1 to represent recall during an active call (that is, not during digit collection). The default is N (No).
EOC:	End of Call Signaling. Enter Y to use a signaling sequence that sends a V5.2 'pulse signal no battery' message from the local exchange to the access node. This message indicates to the subscriber that the call has ended or failed. The end of call signaling feature provides the CPE with an indication of call completion. The default value is N (No).
SUPPIND:	Field Suppression Indication; possible values are: • NO_SUPP - No suppression is allowed. • LE_SUPP - Only a new message generated from the local exchange (LE) shall terminate the pulses being sent out from a user port. An example of a condition involving LE_SUPP would be to initiate a disconnect signal before pulsing has completed. • TE_SUPP - Only a new condition from terminal endpoint (TE) shall terminate the pulses being sent out from a user port. An example involving TE_SUPP would be to perform an on-hook before pulsing has completed. • LE_TE_SUPP - Either messages from the LE or new conditions from TE shall terminate the pulses being sent out from a user port.
PLSDUR:	Pulse Duration; When available for datafill, the value of this field reflects the length of the pulse defined in the Access Node. Enter a value between 0 and 31. The default value is 1.

V5.2 signaling template attributes (Sheet 3 of 3)

Field	Description
MTRPN:	Meter Pulse Notification; not currently supported. If the MTRPN field of V5SIG datafilled to Y, pulse notification will be enabled. Datafilling this field to FALSE will indicate that the V5.2 interface will not enable pulse notification.
LROA:	Line Reversal On Answer. Enter Y to indicate that each V5.2 virtual line in the office receives line reversal on seizure and forward disconnect. Enter N to indicate that V5.2 virtual lines in the office do not receive line reversal on seizure and forward disconnect. (If the entry is N, operating company personnel cannot provision fields LROSFD or RNGTYPE on a V5.2 line.) Enter CHKLN to indicate that V5.2 virtual lines in the office receive line reversal on answer. The line reversal depends on the LROA line option on each line.
SSONHOOK	Signal SS: On-hook message flag; Enter a value of Y to allow or N to disallow.
LROSFD:	If the entry in the field LROA is Y or CHKLN, enter data for field LROSFD to indicate if the office requires line reversal on seizure and forward disconnect signal. Enter Y to indicate all V5.2 virtual lines in the office have line reversal. Enter N to indicated all V5.2 virtual lines in the office do not have line reversal.
RNGTYPE	Ring Type; possible values for V5SIG table field RNGTYPE are: • C3C - The default ring type • C3D - Japanese ringing type • C6F - Portuguese ringing type

View V5.2 carrier and interface endpoint mapping

Purpose of this procedure

Use this procedure to view carrier-to-interface endpoint mapping information associated with a selected carrier or V5.2 interface.

When to use this procedure

Use this procedure when you need to determine the following information:

- the carriers associated with a specific V5.2 interface
- the link IDs used to associate a carrier to an interface
- the V5.2 interface terminating on a particular gateway.

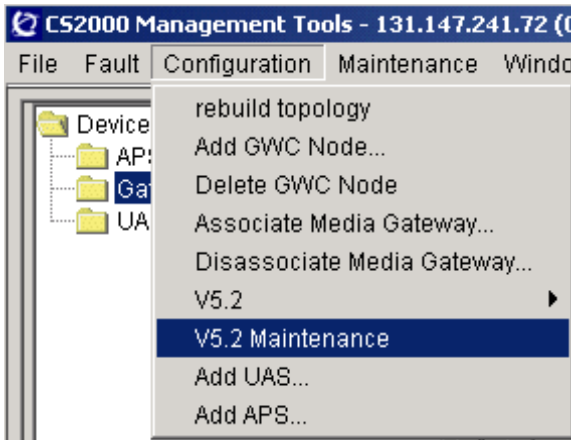
Prerequisites and guidelines

There are no prerequisites or guidelines for this procedure.

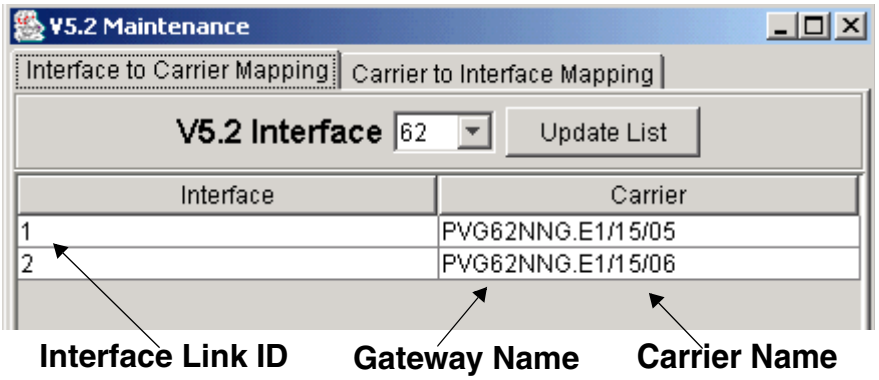
Action

At the CS 2000 GWC Manager client

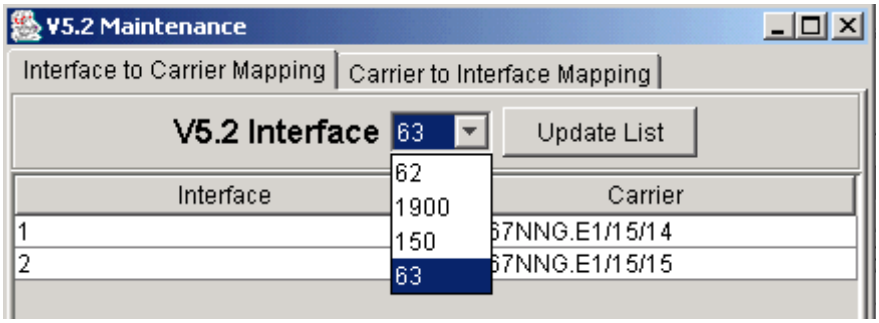
1 Click the **Configuration** menu and select **V5.2 Maintenance**.



The system responds by collecting information about all V5.2 interfaces in the database and presenting a maintenance panel to display them.



2 Click the V5.2 Interface drop-down menu to select an interface.



Note: Carrier links follow the naming convention for the protocol that the gateway they are associated with is running. The protocol may be either ASPEN or MEGACO. Refer to the procedure Add carriers to a GWC on page 201 for the naming convention used for different carriers and their supported protocols.

3 At the V5.2 Maintenance dialog box, perform the following steps:

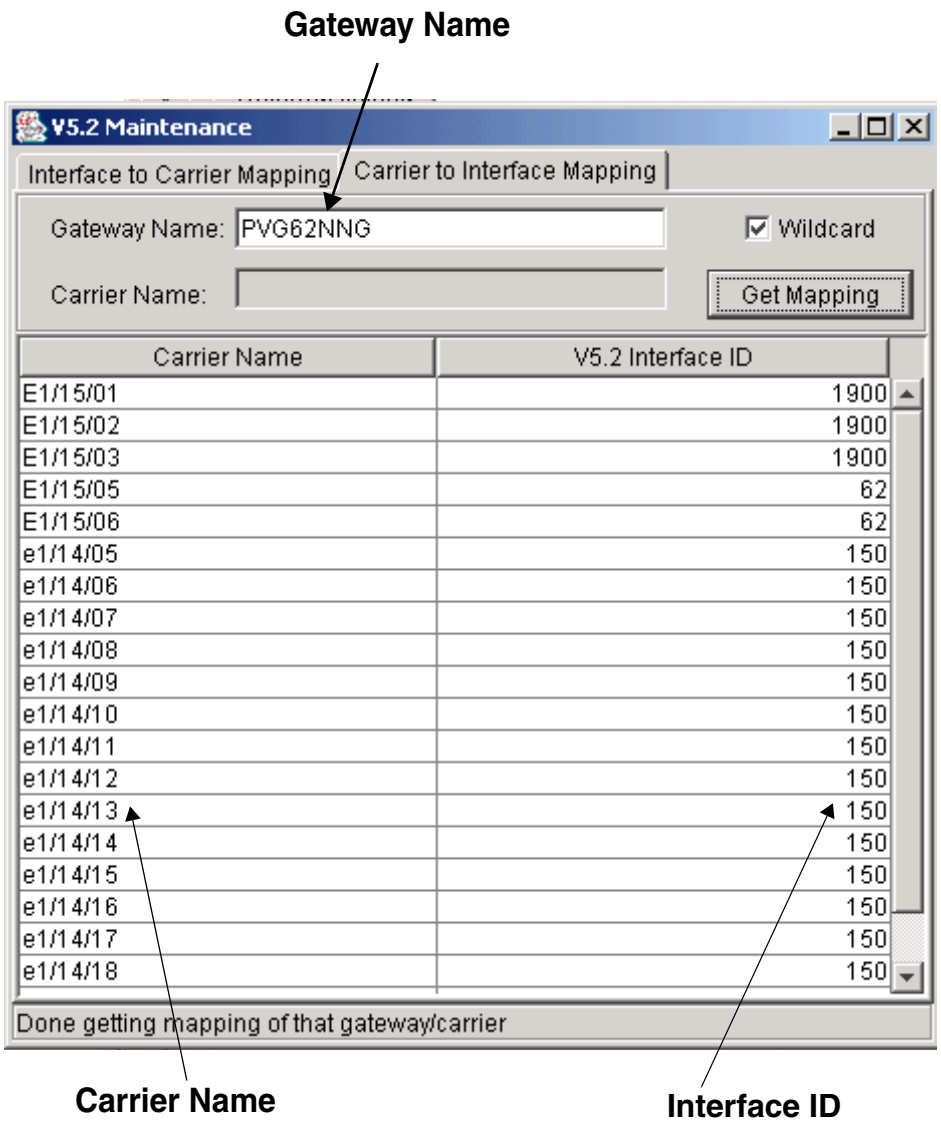
a Click the **Carrier to Interface Mapping** tab to view the V5.2 Interface ID-to-Carrier Name mapping.

b In the Gateway Name field, type the name of a gateway.

c Select the Wildcard check box.

Note: The wildcard option allows the system to examine all endpoints on a given gateway. With this option selected, the system then displays any endpoints associated with a V5 interface.

d Click the **Get Mapping** button.



Note: Carrier links follow the naming convention for the protocol that the Gateway they are associated with is running. The protocol may be either ASPEN or MEGACO. Refer to procedure Add carriers to a GWC on page 201 for the naming convention used for different carriers and their supported protocols.

4 The procedure is complete.

Modify V5.2 interfaces

Purpose of this procedure

Use this procedure to modify the attributes of an existing V5.2 interface.

When to use this procedure

Use this procedure whenever you need to modify an existing V5.2 interface.

Prerequisites and guidelines

The following prerequisites must be implemented before modifying V5.2 interfaces:

- The interface must be deactivated on the XA-Core using the maintenance level of the MAP before making the following modifications:
  - changing the Interface ID
  - changing V5PROV or V5RING templates
- The link must be busied on the XA-Core using the maintenance level of the MAP before making the following modifications:
  - changing or deleting the mapping of a link

Note the following guidelines applicable to this procedure:

- the interface can stay activated on the XA-Core when the following modifications are made:
  - changing V5SIG templates
  - adding a link
- the following interface options cannot be modified and require a new interface to be provisioned:
  - Maxlines (you cannot change the Access Node size of an existing interface)
  - GWC-ID

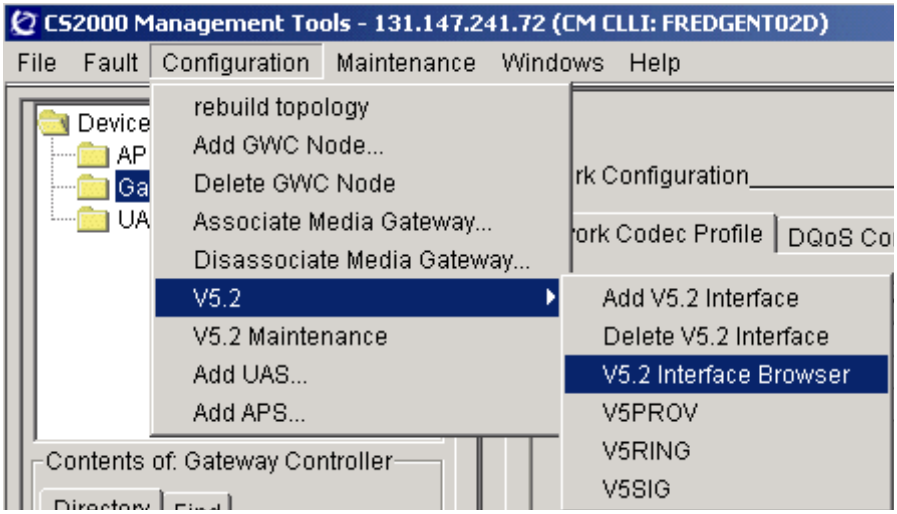
CAUTION

If the interface is deactivated, it will bring down all V5.2 line services on this interface.

Action

At the CS 2000 GWC Manager client

1 Click on the **Configuration** menu, and select **V5.2,** and then **V5.2 Interface Browser**.

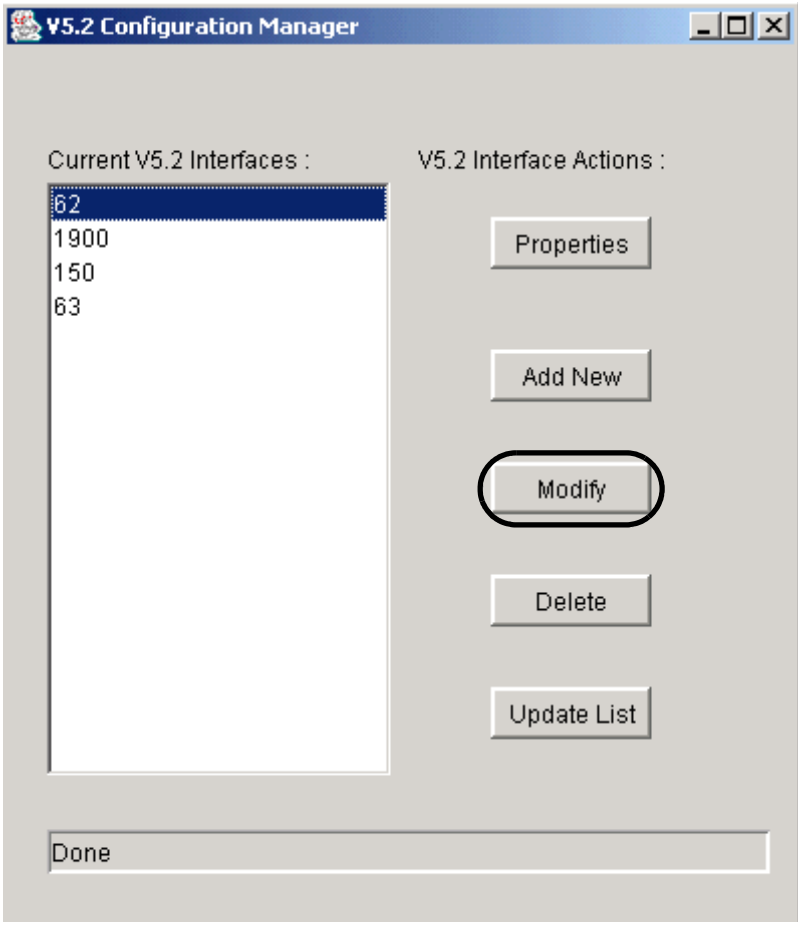


2 At the V5.2 Configuration Manager dialog box, select a V5.2 Interface from the list of available interfaces.

Your selection is highlighted.

