555-4031-904

Nortel Communication Server 2100

H.323

Service Implementation Guide

SE08 Standard 01.03 May 2005

NORTEL

Nortel Communication Server 2100

H.323

Service Implementation Guide

Publication number: 555-4031-904
Product release: SE08
Document release: Standard 01.03
Date: May 2005

Publication history

May 2005

Issue 01.03, Standard SE08. Updated after receiving internal review comments.

January 2005

Issue 01.02, Draft SE08. Updated after receiving internal review comments.

November 2004

Issue 01.01, Draft SE08. This is the first version of the document for internal review purposes.

Contents

About this document

Purpose and audience

This document describes the fundamentals behind the H.323 protocol and how to configure the protocol in a Communication Server 2100 network.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers (for example, 01.01).

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

FOR MORE INFORMATION

To determine whether you have the latest version of this document and how documentation for your product is organized, check the release information in the *Meridian SL-100 Master Index of Publications*.

References in this document

Refer to the following documents for further information relevant to the topics discussed in this document:

- *Meridian SL-100/Communication Server 2100 Product Guide*, 555-4001-806
- *Meridian SL-100/Communication Server 2100 Application Planning Guide*, 555-4001-108
- *Succession Fault Management Logs Reference*, NN10275-909
- *CS2000 Management Tools User Guide*
- *OSSGate Users Guide,* NE10004512
- *Succession Server Platform Foundation Software Security Installation Manual*
- *Operational Measurements Reference Manual,* 555-4031-814

Communication Server 2100 H.323 architecture

The Communication Server 2100 H.323 solution provides Virtual Private Network (VPN) connectivity for multiple enterprises and sites including the following capabilities:

- H.323 connectivity
- VPN services
- translations
- Meridian SL-100 enterprise features
- inter-operability with third-party H.323 gateways

What is H.323?

H.323 is an ITU-defined umbrella specification for use in the definition and implementation of multimedia services supporting the integration of voice, video and data applications. It should be regarded as a framework, or architecture, rather than a protocol in its own right, because it actually comprises a number of different protocols.

The underlying control protocol in the H.323 architecture is H.225, which provides essentially the same range of call control messages as those defined in Q.931. More importantly, H.225 allows other types of H.323 signaling to be conveyed in order to support enhanced capabilities such as the following:

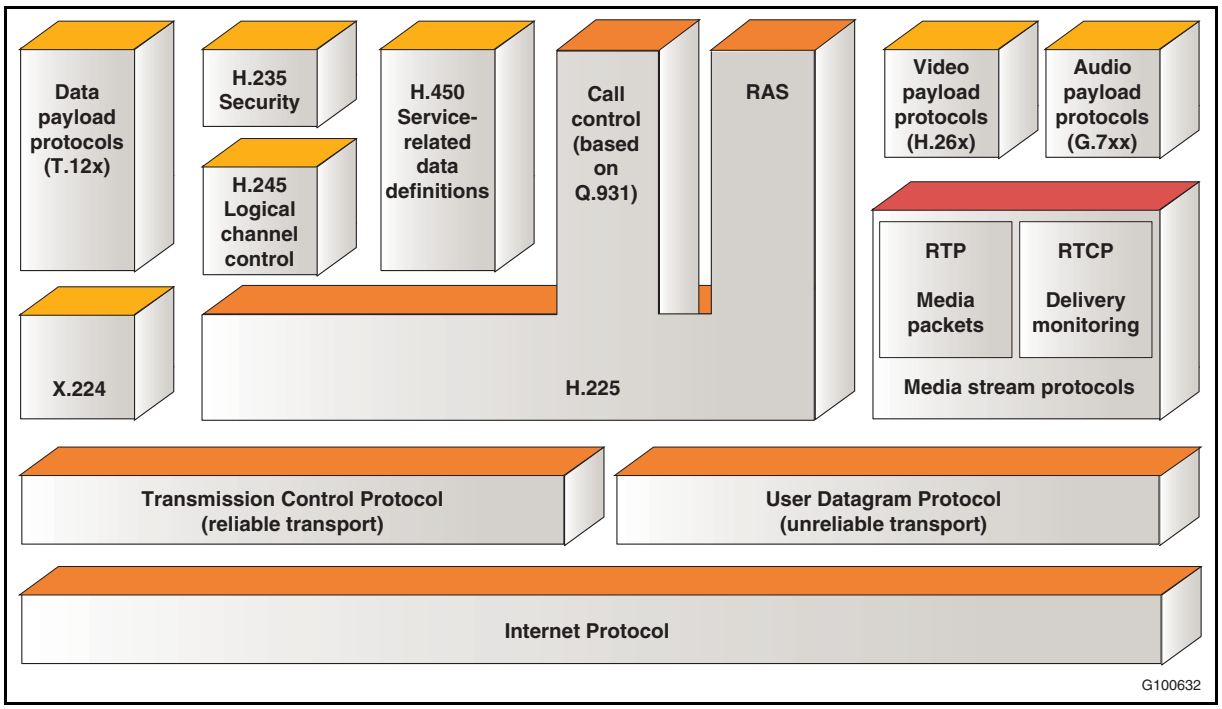
- H.225 defines Registration, Admission and Status (RAS) messages and procedures for controlling access to the network. These allow H.323 endpoints to discover and register with an H.323 gatekeeper, to provide information about their capabilities, and to request the allocation of amounts of bandwidth.

- H.450 protocols provide service-related data definitions in Abstract Syntax Notation 1 (ASN.1) format. H.450.1 defines a general purpose signaling protocol that provides a common basis for the definition of H.323 supplementary services. It is derived from the generic functional protocol specified in ISO/IEC 11582 and includes a mechanism for defining manufacturer-specific protocol extensions that can be used to support proprietary services. H.450.2 to H.450.13 provide data definitions for use in supporting standardized supplementary services. H.450-defined data is conveyed transparently (tunnelled) over H.323 interfaces in User-to-User Information (UUI) IEs in H.225 call control messages.
- H.245 defines messages and procedures to be used in setting up and taking down logical channels within the context of an H.225 call (for example, an additional video or data channel for the exchange of information). It allows endpoints to determine their network-side/user-side roles, to exchange information about their transmit and receive capabilities, and to open and close end-to-end logical channels with characteristics appropriate for the information being exchanged. Like H.450-defined data, H.245 signaling is tunnelled over H.323 in UUI IEs in H.225 call control messages.
- H.235 is used in conjunction with H.245 and allows security characteristics such as encryption to be associated with logical channels.

Audio streams are encoded using protocols such as G.711 and G.729. Video streams are encoded using H.261 and H.263. Audio and video payloads are both conveyed using Real-time Protocol (RTP) over User Datagram Protocol (UDP) transport, with Real-time Control Protocol (RTCP) being used for status and delivery monitoring. Data is encoded using T.12x protocols and conveyed using X.224 over Transmission Control Protocol (TCP) transport.

Figure 1 on page 13 provides a simplified view of the H.323 architecture.

Figure 1
H.323 protocol architecture



Communication Server 2100 H.323 capabilities

The Communication Server 2100 supports H.323 Version 4. Compliance with Version 4 of H.323 implies compliance with all the mandatory requirements of ITU Recommendation H.323 (2000), which references ITU-T Rec. H.225.0 (2000) and H.245 (2000 or later). Version 4 products are identified by H.225.0 messages containing a protocolIdentifier = {itu-t (0) recommendation (0) h (8) 2250 version (0) 4} and H.245 messages containing a protocolIdentifier = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, where “x” is 7 or higher.

The Communication Server 2100 H.323 solution provides Virtual Private Network (VPN) connectivity for multiple enterprises and sites including: H.323 connectivity, VPN services, translations, traditional Meridian SL-100 features and inter operability with third-party H.323 gateways.

Note: H.323 can be implemented on both Communication Server XA-Core and Communication Server Compact systems.

Basic H.323 capabilities supported by the Communication Server 2100 include the following:

- H.225 Registration, Admission and Status
- H.225 fast start and slow start
- End-to-end H.245 supporting using tunneling
- Gatekeeper-routed signaling
- G.711 a-law/μ-law (with PLC), G.729a
- Codec negotiation
- In-band Dual-tone Multifrequency (DTMF) support using RFC 2833
- DTMF out-of-band support (H.245 to in-band)

Carrier-hosted services

In this configuration, the Communication Server 2100 core and H.323 Gateway Controllers provides gatekeeper functionality in an H.323 network. Operating as a gatekeeper enables the Communication Server 2100 to provide carrier-hosted services to gateways and other gatekeepers in an enterprise network. H.323 gateways view the Communication Server 2100 as their gatekeeper and use gatekeeper-routed H.323 signaling to interact with other H.323 gateways, and other line and trunk gateways that are controlled by the Communication Server 2100 (for example, a Packet Voice Gateway such as the Nortel Multiservice Gateway 7480).