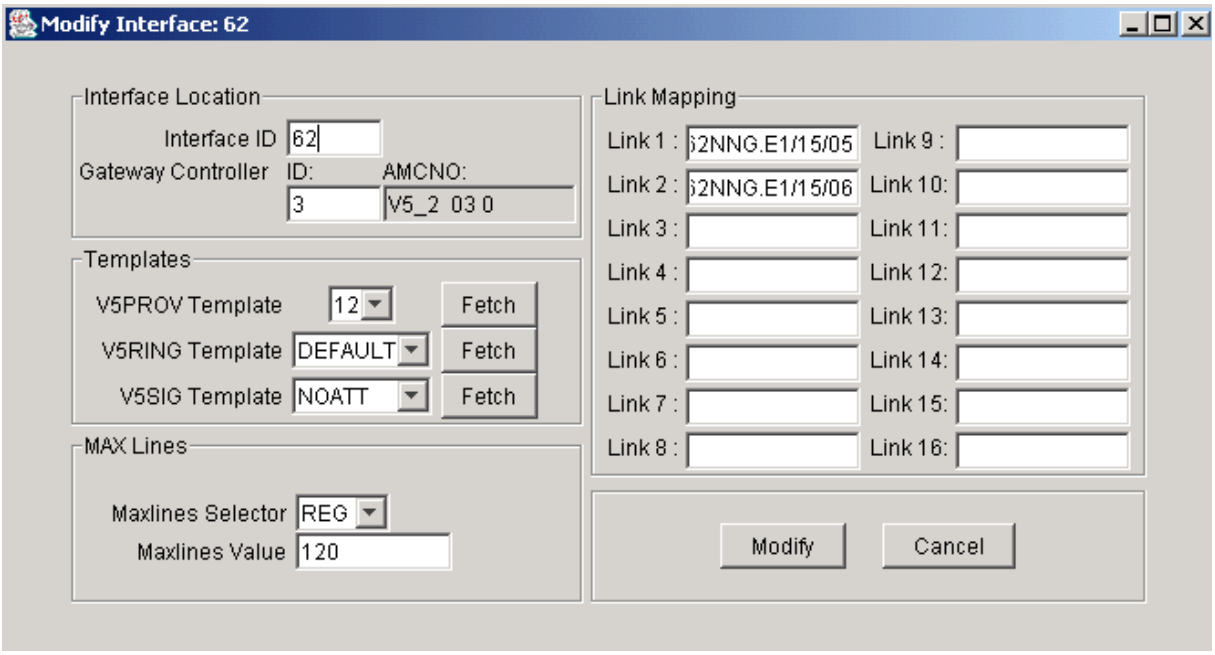
Note: If an interface that was added recently is not shown in the list, click the **Update List** button to force the configuration manager to refresh the list of current interfaces.

3 Click the **Modify** button.



4 Change the attributes in each of the following fields as needed.

Use table V5.2 interface properties on page 486 to assist you when changing attribute values.



5 Click the **Modify** button when you are finished.

6 Click **OK** at the Modify Confirmation box.

7 The procedure is complete.

V5.2 interface properties (Sheet 1 of 2)

Field	Description
Interface ID	The V5.2 interface identifier tuple is a unique number between 0 and 16777215. It is unique between the local exchange and the access node. Up to 53 interfaces can be configured per GWC node.
Gateway Controller ID	Type the GWC number in the range of 1-255.
AMCNO	AN (access node) location, a unique line identifier.
V5PROV Template	Click the drop-down menu button to obtain a list of up to 127 definable provisioning profiles.
V5RING Template	Click the Fetch button to obtain a list of available ringing profiles (up to 127 definable profiles) or select the Default template.

V5.2 interface properties (Sheet 2 of 2)

Field	Description
V5SIG Template	Click the Fetch button to obtain a list of available signaling profiles (up to 127 definable profiles). Do not use the Default template as this will generate error messages from the XA-Core.
MAX Lines Selector	REG (regular) lines or PRIM (primary) lines; only REG lines are supported.
MAX Lines	Maximum number of lines assigned to the interface from 1 to 2048, based on the capacity of the AN.
Link Mapping	V5 link-to-carrier mapping fields (up to 16 for each interface). ***Note:*** Carrier links must follow the naming convention for the protocol that the Gateway they are associated with is running. The protocol may be either ASPEN or MEGACO. Refer to procedure Add carriers to a GWC on page 201 for the naming convention used for various carriers and their applicable supported protocols. ASPEN format carrier links are named as follows: <Gateway Name>.E1_<xxxx> Where Gateway Name is the provisioned name of a PVG gateway, and <xxxx> is a combined shelf slot and E1 number. MEGACO format carrier links are named as follows: <Gateway Name>/E1/<yy>/<zz> Where Gateway Name is the provisioned name of a suitable Gateway, <yy> is a shelf slot number and <zz> is an E1 number.

Modify a V5 interface provisioning template

Purpose of this procedure

Use this procedure to make changes to the V5 interface provisioning template datafill.

When to use this procedure

Use this procedure when you need to modify certain provisioning template datafill.

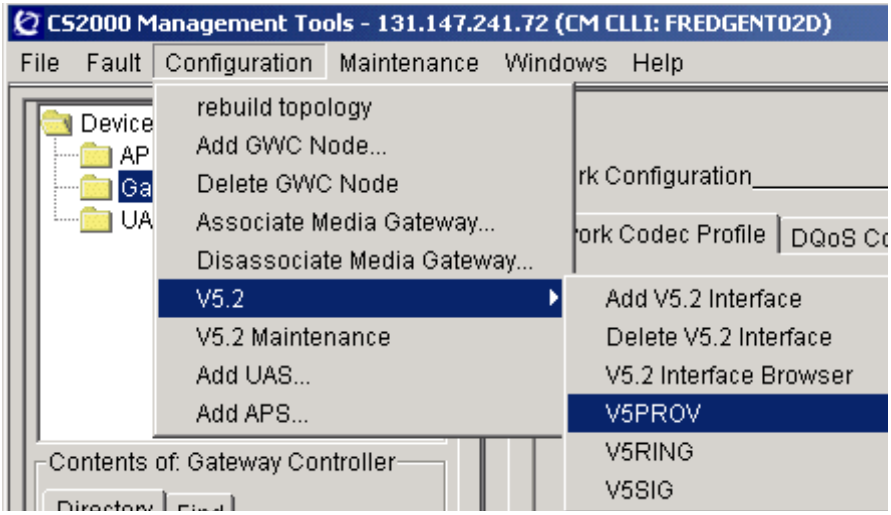
Prerequisites and guidelines

You cannot modify a provisioning template that is currently being used by a V5.2 interface. If necessary, check all existing V5.2 interfaces and modify them to ensure they are not referencing the template being modified. Refer to procedure View V5.2 interface properties on page 461 to perform this task.

Action

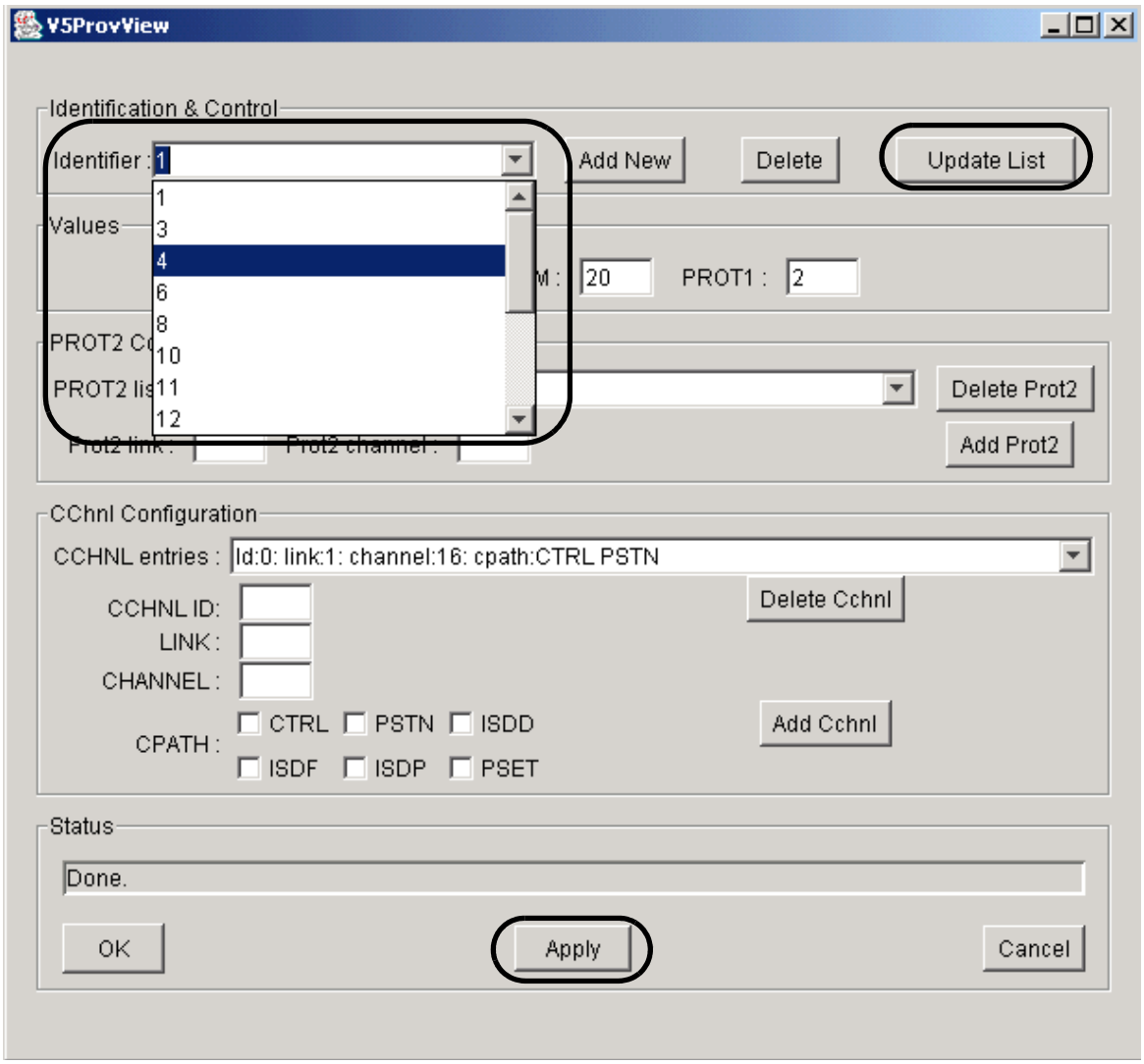
At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5PROV**.



2 Select a provisioning template to modify by choosing an Identifier using the drop-down menu.

If you cannot find the Identifier you need, click the **Update List** button.



3 Use table V5 interface provisioning template on page 491 to review and modify the field entries.

Note the following specific instructions:

- To delete an existing Prot2 link and channel, select the link and channel numbers from the PROT2 drop-down list and click the **Delete Prot2** button.
- To add a new Prot2 link and channel, type the link and channel numbers in the Prot2 link and Prot2 channel data fields and click the **Add Prot2** button.

  Note: For a protected V5.2 interface with protection group 2, four C-channels are needed: primary link and secondary link, time slot 16, and two additional C-channels running active and standby c-path for V5 PSTN protocol.

- To delete a C-channel configuration entry, select the entry from the CCHNL entries drop-down list and click the **Delete Cchnl** button.
- To add a new C-channel configuration entry, type the CCHNL ID, LINK, CHANNEL entries the appropriate data fields, select the appropriate CPATH check boxes and click the **Add Cchnl** button.

4 Click the **Apply** button when you are finished making changes.

5 Click the **OK** button to close the V5 provisioning view window.

6 The procedure is complete.

V5 interface provisioning template (Sheet 1 of 3)

Field	Description
Identifier:	V5 provisioning variant ID. The operating company defines the different V5 provisioning IDs; use a numeric value from 0 to 127.
TBCC	Two bearer channel control timers. Set the timers to between 500 and 1500 ms; use a numeric value between 5 and 15 (5 =500 ms).
LKMJALM	Link manager alarm: threshold level of V5.2 link failure before the link triggers a major alarm. The value is the percentage of fault links that must be exceeded to generate the alarm; use a numeric value between 0 and 100.

V5 interface provisioning template (Sheet 2 of 3)

Field	Description
PROT1	Protection link 1. Secondary link protection group 1 switches to this link if the primary C-channel link fails; use a numeric value from 1 to 16. **Note:** For a protected V5.2 interface with protection group 1, two C-channels are needed (primary link and secondary link, time slot 16). For an unprotected V5.2 interface only one C-channel is needed (primary link, time slot 16).
Add Prot2 Delete Prot2 Buttons	Click the **Add Prot2** button to add protection group 2. Click the **Delete Prot2** button to remove it. **Note:** For a protected V5.2 interface with protection group 2, four C-channels are needed: primary link and secondary link, time slot 16, and two additional C-channels running active and standby c-path for V5 PSTN protocol.
PROT2 list:	Protection link 2. Standby link and C-channel for protection group 2. First entry is the link, the second entry is the channel.
Prot2 link:	Link for standby link for protection group 2.
Prot2 channel:	Channel for standby link for protection group 2.
CCHNL entries:	C-channel link information; a maximum of 43 multiples of fields: CCHNL ID, LINK, CHANNEL, CPATH.
CCHNL ID:	Control channel ID number. An internal C-channel ID number; a numeric value from 0 to 9 of provisioning channel IDs.
LINK:	The V5.2 link number that the C-channel resides on; a numeric value between 1 and 16.
CHANNEL	C-channel number or physical channel that the C-channel is on. Table control only accepts channel 16 for CNTRL. Use channel 31 after channels 15 and 16 have been used.
CPATH	Type of C-path control messages carried on the C-channel.
CTRL	Control channel messages.
PSTN	Public switched telephone network control messages.
ISDD	ISDN D-channel control messages; not currently supported.
ISDF	ISDN F-channel control messages; not currently supported.

V5 interface provisioning template (Sheet 3 of 3)

Field	Description
ISDP	ISDN-P-channel control messages; not currently supported.
PSET	Proprietary phone signaling (EBS); not currently supported.

Modify a V5 ring template

Purpose of this procedure

Use this procedure to modify V5 ring templates for the V5RING table which contains information relating to mappings between ringing cadences and ringing types. Table V5RING is referenced by the main CM table GPPTRNSL.

When to use this procedure

Use this procedure when you need to modify the datafill for a selected template.

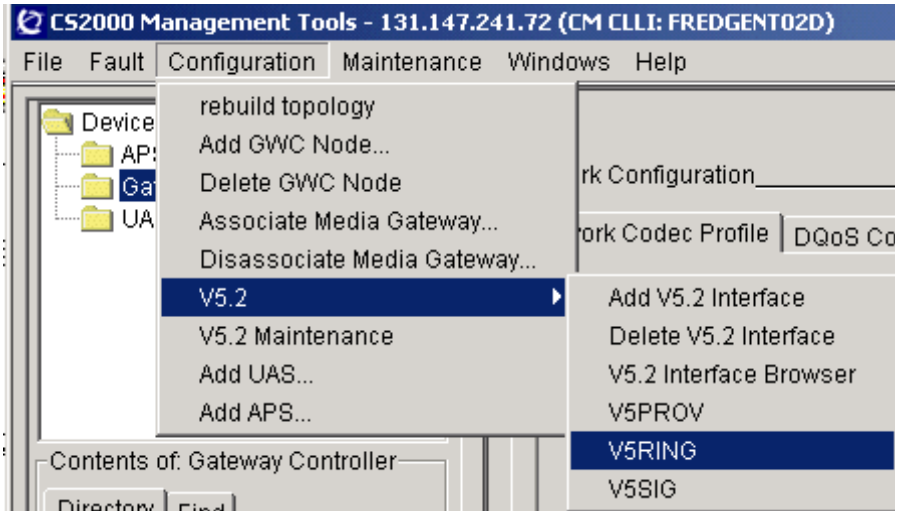
Prerequisites and guidelines

No V5.2 interface can be referencing this template while you are making changes. Check all existing interfaces and make the necessary changes to ensure they are not referencing the template you intend to modify. Refer to procedureView V5.2 interface properties on page 461.