To enable carrier-hosted services at the enterprise, each node must provision a group and dialing plan on the Communication Server 2100. As H.323 call control signaling is received from the H.323 gateways, an H.323 Gateway Controller maps the messages to Primary Rate Interface (PRI) Q.931 and forwards them to the Communication Server 2100 core for processing. The Communication Server 2100 core uses existing PRI Q.931 call processing capabilities to translate and route the call. The call can terminate to any one of the following entities:

- Another H.323 gateway, reached over the PRI trunk group with which it is associated.
- A PRI TDM trunk hosted from a Packet Voice Gateway.
- A line hosted by an IP Client Manager (IPCM).
- A line hosted by a Mediatrix Analog Station Gateway.

Note: For more detailed information about H.323 signaling, see "H.323 message characteristics" on page 23.

The Communication Server 2100 Gateway Controller (GWC) H.323 stack supports the following three call models:

- **H.323 Fast Start**
  In this call model, the media information (that is, H.245 information) of the H.323 endpoint is received in the H.225 SETUP message.
- **H.323 Slow Start (Early Media)**
  In this call model, H.225 and H.245 procedures occur in parallel.
- **H.323 Slow Start (Delayed Media)**
  In this call model, the H.225 procedure takes place first, followed by the H.245 procedure.

For an H.323 PRI – H.323 PRI call, the network/user side determination is performed according to the following criteria:

1. If the incoming H.323 is fast start, the system assigns it as the user side.
2. If the incoming H.323 is slow start, the system assigns it as the network side.

A PRI trunk can operate as network side, as well as user side. During call setup the Computing Module (CM) randomly assigns it as network or user side. H.323 PRI operation modifies this operation.

The Computing Module assigns H.323 PRI as network side in the following scenarios:

- H.323 PRI (slow start) – TDM trunk call
- H.323 PRI (slow start) – line call
- H.323 PRI (slow start) – SIP-T call
- TDM trunk – H.323 (slow start/fast start) call
- Line – H.323 PRI (slow start/fast start) call

The Computing Module assigns H.323 PRI as user side in the following scenarios:

- H.323 PRI (fast start) – TDM trunk call
- H.323 PRI (fast start) – line call

Benefits of H.323

Large enterprises can reap the following benefits from implementing H.323 on the Communication Server 2100:

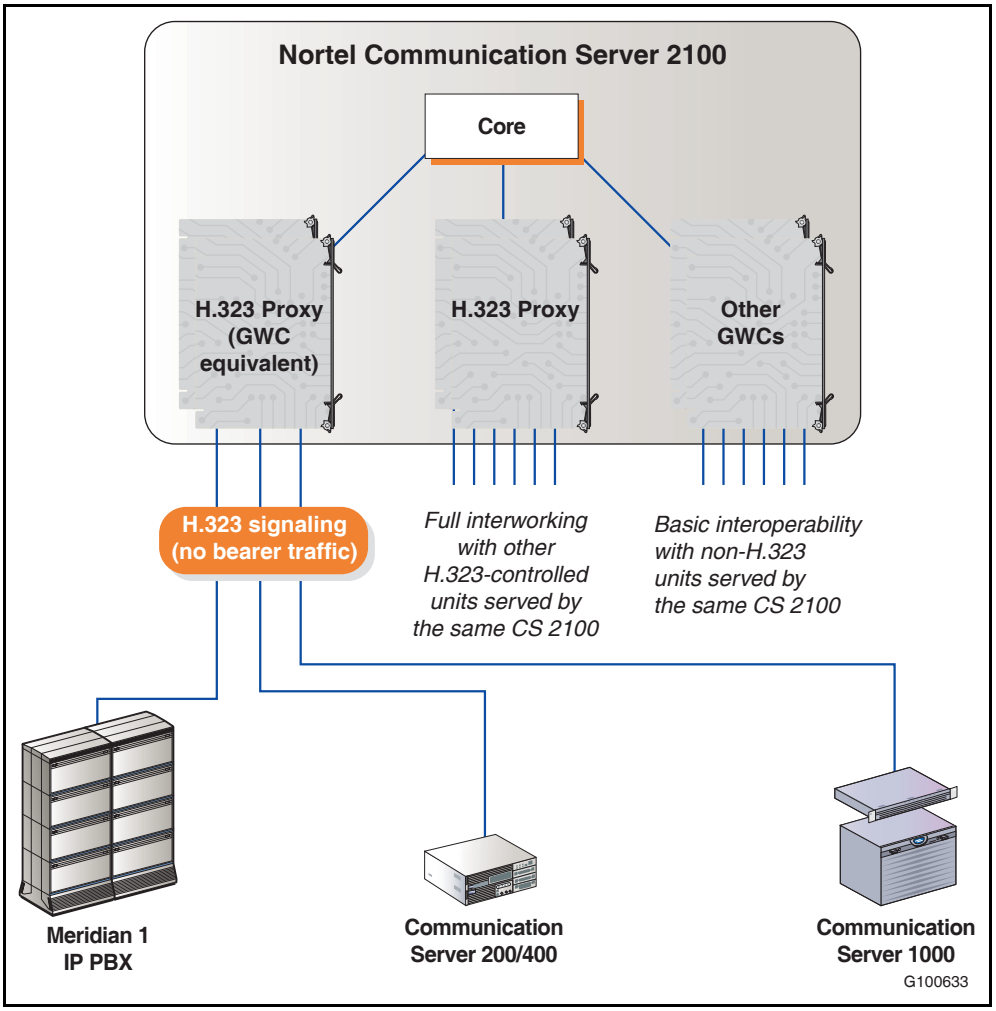
- Cost savings through converged access and long distance bypass
- Operational savings through the following:
  - simplified management of individuals or sites within a VPN
  - TDM and virtual mesh removal
  - better utilization of LAN/WAN facilities