Action

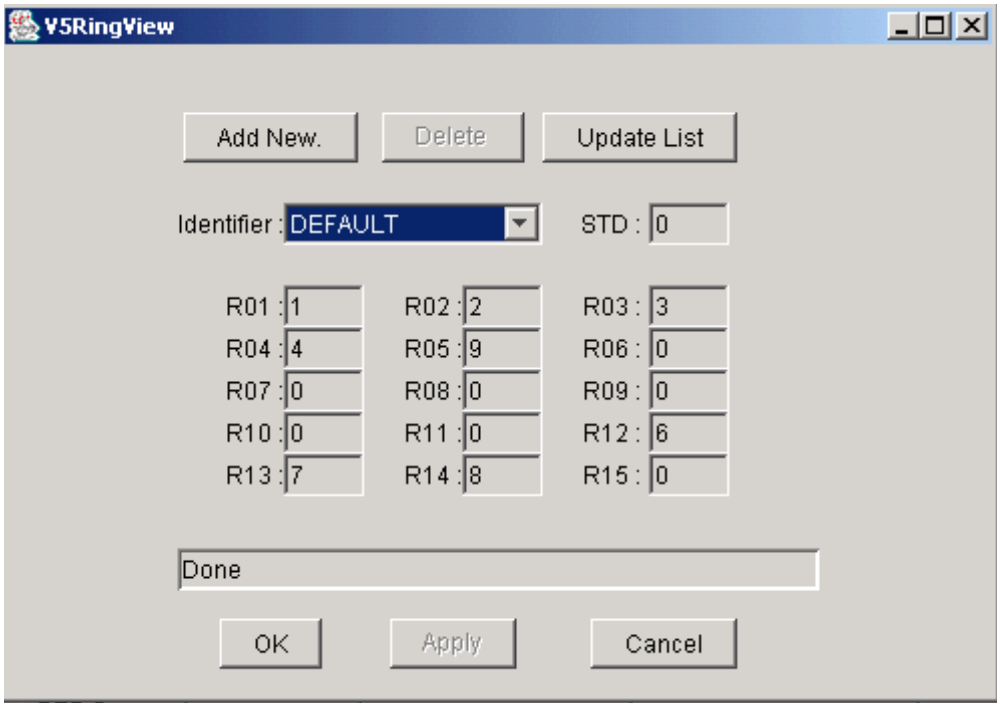
At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5RING**.



The system displays the V5RingView dialog box.

2 Use table V5.2 ring template attributes on page 496 to modify the ring attributes for a V5.2 ring template.



3 Click the **Apply** button when you are finished modifying the ring template.

4 Click the **OK** button to close the V5 ring view window.

5 The procedure is complete.

V5.2 ring template attributes (Sheet 1 of 3)

Field	Description
Identifier	The V5 ring mapping ID. The operating company defines the different V5 ring mapping IDs; use an alphanumeric string up to16 characters that uniquely identifies the ring character to ring type mapping set.
STD	Standard Ring; a number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 0.
R01	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 1. XPM Ring Char 1 is commonly used for Distinctive Ringing 1.

V5.2 ring template attributes (Sheet 2 of 3)

Field	Description
R02	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 2. XPM Ring Char 2 is commonly used for Distinctive Ringing 2.
R03	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 3. XPM Ring Char 3 is commonly used for Distinctive Ringing 3.
R04	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 4. XPM Ring Char 4 is commonly used for Distinctive Ringing 4 and Automatic Recall.
R05	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 5. XPM Ring Char 5 is commonly used for Distinctive Ringing 5.
R06	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 6. No known service matching.
R07	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 7. No known service matching.
R08	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 8. No known service matching.
R09	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 9. No known service matching.
R10	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 10. No known service matching.
R11	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 11. No known service matching.
R12	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 12. Ring Char 12 is most commonly used for Distinctive Ringing 6 and Teen Service SDN1.
R13	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 13. Ring Char 13 is most commonly used for Distinctive Ringing 7 and Teen Service SDN2.

V5.2 ring template attributes (Sheet 3 of 3)

Field	Description
R14	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 04. Ring Char 14 is most commonly used for Distinctive Ringing 8 and Teen Service SDN3.
R15	A number (0-31) representing the V5 cadenced-ringing type to be mapped to XPM Ring Char 15. No known service matching.

Modify a V5 signaling template

Purpose of this procedure

Use this procedure to modify an existing datafilled interface signaling template.

When to use this procedure

Use this procedure when you wish to change the datafill for an existing interface signaling template.

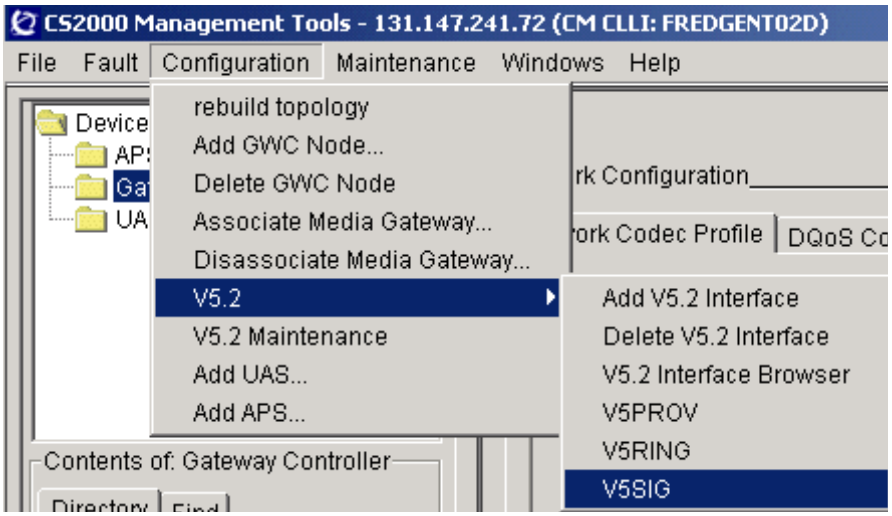
Prerequisites and guidelines

Ensure that the signaling template to be removed is not in use by a V5.2 interface. Refer to the procedure View V5.2 interface properties on page 461 in this NTP.

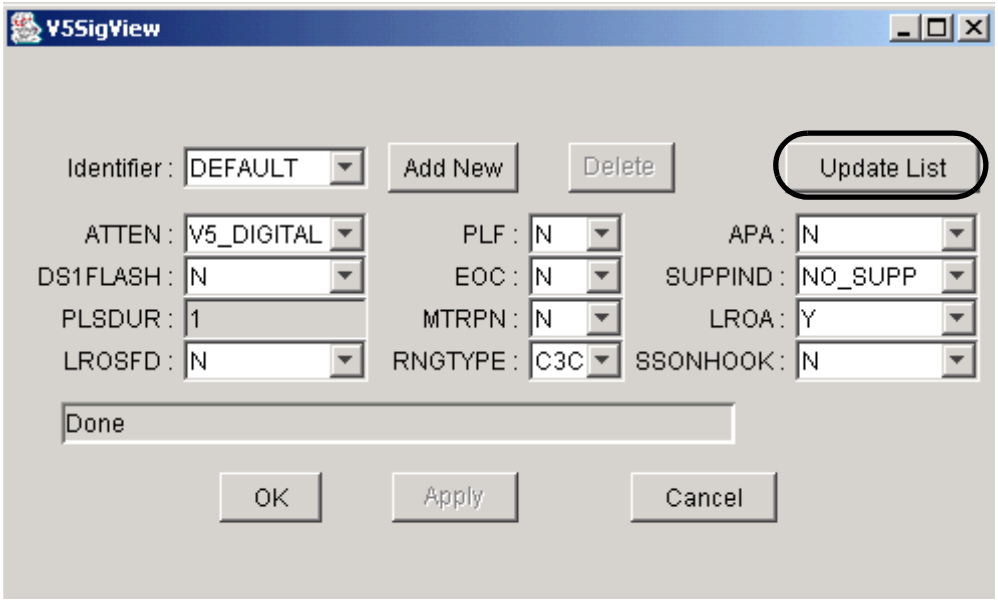
Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5.2SIG**.



2 Select a template identifier to modify using the Identifier drop-down menu. If the identifier is not available, click the **Update List** button.



3 Refer to table V5.2 signaling template attributes on page 500 for information on modifying the datafill for all signaling attributes on a selected V5.2 interface.

4 Click the **Apply** button when you are finished modifying the sig template.

5 Click the **OK** button to close the V5 sig view window.

6 The procedure is complete.

V5.2 signaling template attributes (Sheet 1 of 3)

Field	Description
Identifier	The V5 sig profile ID. The operating company can define up to 127 different V5 signaling profile IDs; use an alphanumeric string of up to16 characters that uniquely identifies the ring character to ring type mapping set.
ATTEN:	Line attenuation field; possible values are: • V5_NONE-no additional attenuation is inserted • V5-DIGITAL-not currently supported • V5-ANALOG-attenuation is added at the AN line card

V5.2 signaling template attributes (Sheet 2 of 3)

Field	Description
PLF:	Parked Line Feed fictionalizing; Enter Y if the battery signal should be sent from the local exchange to an access node when the line enters the lock or blocked state. The reduced battery signal allows the access node to save power. The default is N (No).
APA:	Accelerated Port Alignment: Enter Y to allow the alignment of port states without supply block and unblock messages for each port. The default is N (No).
DS1FLASH:	Digit 1 register recall. Enter Y to use digit 1 to represent recall during an active call (that is, not during digit collection). The default is N (No).
EOC:	End of Call Signaling. Enter Y to use a signaling sequence that sends a V5.2 'pulse signal no battery' message from the local exchange to the access node. This message indicates to the subscriber that the call has ended or failed. The end of call signaling feature provides the CPE with an indication of call completion. The default value is N (No).
SUPPIND:	Field Suppression Indication; possible values are: • NO_SUPP - No suppression is allowed. • LE_SUPP - Only a new message generated from the local exchange (LE) shall terminate the pulses being sent out from a user port. An example of a condition involving LE_SUPP would be to initiate a disconnect signal before pulsing has completed. • TE_SUPP - Only a new condition from terminal endpoint (TE) shall terminate the pulses being sent out from a user port. An example involving TE_SUPP would be to perform an on-hook before pulsing has completed. • LE_TE_SUPP - Either messages from the LE or new conditions from TE shall terminate the pulses being sent out from a user port.
PLSDUR:	Pulse Duration; When available for datafill, the value of this field reflects the length of the pulse defined in the Access Node. Enter a value between 0 and 31. The default value is 1.

V5.2 signaling template attributes (Sheet 3 of 3)

Field	Description
MTRPN:	Meter Pulse Notification; not currently supported. If the MTRPN field of V5SIG datafilled to Y, pulse notification will be enabled. Datafilling this field to FALSE will indicate that the V5.2 interface will not enable pulse notification.
LROA:	Line Reversal On Answer. Enter Y to indicate that each V5.2 virtual line in the office receives line reversal on seizure and forward disconnect. Enter N to indicate that V5.2 virtual lines in the office do not receive line reversal on seizure and forward disconnect. (If the entry is N, operating company personnel cannot provision fields LROSFD or RNGTYPE on a V5.2 line.) Enter CHKLN to indicate that V5.2 virtual lines in the office receive line reversal on answer. The line reversal depends on the LROA line option on each line.
SSONHOOK	Signal SS: On-hook message flag; Enter a value of Y to allow or N to disallow.
LROSFD:	If the entry in the field LROA is Y or CHKLN, enter data for field LROSFD to indicate if the office requires line reversal on seizure and forward disconnect signal. Enter Y to indicate all V5.2 virtual lines in the office have line reversal. Enter N to indicated all V5.2 virtual lines in the office do not have line reversal.
RNGTYPE	Ring Type; possible values for field RNGTYPE are: • C3C - The default ring type • C3D - Japanese ringing type • C6F - Portuguese ringing type

Delete V5.2 interfaces

Purpose of this procedure

Use this procedure to decommission a V5.2 interface.

When to use this procedure

Use this procedure when you wish to delete an existing V5.2 interface that is no longer in use.

Prerequisites and guidelines

The following prerequisites must be implemented before removing V5.2 interfaces:

- lines associated with the interface must be deleted
- all lines referenced on the interface must be de-provisioned
- the interface must be deactivated in the XA-Core using the maintenance level of the MAP

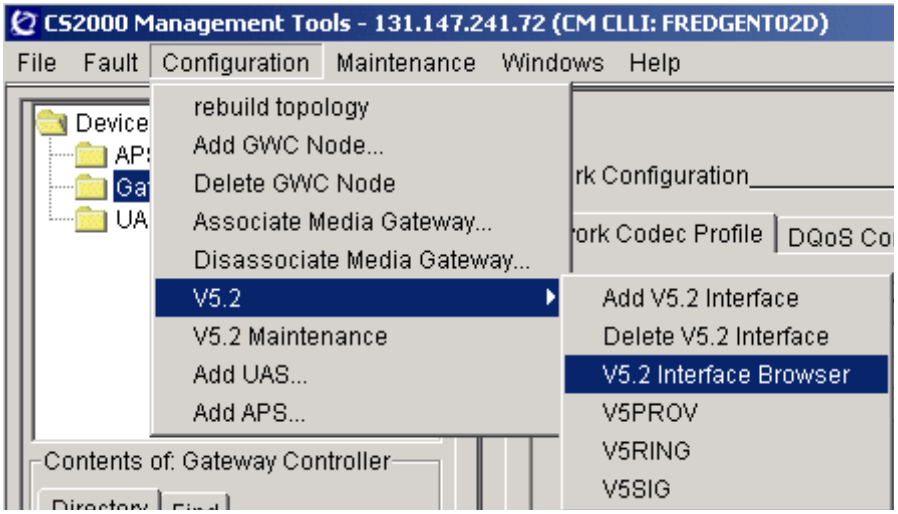
CAUTION

This procedure will bring down all V5.2 line services on the interface.

Action

At the CS 2000 GWC Manager client

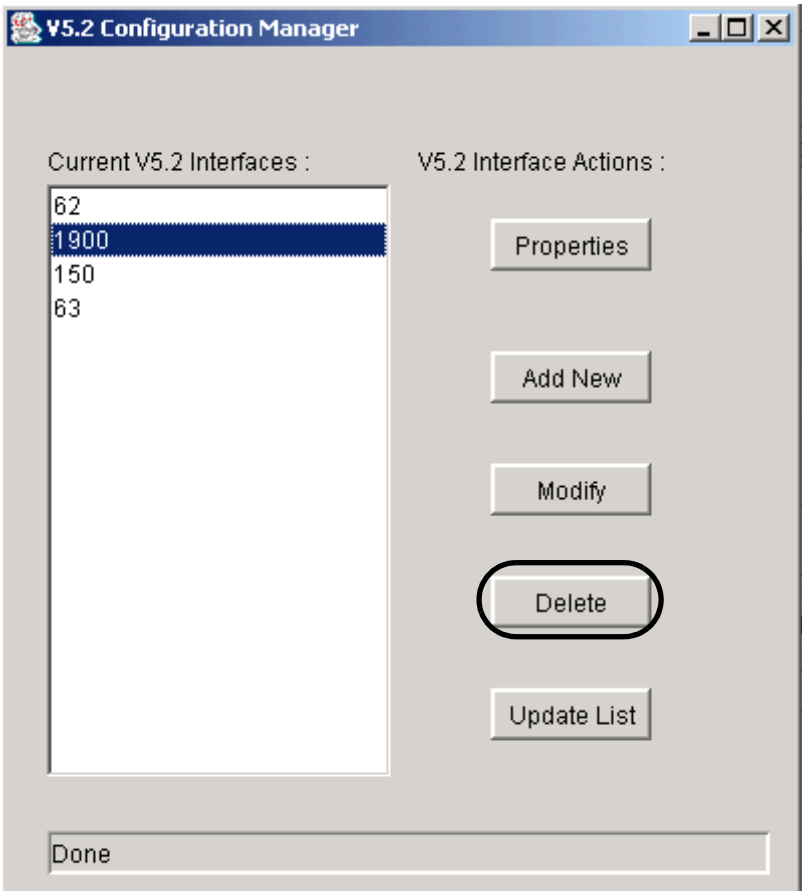
1 Click on the **Configuration** menu and select **V5.2** and then **V5.2 Interface Browser**.