Network role

External H.323 interfaces

The Communication Server 2100 supports a wide variety of units using H.323. These units are typically deployed on customer premises in support of enterprise networks that support both voice and data applications. Figure 2 illustrates Communication Server 2100 support for Customer Premises Equipment (CPE) units through H.323.

Figure 2
The role of H.323 in a Communication Server 2100 network



H.323 interoperability and tunneling

The Communication Server 2100 does not support an H.323 call processing agent. Instead, H.323 support is provided primarily by the H.323 proxy, which is a twin-card Gateway Controller unit that has been configured for H.323. The main H.323 functions provided by the H.323 proxy are as follows:

Note: Features supported by the various Call Servers can differ. Check current documentation and engineering rules to understand what is, and what is not, supported.

- **Support for H.225 Registration, Administration and Status**

  H.225 defines RAS messages and procedures for controlling access to the network. These enable H.323 endpoints to discover and register with an H.323 gatekeeper, to provide information about their capabilities, and to request the allocation of appropriate amounts of bandwidth.

  RAS signaling is handled entirely by the H.323 proxy. Registration is controlled by the state of the D-channel in the Communication Server 2100 core.

- **Support for H.225 call control**

  H.225 call control signaling makes use of essentially the same range of messages as Q.931 (for example, SETUP, ALERTING, CONNECT).

  The H.323 proxy terminates H.225 call control signaling and maps incoming H.225 call control messages on their PRI equivalents to be conveyed to the Communication Server 2100 core for call processing.

- **Support for H.323 tunneling (feature transparency)**

  Feature transparency involves the end-to-end tunneling of H.323 information, such as H.450 service-related data and H.245 logical channel control messaging. Services can thus be supported between H.323 endpoints even if the intermediate nodes between those endpoints cannot understand the H.323 data being conveyed, provided that they are capable of relaying it.

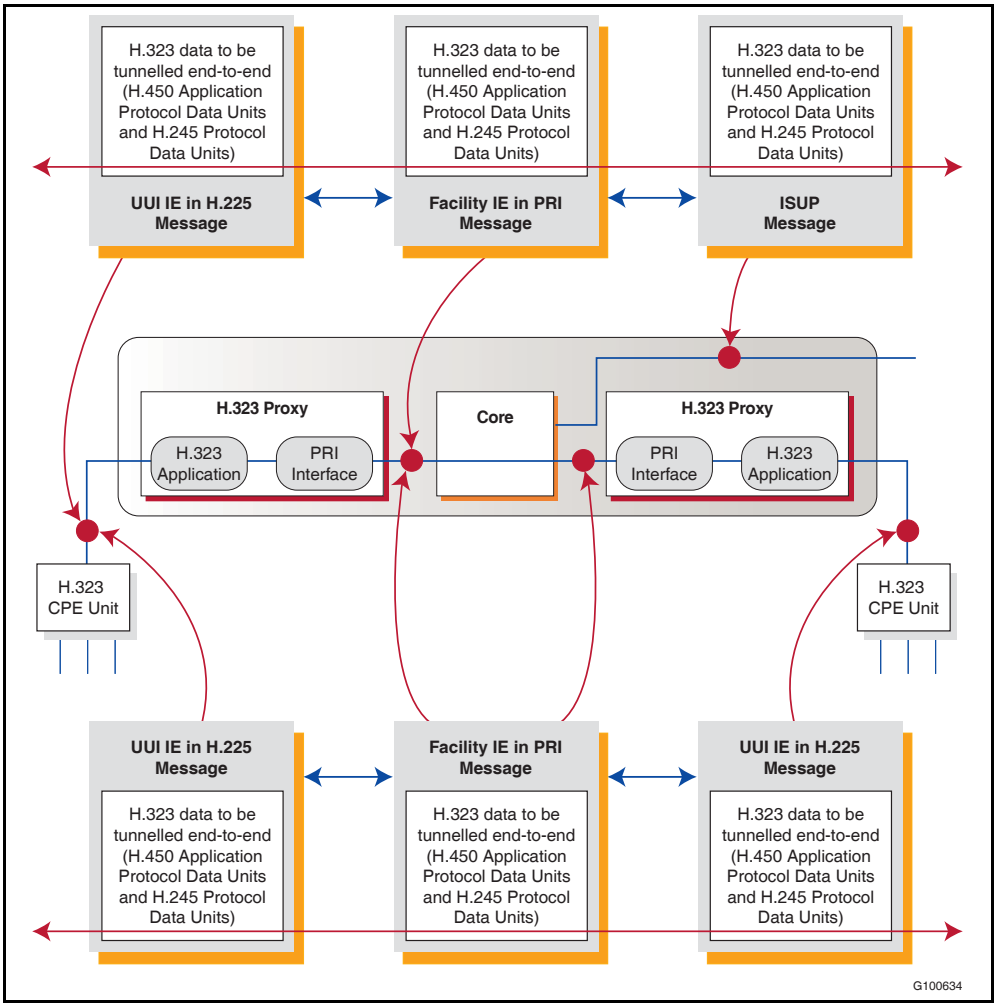
Information to be tunnelled is conveyed from an H.323 endpoint to the H.323 proxy in a User-to-User Information IE in an H.225 call control message. The H.323 proxy then encapsulates the content of the UUI IE in a Facility IE in a corresponding PRI call control message to be relayed to its destination.

Between two H.323 endpoints served by the same Communication Server 2100, the Facility IE with the tunnelled information is conveyed from the PRI interface serving the originating H.323 proxy to the PRI interface serving the terminating H.323 proxy.

Between two endpoints served by different Communication Server 2100s, the mechanism used to convey tunnelled H.323 information is PRI Feature Transparency. Feature Transparency uses the Integrated Services Digital Network User Part (ISUP) Application Transport Mechanism (APM) to encapsulate and convey any service-related PRI signaling that cannot be directly interworked to ISUP. This enables services to be supported end-to-end even if the corresponding signaling has to be routed over nodes that do not support PRI functionality. Feature Transparency across a packet backbone network involves two levels of encapsulation. First PRI signaling is encapsulated in ISUP and then ISUP is encapsulated in SIP-T.

Figure 3 on page 20 illustrates the message mapping involved in H.323 tunneling for intra-Communication Server calls and inter-Communication Calls using Feature Transparency.

Figure 3
Message mapping for H.323 tunneling



H.323 feature interactions operate in a similar manner to NTNA PRI. The following features operate transparently between H.323 nodes in a Communication Server 2100 network:

- Calling Name Delivery
- Calling Number Delivery
- Calling Name Delivery Blocking
- Calling Number Delivery Blocking
- Network Message Service
- Release Line Trunk
- DTMF Passing
- Call Transfer Blind

- Call Transfer Normal
- Called Party Busy
- Call Forwarding No Reply
- Call Forwarding Busy
- Call Forwarding Universal
- Ring Again No Answer
- Ring Again Busy

In addition, the H.323 configuration supports Private Numbering Plans.

Impacted components

The H.323 provisioning activity adds functionality to support H.323 node additions to four main components: the Communication Server 2000 Management Tools Graphical User Interface (GUI), OSSGate, the Node Provisioning application, and the Gateway Controller Element Manager (GWC EM). Modifications have also been made to the Service Broker, Network View, and Gateway Controller software to support the additional Gateway Controller and gateway profiles that the H.323 feature introduces.

In summary, the H.323 feature impacts the following components:

- Communication Server 2000 Management Tools
- OSSGate XML interface
- Node Provisioning application
- Gateway Controller Element Manager
- Service Broker
- Network View
- Gateway Controller

External interfacing systems

An H.323-enabled Communication Server 2100 can interface to any H.323-enabled media gateway. Supported Nortel gateways include the following:

- Communication Server 500
- Communication Server 1000
- Survivable Remote Gateway
- Nortel Media Gateway 3200 and the Nortel Media Gateway 3500