2 At the V5.2 Configuration Manger dialog box, select the interface you wish to delete.

Your selection is highlighted.

3 Click the **Delete** button.



4 Click **OK** at the Delete Confirmation box.

5 The procedure is complete.

Delete a V5 interface provisioning template

Purpose of this procedure

Use this procedure to remove a datafilled V5 interface provisioning template.

When to use this procedure

Use this procedure when the template is no longer needed, or if it is being replaced by another template.

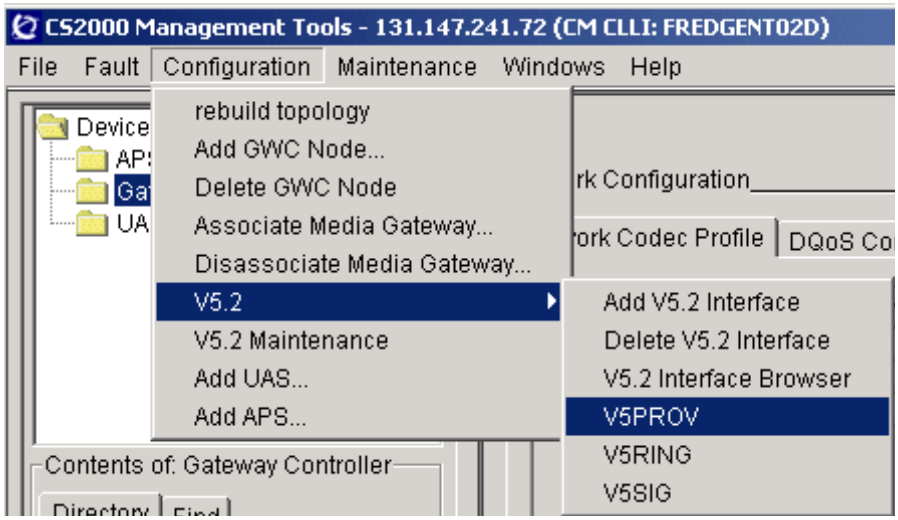
Prerequisites and guidelines

Ensure that no V5.2 interface is referencing this template when it is removed. Check all existing interfaces and modify them to ensure they are not referencing the template being removed. Refer to procedure View V5.2 interface properties on page 461.

Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5PROV**.



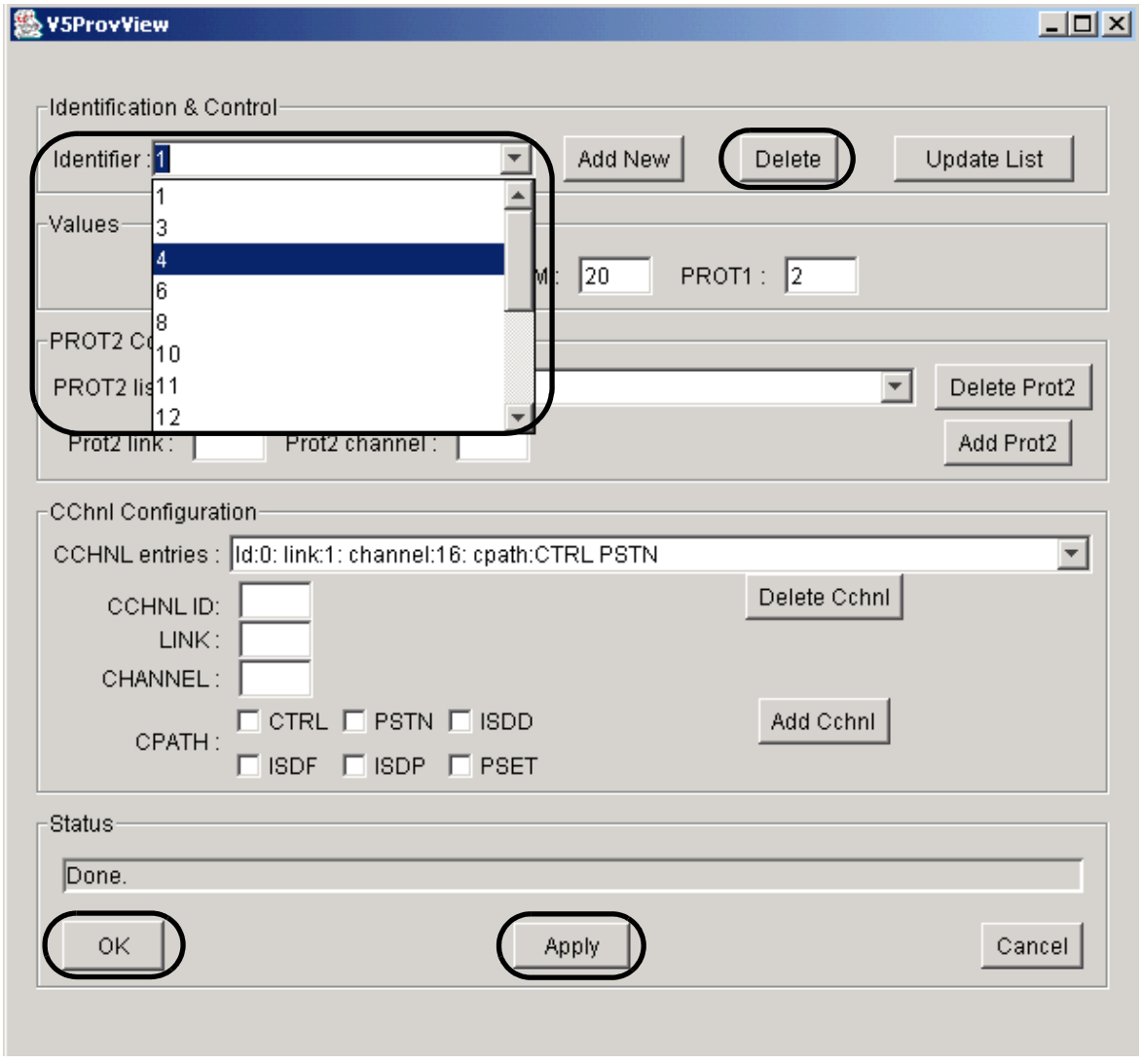
2 Select a provisioning template identifier using the drop-down menu.

Your selection is highlighted.

3 Click the **Delete** button.

4 Click the **Apply** button when you are finished deleting provisioning templates.

5 Click the **OK** button to close the V5 provisioning view window.



6 The procedure is complete.

Delete a V5 ring template

Purpose of this procedure

Use this procedure to delete an existing V5 ring template.

When to use this procedure

Use this procedure when you wish to remove a ring template from the identifier list.

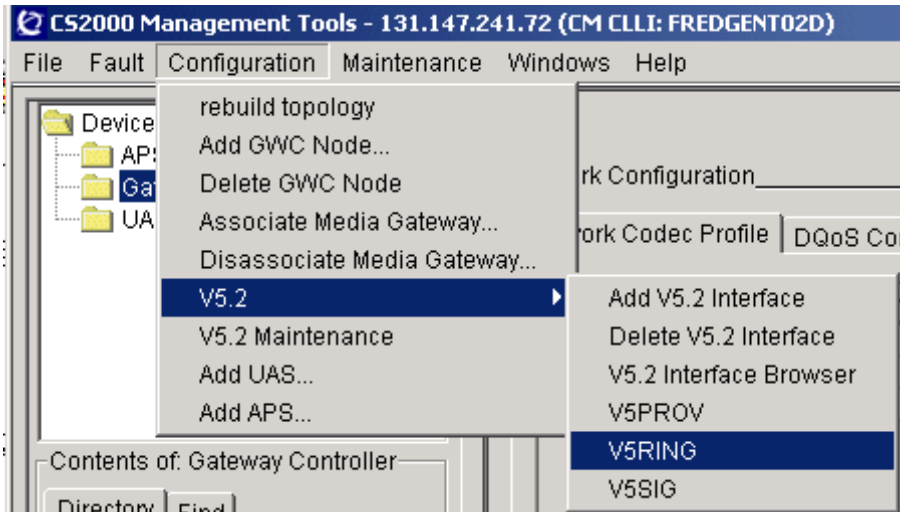
Prerequisites and guidelines

Ensure that the ring template to be removed is not currently being used by a V5.2 interface.

Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5RING**.



2 At the V5RingView dialog box, select a ring mapping identifier to delete using the Identifier drop-down menu.

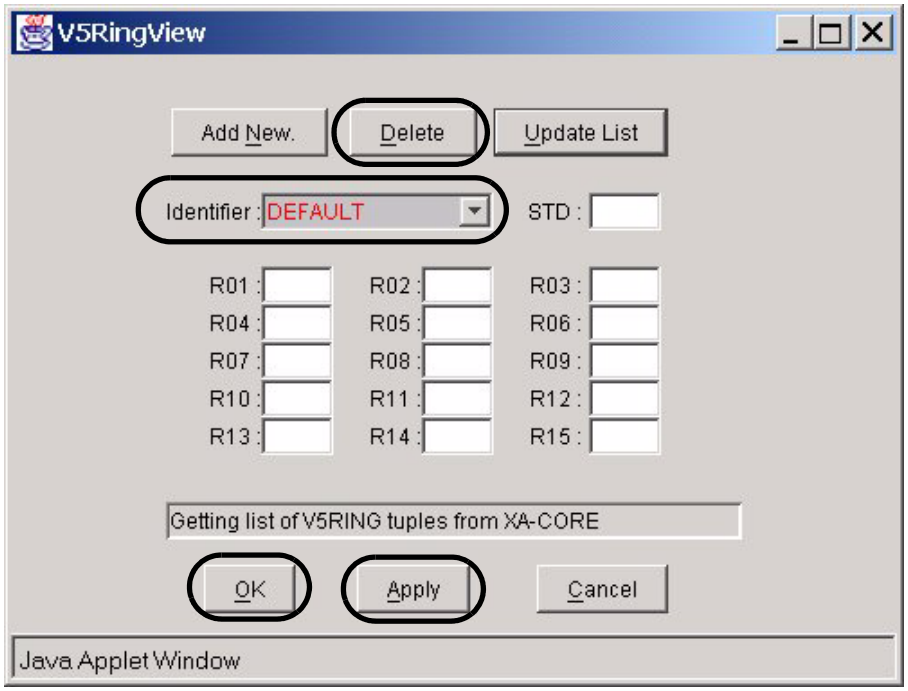
If the identifier is not available, click the **Update List** button.

Note: You cannot delete the default identifier.

3 Click the **Delete** button to delete the ring template.

4 Click the **Apply** button when you are finished deleting ring templates.

5 Click the **OK** button to close the V5 ring view window.



6 The procedure is complete.

Delete a V5 signaling template

Purpose of this procedure

Use this procedure to delete a datafilled interface signaling template.

When to use this procedure

Use this procedure when you wish to remove a signaling template from the identifier list.

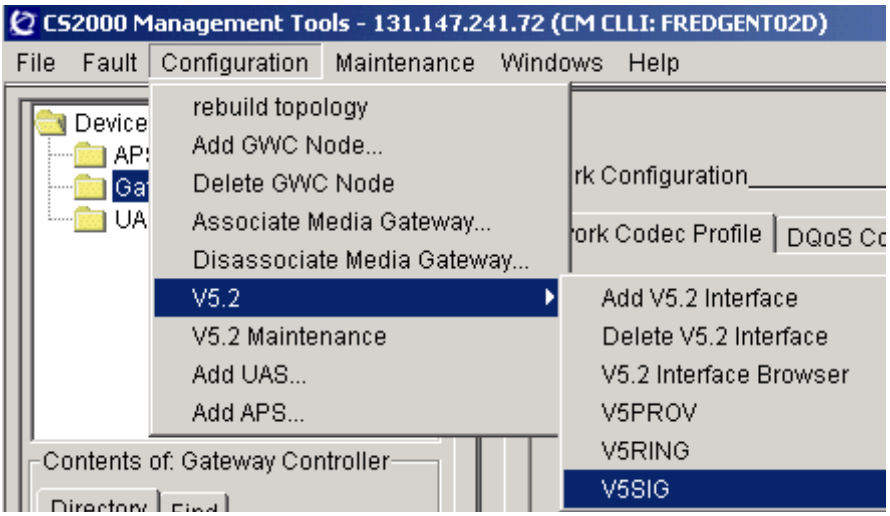
Prerequisites and guidelines

Ensure that the signaling template to be removed is not currently being used by a V5.2 interface. Refer to procedure View V5.2 interface properties on page 461 in this NTP.

Action

At the CS 2000 GWC Manager client

1 Click the **Configuration** menu, select **V5.2,** and then **V5.2SIG**.



2 At the V5SigView dialog box, select a template identifier to delete using the Identifier drop-down menu.

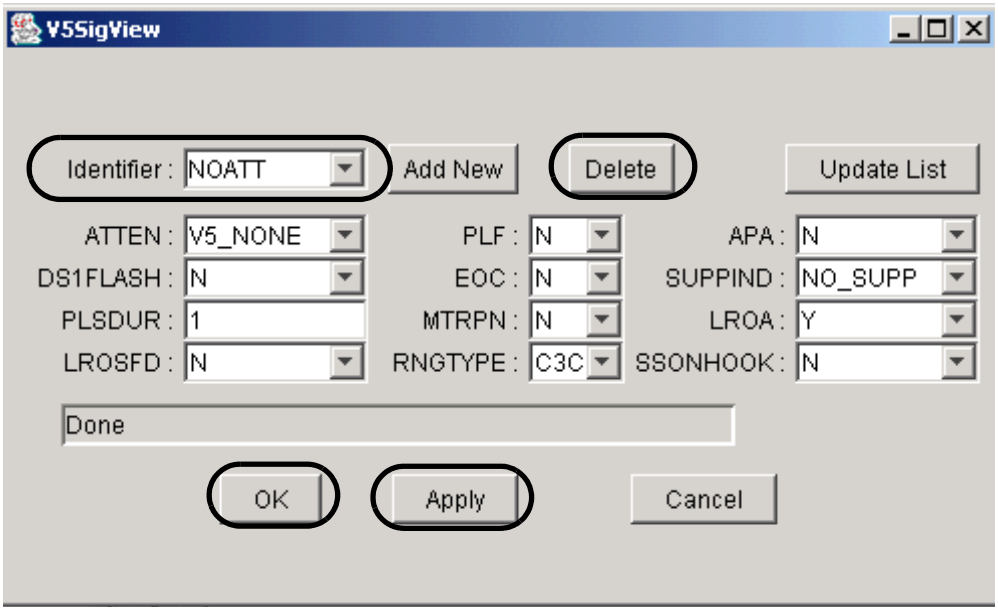
If the identifier is not available, click the **Update List** button.

3 Click the **Delete** button to delete the template.

4 If necessary, repeat step 2 and step 3 to delete other sig templates.

5 Click the **Apply** button when you are finished deleting sig templates.

6 Click the **OK** button to close the V5SigView dialog box.



7 The procedure is complete.

Busy a GWC node

Purpose of this procedure

Use this procedure to busy the services allocated on a fully configured Gateway Controller (GWC) node, comprised of unit 0 and unit 1 GWC cards.

When to use this procedure

Use this procedure when it is necessary to make the gateway services provided by either the active or standby GWC card unavailable for call processing activity.