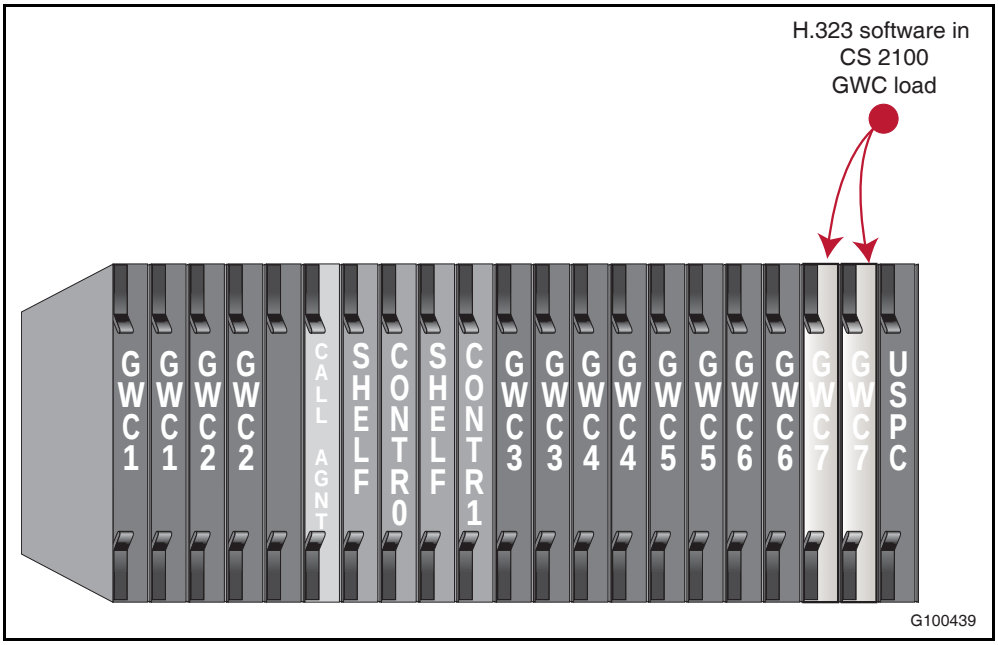
Communication Server 2100 hardware

H.323 implementation requires the following Communication Server 2100 hardware components:

- SAM21 shelf
  - — Motorola CPX8221 CPCI shelf
  - — 17 I/O slots and two system slots per shelf
- H.323 application integrated into Communication Server 2100 software load has the following characteristics:
  - — Runs on a pair of Motorola MCPN750 cards (1+1 redundancy)
  - — The number of Gateway Controller cards are engineered according to H.323 traffic requirements.

Figure 4 shows a sample Communication Server 2100 H.323 shelf configuration.

Figure 4
H.323 card configuration in SAM21 shelf



H.323 message characteristics

This chapter provides further information about the H.323 protocols introduced in “Communication Server 2100 H.323 architecture” on page 11, including descriptions of message formats and details of how specific protocol capabilities are supported on the Communication Server 2100.

H.225 protocol

TheH.225 protocol specification defines the following two different types of signaling:

- H.225 RAS signaling, which enables H.323 endpoints to register with an H.323 gatekeeper and request the allocation of appropriate amounts of bandwidth. Successful completion of RAS registration is a prerequisite for the use of H.225 call control signaling.
- H.225 call control signaling, which makes use of essentially the same range of messages as Q.931.

H.225 RAS signaling

Registration, Admission and Status (RAS) is an essential prerequisite for the setting up of an H.323 call using H.225 call control signaling. The RAS channel is used to convey messages used in the gatekeeper discovery and endpoint registration process.

Gatekeeper discovery is the process whereby an H.323 endpoint determines the gatekeeper with which is should be registered. The process can be manual or automatic.

With manual gatekeeper discovery, the endpoint is configured with the transport address of its gatekeeper through datafill or an initialization file, in which case the discovery process involves no RAS messaging and is outside the scope of H.323.

With automatic gatekeeper discovery, the endpoint initiates the process by sending a Gatekeeper Request (GRQ) message asking, “who is my gatekeeper?” to the well-known Gatekeeper Discovery Multicast Address. One or more gatekeepers then respond with a Gatekeeper Confirmation (GCF) message containing the transport address of the gatekeeper’s RAS channel.

Note: An H.323 unit supporting multiple endpoints must send a separate GRQ for each one.

In the Communication Server 2100 implementation, H.323 gatekeeper functionality is provided by the H.323 proxy Gateway Controller.

Because RAS messages are transmitted on an unreliable channel (H.225 RAS over UDP), the system uses time-outs and retry counts. An endpoint or gatekeeper that cannot respond to a request within the specified timeout can use the Request in Progress (RIP) message to indicate that it is still processing the request. An endpoint or gatekeeper receiving a RIP message can then reset its timeout timer and retry counter.

The information provided in GRQ and GCF messages is as follows:

- GatekeeperRequest (GRQ) message content
  - **rasAddress**
    The transport address of the originating H.323 endpoint.
  - **endpointType**
    Defines the capabilities of the originating endpoint, in particular:
    - The **supportedtunnelledProtocols** field contains a prioritized list of the tunnelled protocols that the endpoint can support, together with the data rates supported for each protocol the device supports.
    - The **callCapacity** field indicates the endpoint’s maximum capacity and currently available capacity for different types of call.
  - **gatekeeperIdentifier**
    Identifies the gatekeeper with which the endpoint wishes to register (a missing or null string indicates that any available gatekeeper is acceptable)

— **authenticationCapability**
Indicates the authentication mechanisms supported by the endpoint.

- GatekeeperConfirm (GCF) message content
  — **rasAddress**
  The transport address of the H.323 gatekeeper
  — **authenticationMode**
  Indicates the authentication mechanism to be used (one of those supported by the endpoint)

When an H.323 endpoint has discovered the transport address of the gatekeeper with which it should be registered, it can proceed to register itself with the gatekeeper and request admission to the backbone packet network. Table 1 lists and briefly describes the H.225 RAS messages used for these and other purposes.

Table 1
Important RAS messages

Message	Function
RegistrationRequest (RRQ)	Request from a terminal or gateway to register with a gatekeeper. The gatekeeper either confirms or rejects (RCF or RRJ).
AdmissionRequest (ARQ)	Request for access to the packet network from a terminal to a gatekeeper. Request can include indication of the specific protocol to be tunnelled. The gatekeeper either confirms or rejects (ACF or ARJ).
BandwidthRequest (BRQ)	Request for changed bandwidth allocation, from a terminal to a gatekeeper. The gatekeeper either confirms or rejects (BCF or BRJ).
DisengageRequest (DRQ)	If sent from an endpoint to a gatekeeper, DRQ informs the gatekeeper that the endpoint is being dropped. If sent from the gatekeeper to the endpoint, DRQ forces the call to be dropped.
InfoRequest (IRQ)	Request for status information from the gatekeeper to the terminal.
InfoRequestResponse (IRR)	Response to IRQ. Can be sent unsolicited by a terminal to a gatekeeper at predetermined times.
RAS timers and Request in Progress (RIP)	Recommended default time-out values for response to RAS messages and subsequently retry counts if response is not received.

H.225 call control signaling

H.225 call control signaling is based on Q.931. It uses a subset of Q.931 message types, all of which can include UUI IEs conveying encapsulated H.450 or H.245 signaling.

With the Communication Server 2100 implementation of H.323, the H.323 proxy Gateway Controller performs message mapping between H.225 call control messages and equivalent PRI messages. For H.323 tunneling, this message mapping involves converting H.225 IEs conveying encapsulated H.450 and H.245 signaling into PRI Facility IEs conveying the same encapsulated signaling unmodified.

Each H.323 entity must have at least one network address that uniquely identifies the H.323 entity on the network. An endpoint can use different network addresses for different channels within the same call. For each network address, each H.323 entity can have several Transport Service Access Point (TSAP) identifiers. These allow multiplexing of several channels sharing the same network address.

An endpoint can tunnel a signaling protocol by including the tunnelledSignalingMessage in a UUI IE in any H.225 call signaling messages that are not of end-to-end significance, such as CALL PROCEEDING, since the information may not be received by the far end.

If an originating endpoint wishes call setup to proceed only if tunneling is supported, it should set the tunnelingRequired flag in the SETUP Message. If an endpoint receives a tunnelledSignalingMessage within the SETUP message and is not able to tunnel the protocol, it terminates the call by sending a RELEASE COMPLETE message.

The tunnelled protocol information is included in the messageContent field and the tunnelledProtocolID field identifies the protocol being tunnelled.

H.225 can be used to establish a call-independent signaling connection between H.323 endpoints. Tunneling can be used in this case to provide bearer-independent signaling for the tunnelled protocol. No H.245 control channel and no media channels are required.

H.323 tunneling using H.225 User-to-User Information IEs

User information to be exchanged between H.323 endpoints is conveyed in the User-to-User Information IE in appropriate call control messages. This User-to-User IE is based on the Q.931 definition of the User-to-User IE, but incorporates some modifications and enhancements that are specific to H.323.