Prerequisites and guidelines

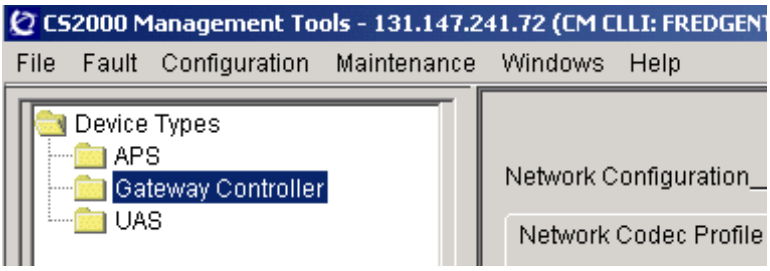
CAUTION
Partial service disruption
This procedure busies call processing service on an entire GWC node. All services provisioned for the GWC cards in the node will be disabled.

If you wish to busy (lock) the services for a single, standby GWC card in a node, while allowing the other card to continue processing call traffic, refer to procedure “Disable (BSY) GWC services” for a single card in the *Gateway Controller Security and Administration* NTP, NN10213-611.

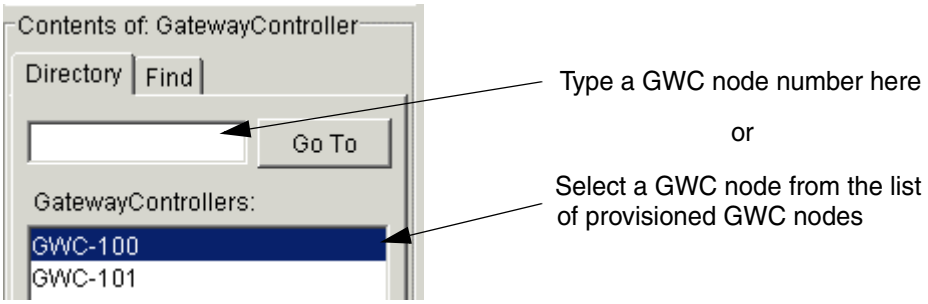
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



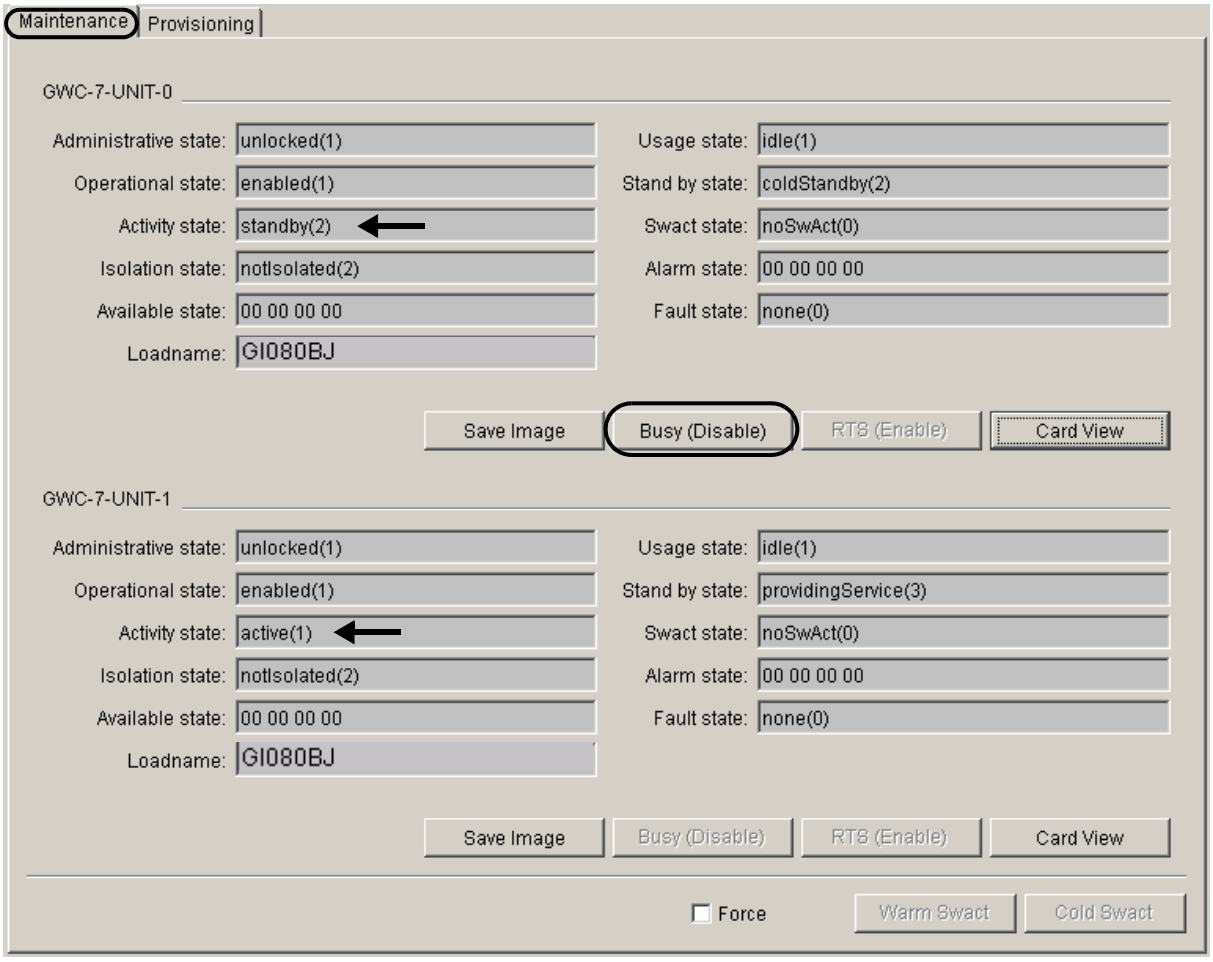
2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to busy.



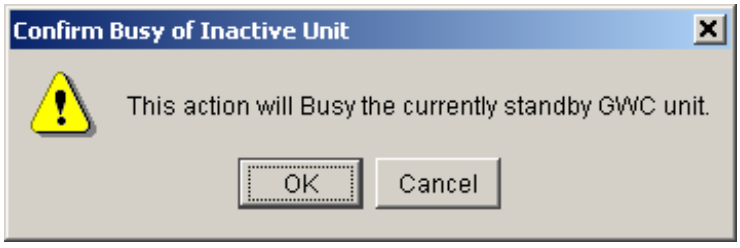
3 Click the **Maintenance** tab.

4 Locate the Activity state field for each GWC unit and determine which unit (card) is active and which is standby.

5 Click the **Busy (Disable)** button for the standby GWC unit.



6 At the confirmation box, click **OK** to continue busy the standby GWC unit.

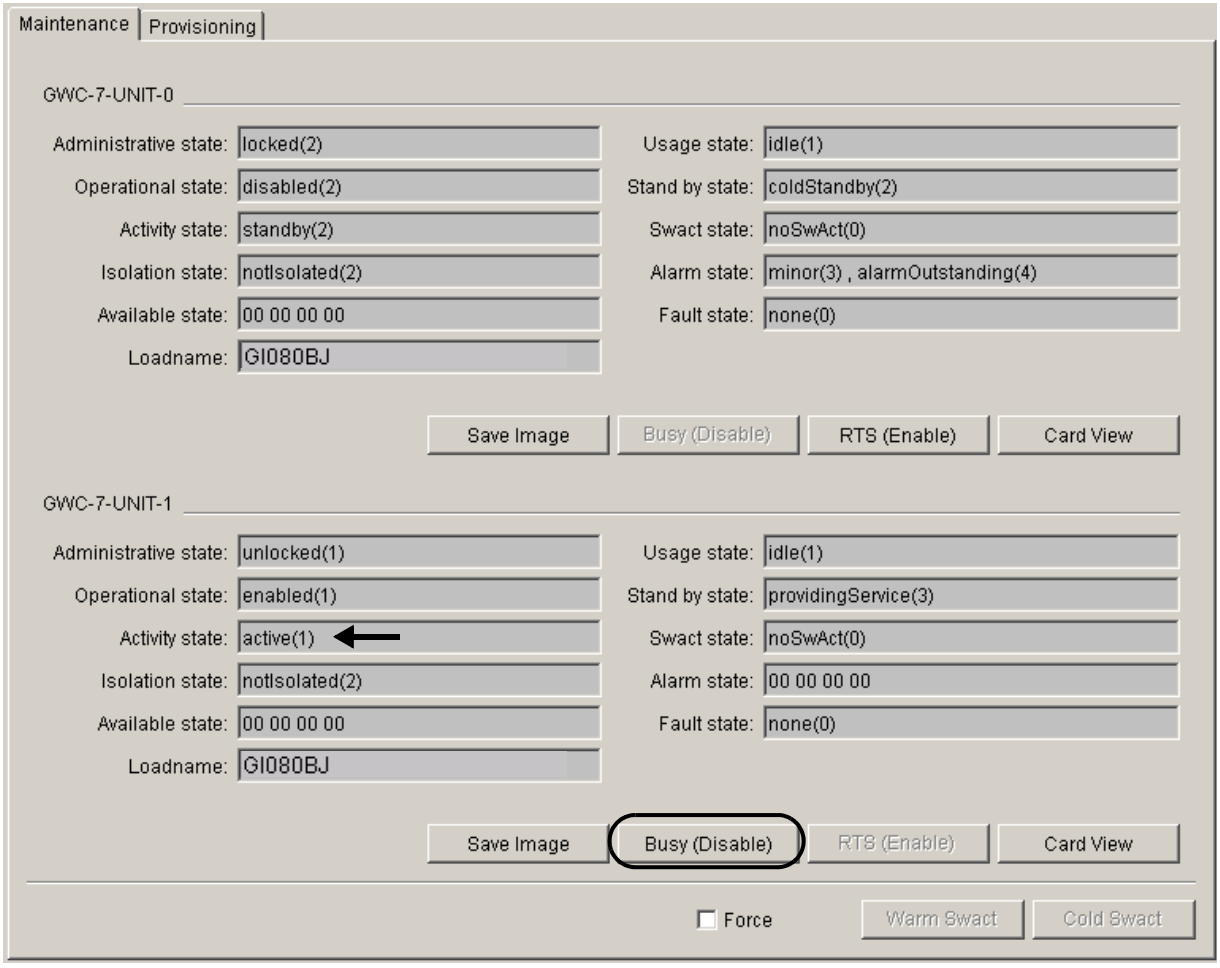


7 Verify that the states for the unit are set as follows:

8 Use the following table to determine your next step.

If you need to busy	Do
both the standby and the active GWC units (the entire node)	go to step 9.
only the standby GWC unit	go to step 12.

9 Click the **Busy (Disable)** button for the active GWC unit.



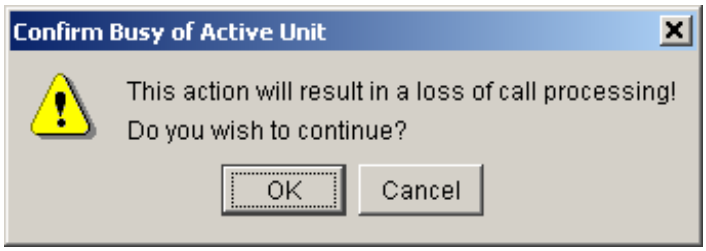
Note: If the **Busy (Disable)** button for the active GWC is not available, wait for 30 seconds.

You can refresh the screen as follows: At the top of the CS 2000 GWC Manager screen, click the **Windows** menu item and select **Refresh GWC Status**.

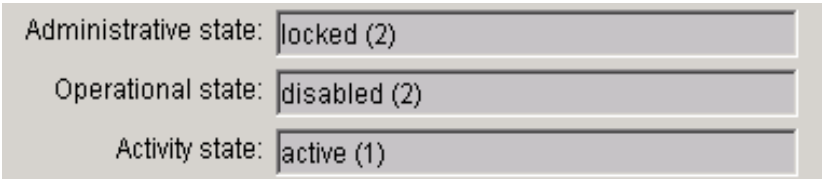
10

CAUTION
Partial service disruption
Continuing this procedure removes all service from the entire GWC node. All services provisioned for the GWC cards in the node will be disabled.

At the confirmation box, click **OK** to continue busying the active GWC unit.



11 Verify that the states for the unit that you busied are set as follows:



12 Repeat this procedure for other GWC nodes you wish to busy.

13 The procedure is complete.

Lock a GWC card

Purpose of this procedure

Use this procedure to lock a Gateway Controller (GWC) card using the CS 2000 SAM21 Manager. This action takes the GWC card hardware out of service.

When to use this procedure

Use this procedure in the following contexts:

- When you are removing the card from service.
- With procedure Unlock a GWC card on page 523 to reboot a GWC and force a software download.
- As part of fault clearing activity to determine if a problem is temporary or persistent.
- When you have applied a patch to (or removed a patch from) the GWC software using the Network Patch Manager (NPM) and have created a new GWC software image on the CS 2000 Core Manager or Core and Billing Manager (CBM).
- When you are removing a GWC node from the CS 2000 GWC Manager database.

Prerequisites and guidelines

If the card you want to lock is currently active, you need to switch call processing to its mate card in the node. This switch places the card in standby mode. Refer to procedure “Invoke a manual protection switch (warm swact)” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

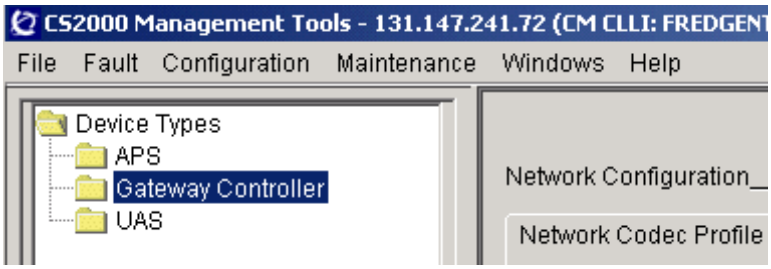
When the card is in standby mode, you need to disable (busy) services on the card. Refer to procedure “Disable (Busy) GWC card services” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

Once services on a standby card have been disabled, you can proceed with locking the card.

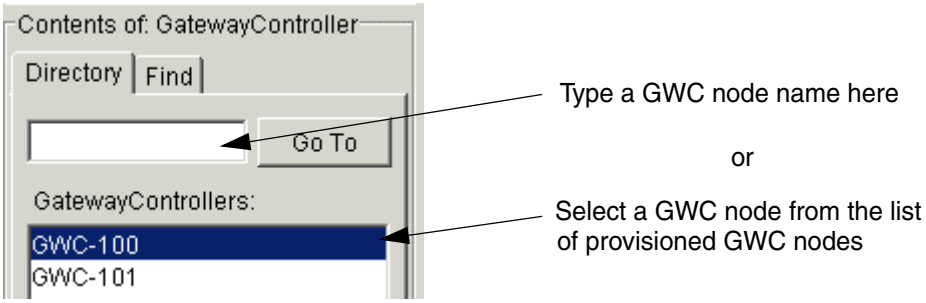
Action

At the CS 2000 GWC Manager client

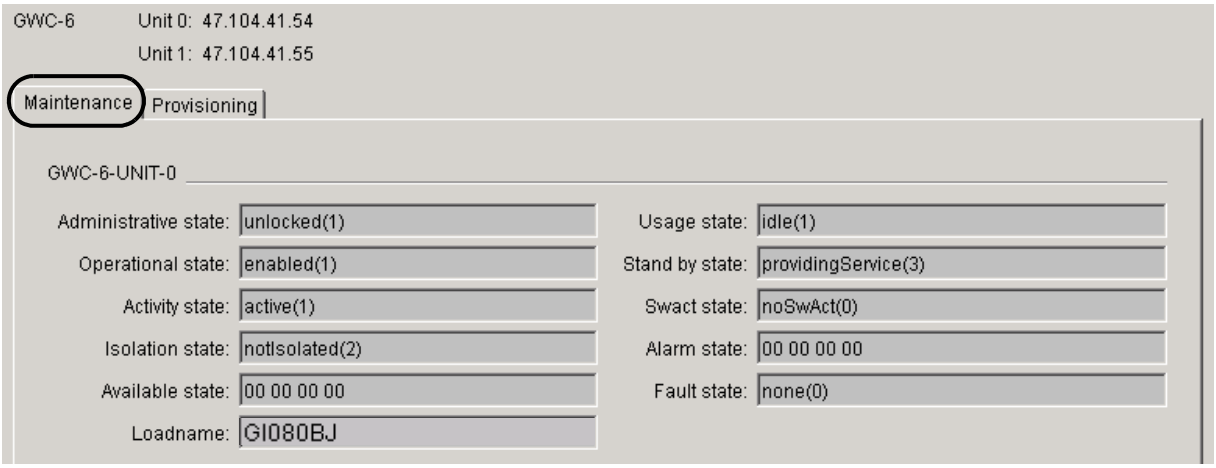
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



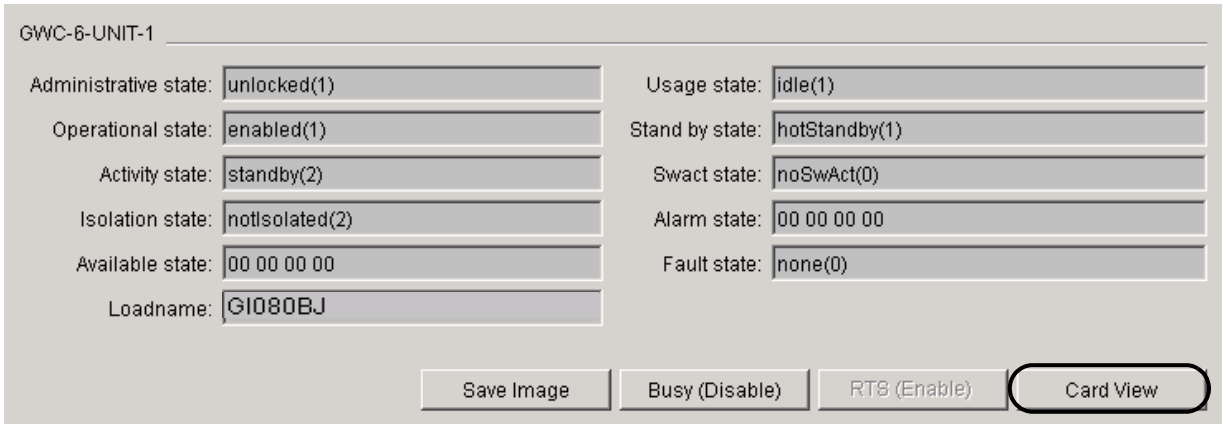
2 From the Contents of: Gateway Controller frame, select the GWC node that you want to lock.



3 Select the **Maintenance** tab to display maintenance information about the node.

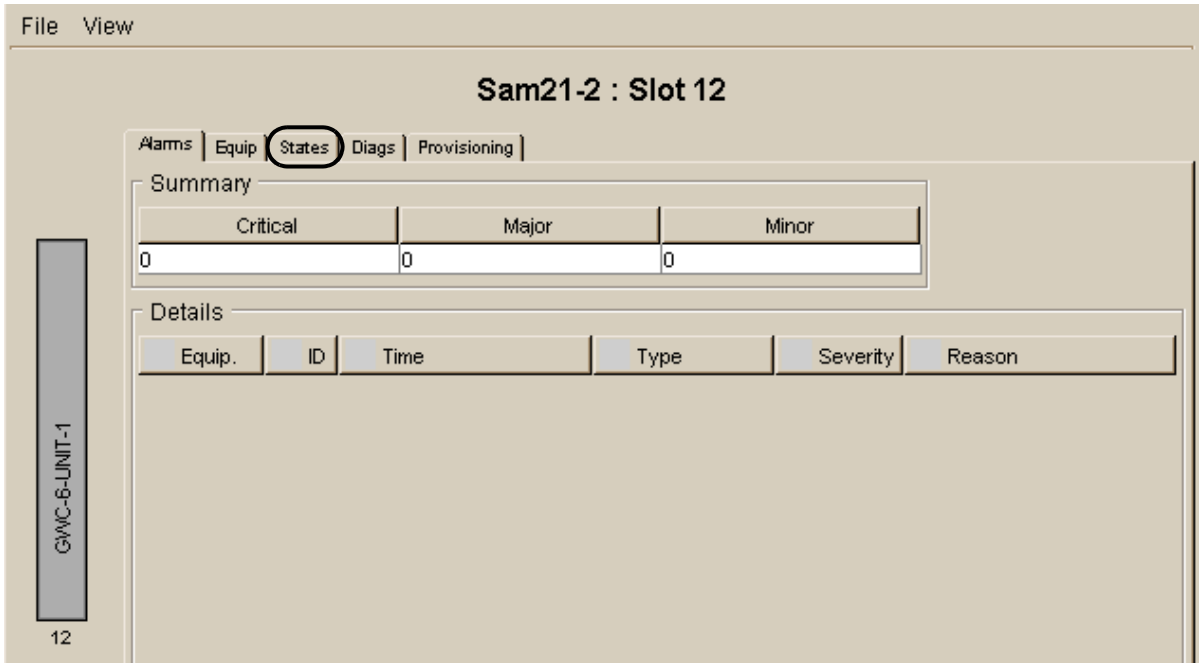


4 Click the **Card View** button for the card you want to lock. This opens the CS 2000 SAM21 Manager.

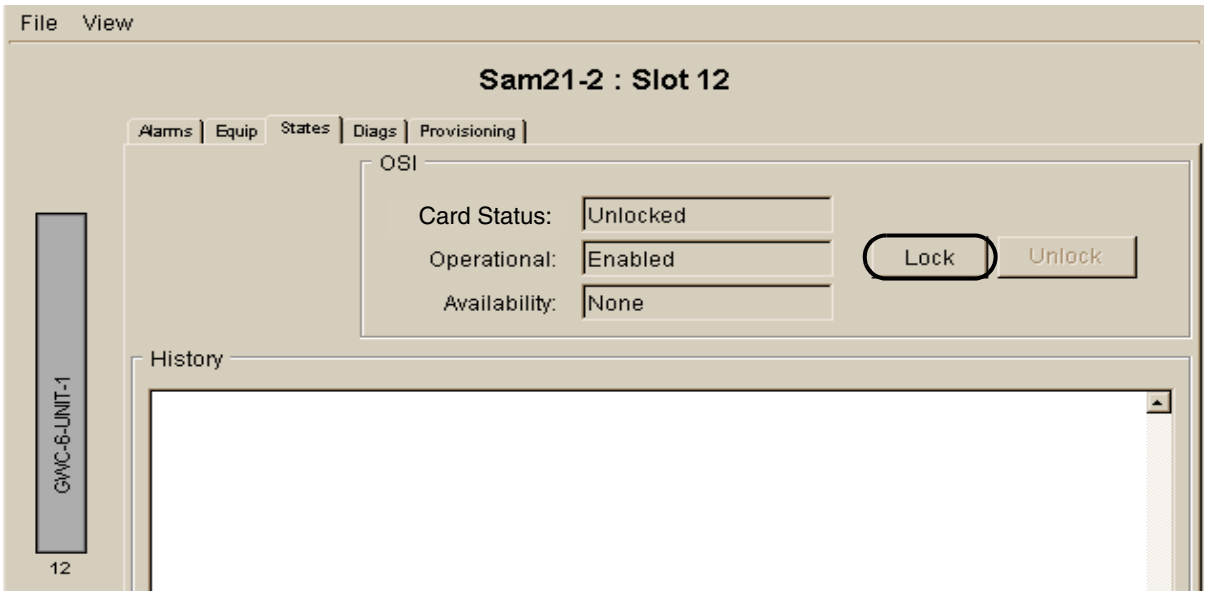


At the CS 2000 SAM21 Manager client

5 In the card view, select the **States** tab.

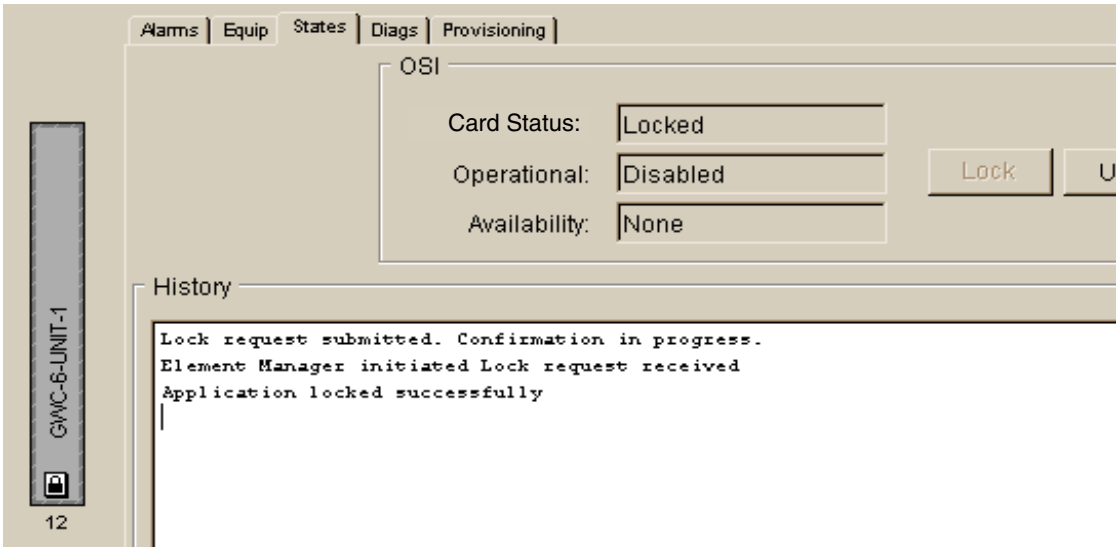


6 In the States display, click the **Lock** button to lock the card.



7 Note the system response in the History window.

The card is locked when you see the text “Application locked successfully” in the History display. The lock icon should also be present on the card graphic at the left of the screen:



8 If necessary, return to step 2 and repeat this procedure for the next GWC card in the node.

9 The procedure is complete.

Unlock a GWC card

Purpose of this procedure

Use this procedure to reboot a GWC card, forcing it to reload its software from the CS 2000 Core Manager or Core and Billing Manager (CBM).

When to use this procedure

Use this procedure in the following contexts:

- After replacing a GWC card.
- As part of a fault clearing activity.
- When a new software load is available.
- When you have completed re-provisioning of a GWC card or GWC node and you would like the card or node to begin using the new provisioning values.
- When you have applied a patch to (or removed a patch from) the GWC software using the Network Patch Manager (NPM) and have created a new GWC software image on the CS 2000 Core Manager or Core and Billing Manager (CBM).

  Note: For more information about upgrading GWC software, refer to the *Upgrading the Gateway Controller* NTP, NN10196-461.

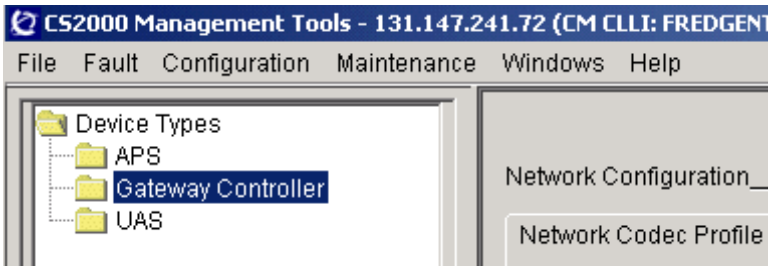
Prerequisites and guidelines

The GWC card must be locked. Refer to procedure Lock a GWC card on page 519 in this NTP to lock a GWC card.

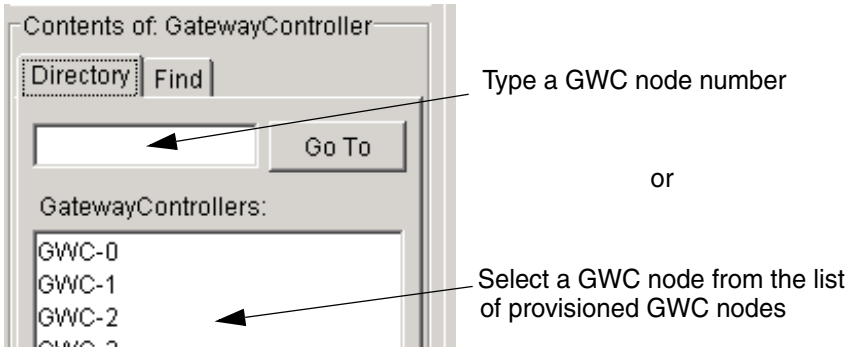
Action

At the CS 2000 GWC Manager client

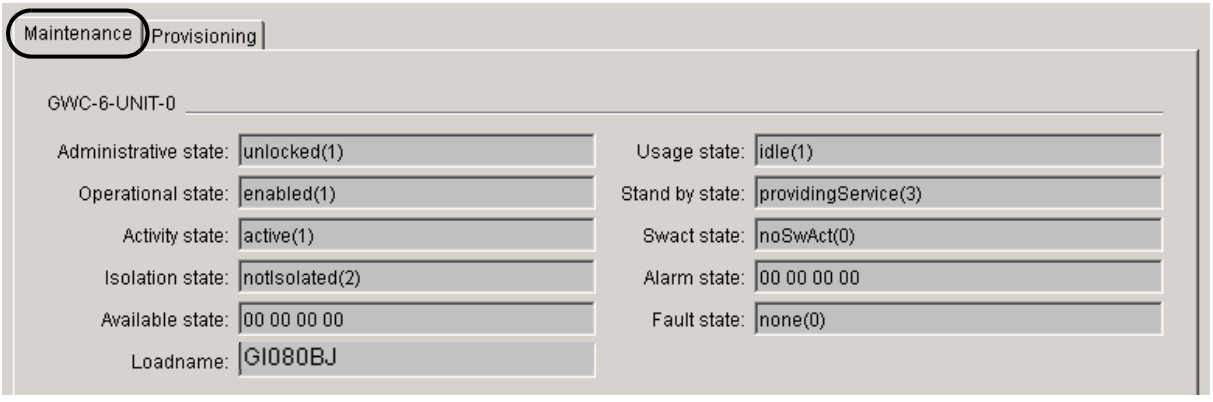
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



2 From the Contents of: Gateway Controller frame, select the GWC node that contains the card you want to unlock.

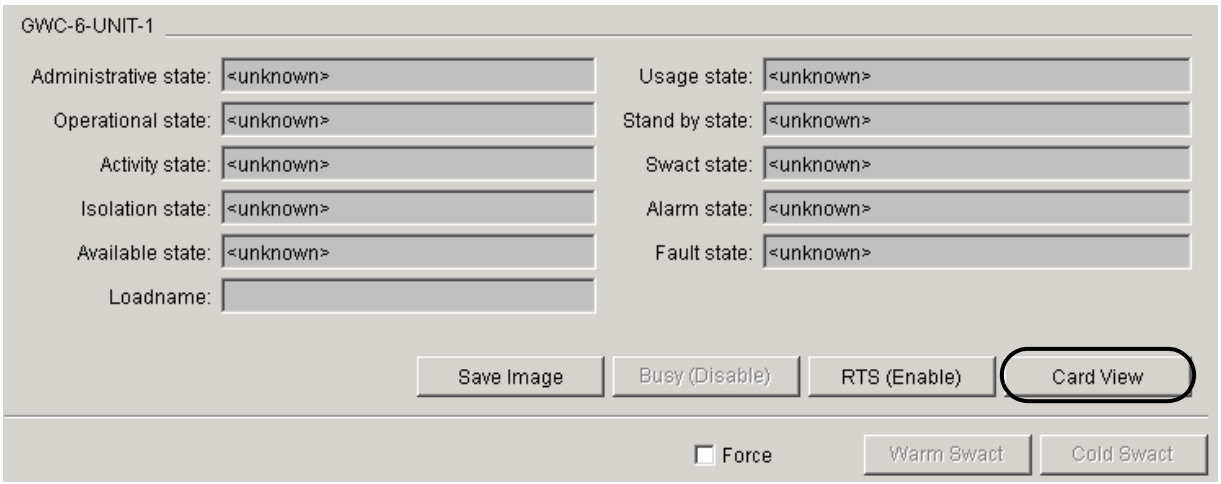


3 Select the **Maintenance** tab to display maintenance information about the node.



4 Click the **Card View** button for the card you want to unlock. This action opens the CS 2000 SAM21 Manager.

Note: If a card is currently locked, all fields display the value <unknown>.

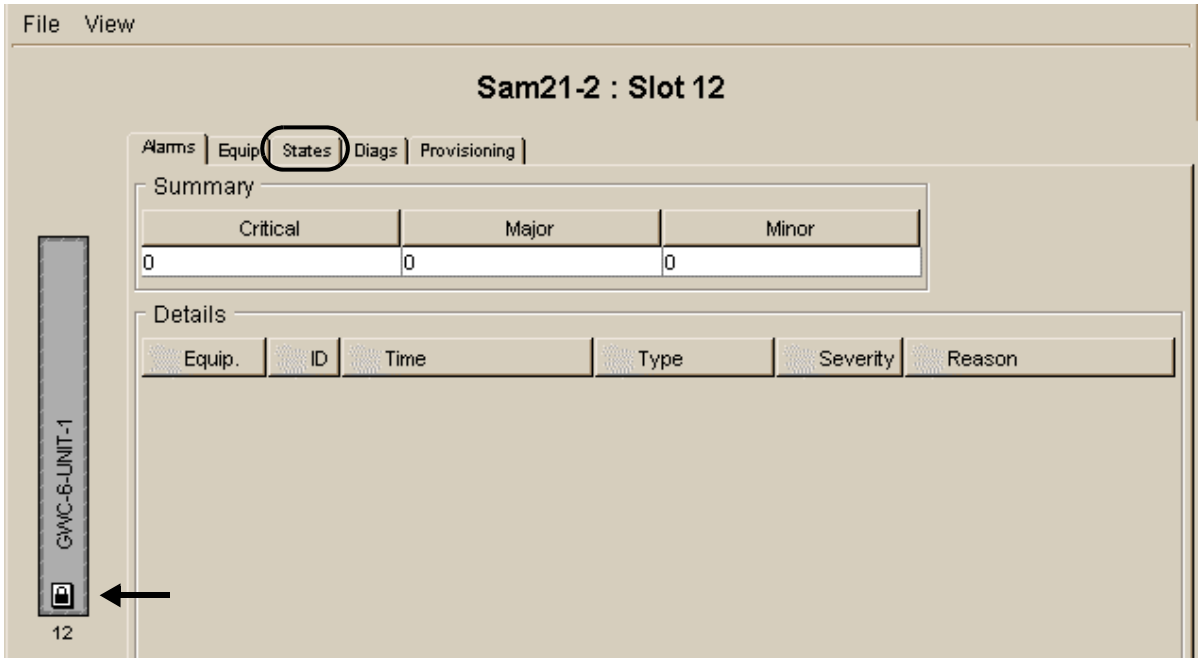


At the CS 2000 SAM21 Manager

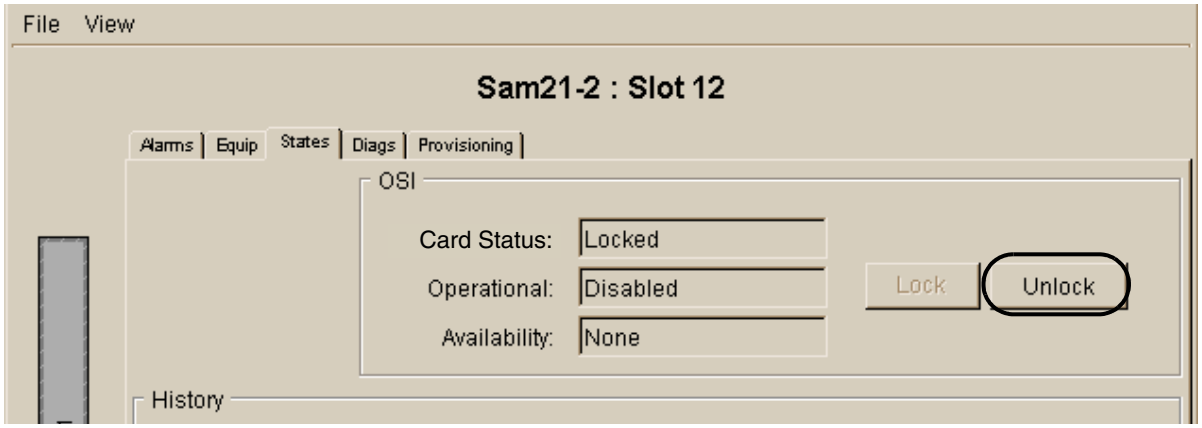
5 In the card view, select the **States** tab.

The lock icon appears at the bottom of the card diagram.

Note: If you want to display the status of all cards in the shelf, click the **View** menu and select **Shelf View**.

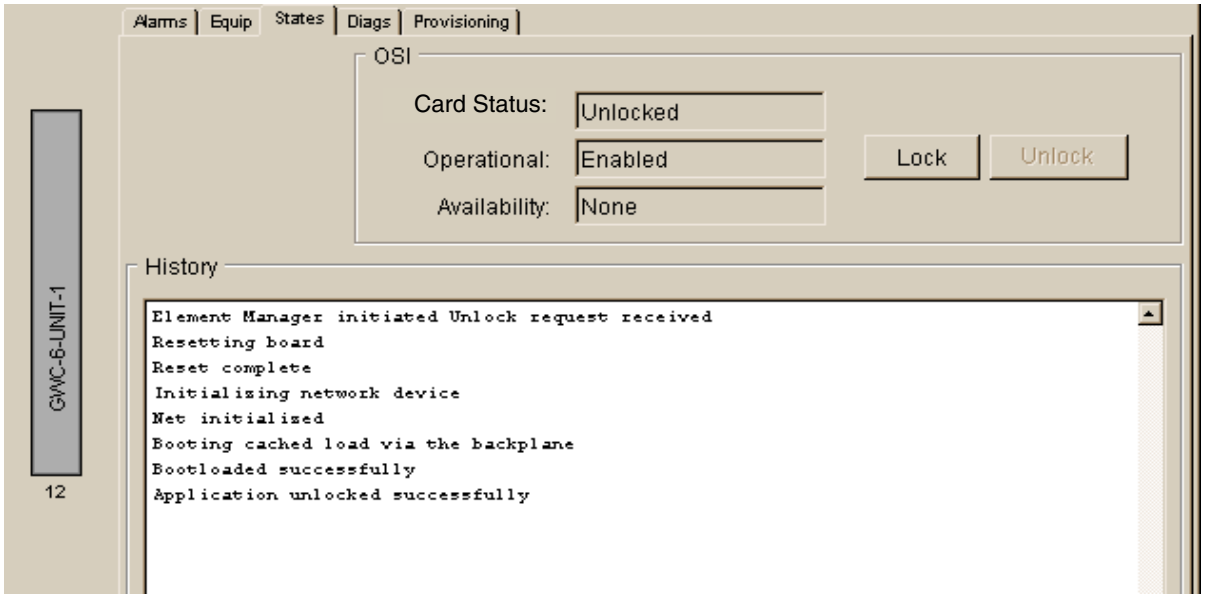


6 In the States display, click the **Unlock** button to unlock the card.



7 Note the system response in the History window.

The card is unlocked when you see the text “Application unlocked successfully”.



8 Return to step 2 and repeat this procedure for the next GWC card until all the GWC cards have been unlocked and brought into service. Remember, each GWC node has two GWC cards.

9 The procedure is complete.

Manually return a GWC node to service

Purpose of this procedure

Use this procedure to make services and resources allocated on a specific Gateway Controller (GWC) node available for call processing.

This task is commonly referred to as return to service (RTS).

When to use this procedure

Use this procedure when you wish to return to service the services associated with a specific GWC node.

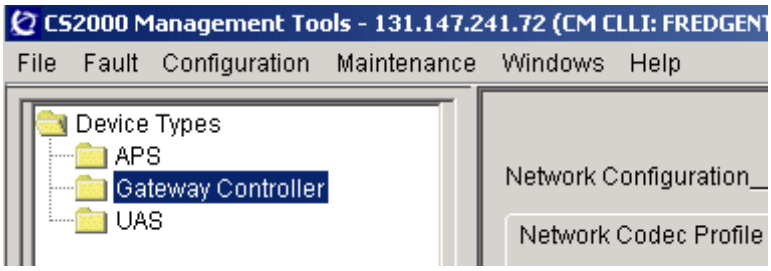
Prerequisites and guidelines

A GWC node must already be disabled (busied) before it can be returned to service. Before executing the steps in this procedure, refer to the procedure View and interpret the operational status of a GWC node on page 533 to determine if either of the GWC units in the node is disabled (busied).

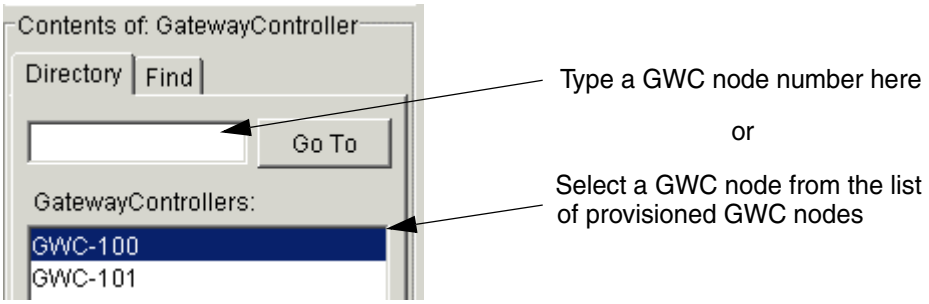
Action

At the CS 2000 GWC Manager Client

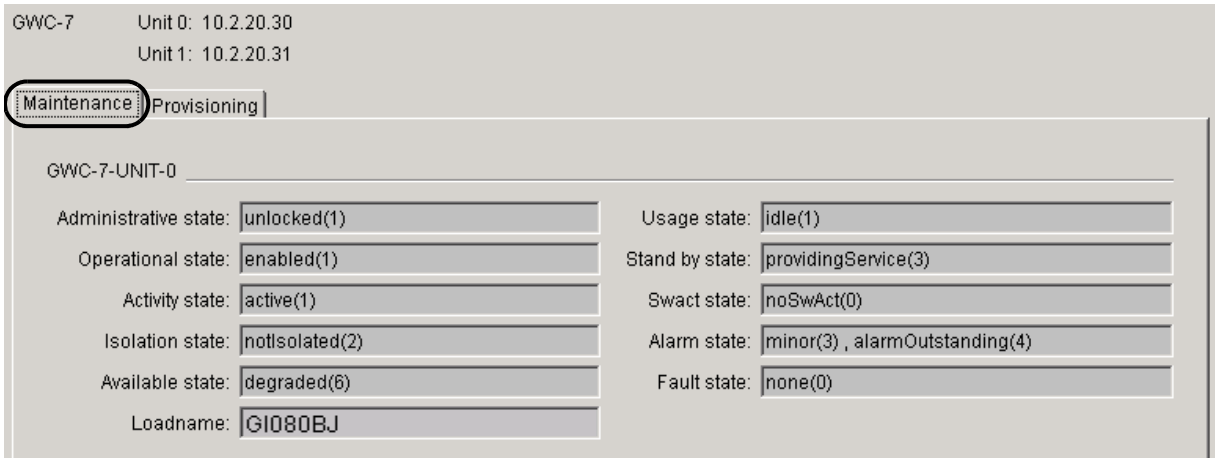
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



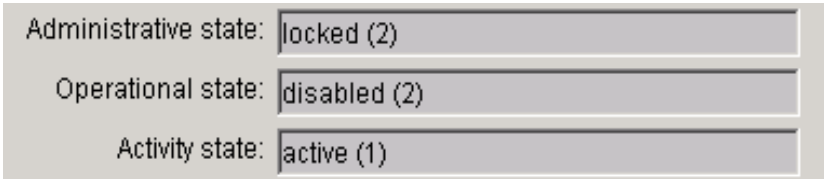
2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to return to service (RTS).



3 Select the **Maintenance** tab.

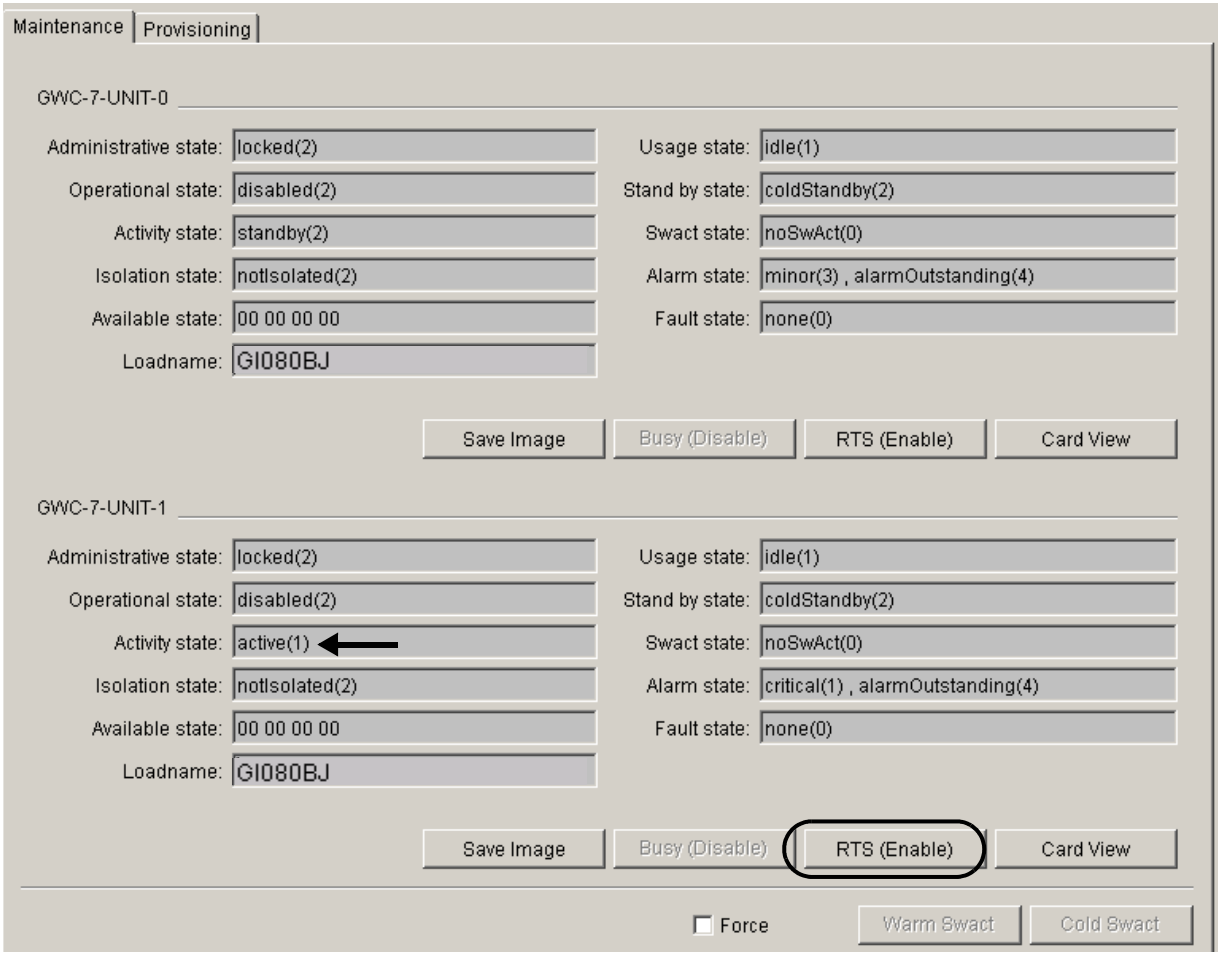


4 Use the following figure to determine whether the active GWC unit is currently disabled (busied). The figure shows the status fields for a disabled (busied) active GWC unit.

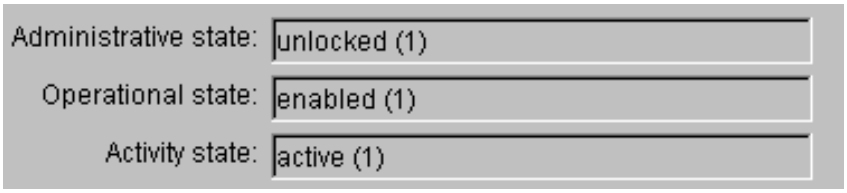


If the active unit is	Do
disabled (busied)	step 5
not disabled (busied)	step 6

5 Return the active unit to service. Click the **RTS (Enable)** button for the active unit you wish to return to service (either Unit 0 or Unit 1).



After 30 seconds, the Administrative state: field changes to unlocked and the Operational state field changes to enabled.

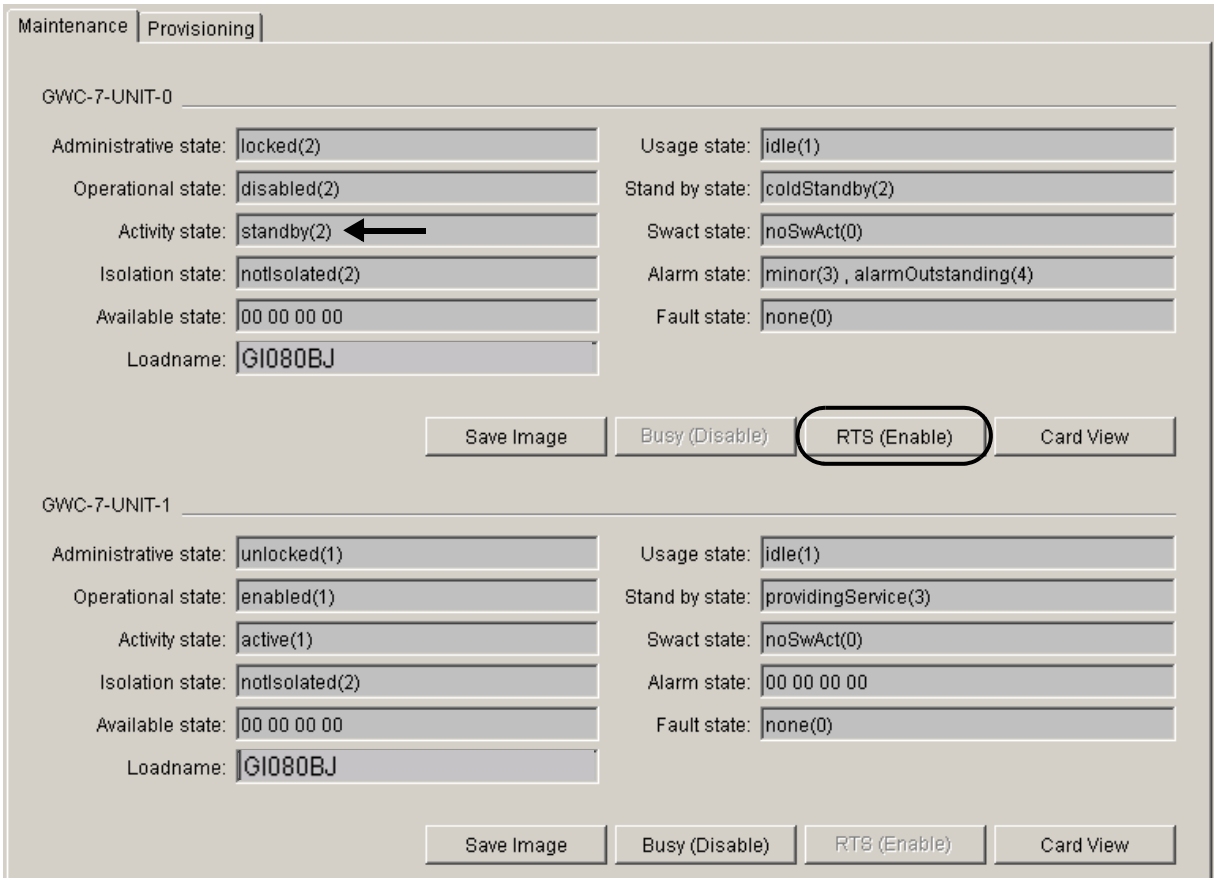


Note: In most cases, the system displays this state change automatically. However, you may need to refresh the display. If necessary, click the **Windows** menu at the top of the screen and select **Refresh GWC Status**.

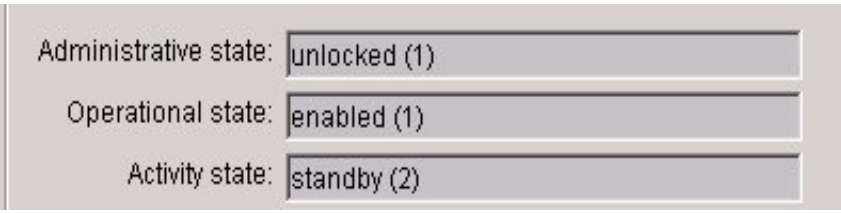
6 Determine whether the standby GWC unit is disabled (busied).

If the standby unit is	Do
disabled (busied)	go step 7
not disabled (not busied)	go step 8

7 Click the **RTS (Enable)** button for the standby unit to return the standby unit to service.



After 30 seconds, the Administrative state: field changes to unlocked and the Operational state field changes to enabled.



Note: In most cases, the system displays this state change automatically. However, you may need to refresh the display. If necessary, click the **Windows** menu at the top of the screen and select **Refresh GWC Status**.

8 Repeat this procedure for all GWC nodes you wish to return to service.

9 The procedure is complete.

View and interpret the operational status of a GWC node

Purpose of this procedure

Use this procedure to determine the operational status of a selected Gateway Controller (GWC) node using the CS 2000 GWC Manager.

Note: Refer to table CS 2000 GWC Manager status fields on page 535 to interpret the GWC cards (units) status fields.

When to use this procedure

Use this procedure as a primary source of information about the operational status of a GWC card or GWC node.

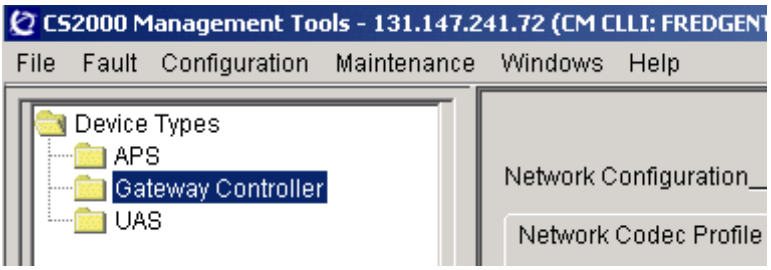
Prerequisites or guidelines

This procedure has no prerequisites or guidelines.

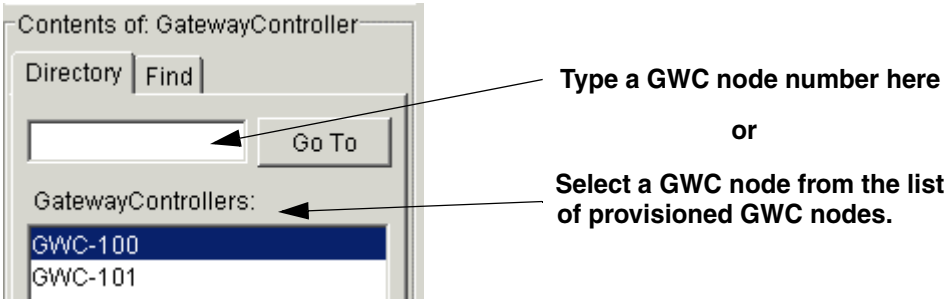
Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

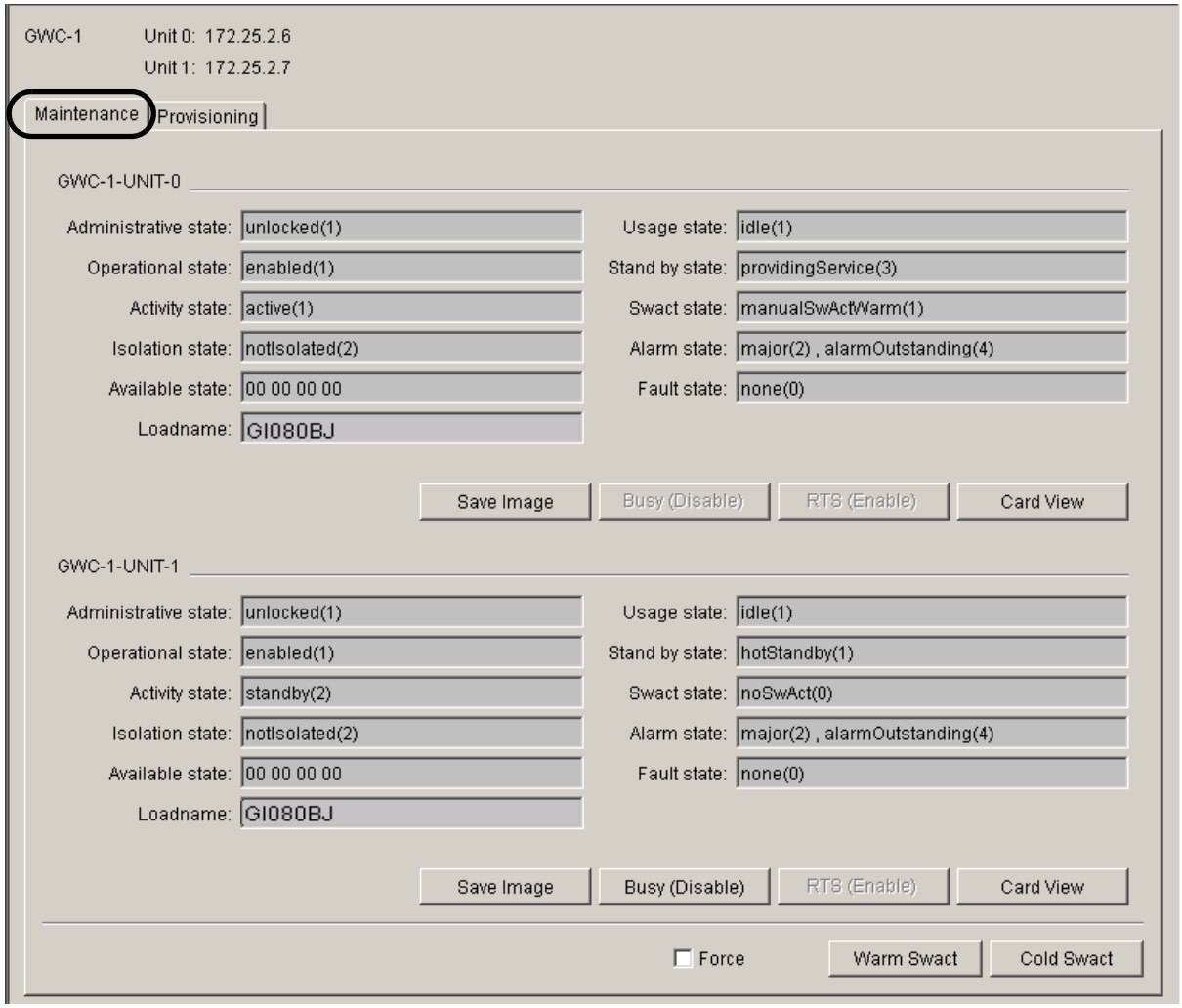


2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to view.



3 Click the **Maintenance** tab.

The GUI displays the Maintenance panel with two independent status views, one for each of the GWC cards in the node.



4 Refer to table CS 2000 GWC Manager status fields on page 535 following this procedure to interpret the GWC card (unit) status fields.

5 Repeat this procedure for other cards that you wish to view.

6 Thd procedure is complete.

The following table describes the GWC card (unit) status fields.

CS 2000 GWC Manager status fields (Sheet 1 of 4)

Status field	Possible values	Meaning
Administrative state:	locked	The unit is prohibited, administratively, from providing service to users. ***Note:*** A status of "locked" on the CS 2000 GWC Manager indicates that the software application on the card is no longer performing its primary call processing function, but the card is still running. (The call processing function has been "busied", but underlying maintenance and communications activities are still functioning.) A status of "locked" on the CS 2000 SAM21 Manager indicates that the hardware is locked to ROM level, and the software application is no longer running.
	unlocked	The unit is permitted, administratively, to provide service to users.
Operational state:	enabled	The unit is partially or fully providing service to users.
	disabled	The unit is not operating or providing service to users. If the Administrative state for this unit is "locked", then the unit has been manually busied. If the Administrative state for this unit is "unlocked", then the unit has been busied by the system.
Activity state:	active	The unit is currently providing end user services. This is the state of the node as seen by other network elements.
	standby	The unit is not providing end user services but can be switched to Active at any time if the active (mate) unit fails.
Isolation state:	isolated	The unit is not communicating with the XA-Core.
	notisolated	The unit is communicating with the XA-Core.

CS 2000 GWC Manager status fields (Sheet 2 of 4)

Status field	Possible values	Meaning
Available state:	offLine(3)	The unit has not received its configuration data from the CS 2000 GWC Manager. The unit cannot provide service until it is booted and receives configuration data.
	degraded(6)	The unit does not have heartbeat communication with its mate and it is operating without fault-tolerant redundancy.
	offLine(3), degraded(6)	The unit has both: offline and degraded conditions.
	00 00 00 00	The unit does not have either of the above conditions.
Loadname:	<string_of_ alphanumeric_ characters>	This is the name of the load file that the unit currently boots from. The file is located on the CS 2000 Core Manager or Core and Billing Manager (CBM) disk drive.
Usage state:	idle	The GWC maintenance system is not currently working on a request, such as a Return to Service (RTS). The unit is available for maintenance requests.
	busy	Maintenance is in progress on this unit and no further requests are accepted.
Stand by state:	providingService	The unit is the active unit and is providing service.
	hotStandby	The unit is the standby unit - ready to provide service.
	coldStandby	The unit is synchronizing with the active unit (not providing redundancy). After completion of synchronization, the status changes to hotStandby when the Operational state is enabled.

CS 2000 GWC Manager status fields (Sheet 3 of 4)

Status field	Possible values	Meaning
Swact state:		This field indicates the last switch of activity for the unit.
	manualSwActWarm	Last switch of activity was due to a manual warm SwAct. Requested by a user, a warm SwAct causes no service interruption to stable calls, but calls in the setup processes can be lost.
	manualSwActCold	Last switch of activity was due to a manual cold SwAct. Requested by a user, a cold SwAct temporarily takes both units out of service and takes down all calls.
	autonomousSwActWarm	Last switch of activity was due to a system warm SwAct. These SwActs are automatically performed by the device in response to faults or failures. Established calls are preserved. Calls in setup are lost.
	autonomousSwActCold	Last switch of activity was due to a system cold SwAct. These SwActs are automatically performed by the device in response to faults or failures. All calls are lost.
	noSwAct	No switch of activity has occurred.

CS 2000 GWC Manager status fields (Sheet 4 of 4)

Status field	Possible values	Meaning
Alarm state:		This field indicates the severity of the currently raised alarms.
	00 00 00 00	There are no alarms raised on the GWC card unit.
	critical(1)	If present, indicates that one or more critical alarms have been raised.
	major(2)	If present, indicates that one or more major alarms have been raised.
	minor(3)	If present, indicates that one or more minor alarms have been raised.
	alarmOutstanding(4)	If present, indicates that at least one or a combination of different alarms has been raised.
Fault state:	none(0)	This field is not used.