Actual user-to-user information to be exchanged only between the involved terminals is nested in the user-data field of the of the H323-UserInformation Protocol Data Unit (PDU). This is an Abstract Syntax Notation 1 (ASN.1) structure that includes H.323 information, as well as user data. The ASN.1 is encoded using the aligned variant of the packed encoding rules as specified in ITU-T X.691.

The most important fields in the H323-UserInformation structure are as follows:

- The **h323-uu-pdu** field of the H323-UserInformation structure contains the following fields (note that not all fields are permitted in every H.225 message):
  - **h323-message-body**
    This field contains information specific to a particular Q.931 message.
  - **h4501SupplementaryService**
    This field carries a sequence of H4501SupplementaryService Application Protocol Data Units (APDUs).
  - **h245Tunneling**
    This element is set to TRUE if tunneling of H.245 messages is enabled. Systems compliant with H.225.0 version 4 or higher must set this element to TRUE if the Fast Connect procedure is used to establish the call.
  - **h245Control**
    This field carries a sequence of tunnelled H.245 PDUs.
  - **callLinkage**
    The contents of this field are typically controlled by a call linkage service.

- **tunnelledSignalingMessage**
  This is a tunnelled entire signaling message in its native format to support additional end-to-end call control signaling. The tunnelledProtocolID field identifies the protocol being tunnelled. The messageContent field is a sequence of actual entire tunnelled messages in their native binary format; this allows aggregation of tunnelled messages in one H.225 message. If the tunnelingRequired field is set in the SETUP message, the call proceeds only if tunneling is supported.
- **genericData**
  This field is a list of generic elements related to features that are defined outside of the base H.225.0 specification. These parameters can be used, for example, for tunneling information transparently through H.225.0.

- The **user-data** field of the H323-UserInformation structure contains the following fields, coded as defined in Q.931:
  - **protocol-discriminator**
  - **user-information**

    Note: An H.323 User-to-USer Information IE has a two-byte length field (that is, it can be up to 65, 535 bytes long, while a PRI Facility IE has a one-byte length field and can be no more than 225 bytes long. If necessary, an H.323 User-to-User Information IE will be split and distributed between multiple PRI Facility IEs in the same PRI message.

H.450 protocols

H.450 protocols are used to exchange signaling information to control supplementary services. They provide service-related data definitions in ASN.1 format. H.450 APDUs are tunnelled between H.323 endpoints in User-to-User Information IEs in H.225 call control messages.

The H.450.a specification defines a general-purpose signaling protocol that provides a common basis for the definition of H.323 supplementary services. It is derived from the generic functional protocol specified in ISO/IEC 11582 and used by PRI and includes a mechanism for defining manufacturer-specific protocol extensions that can be used to support proprietary services.

Table 2 lists the H.450.2 to H.450.13 variants that provide data definitions for use in supporting specific standardized supplementary services.

Table 2
H.450 Supplementary Services data definitions

H.450 variant	Supplementary Service
H.450.2	Call Transfer
H.450.3	Call Diversion
H.450.4	Call Hold
H.450.5	Call Park
H.450.6	Call Waiting
H.450.7	Message Waiting Indication
H.450.8	Calling Party Name Presentation
H.450.9	Call Completion to Busy Subscriber
H.450.10	Call Offer
H.450.11	Call Intrusion
H.450.12	Additional Network Feature for the exchange of Common Information between endpoints

H.245 protocol

H.245 defines messages and procedures to be used in setting up and taking down logical channels within the context of an H.225 call (for example, an additional video or data channel for the exchange of information). It allows endpoints to determine the network-side/user-side roles, to exchange information about their transmit and receive capabilities and to open and close end-to-end logical channels with characteristics appropriate for the information being exchanged. Like H.450-defined data, H.245 PDUs are tunnelled over H.323 in User-to-User Information IEs in H.225 call control messages.

Each H.245 message is categorized as a request, response, command or indication on the basis of whether it requires a response, requests action or provides information as follows:

- A Request message results in action and requires an immediate response.
- A Response message is the response to a Request message.
- A Command message results in action, but requires no response.
- An Indication message provides information and requires no action or response.

H.245 messages are defined using ASN.1. They are grouped into a number of different functional message sets. Table 3 provides brief descriptions of the most important messages, which come from the network-side/user-side determination, terminal capability and logical channel signaling message sets.

Table 3
Important H.245 messages

Message	Function	Possible replies
Master-Slave Determination	Determines which terminal is Network-side (master) and which is the user-side (slave).	Acknowledge Reject Release (1)
Send Terminal Capability Set	Commands the far-end terminal to indicate its transmit and receive capabilities by sending one or more Terminal Capability Sets.	Terminal Capability Set message(s)
Terminal Capability Set	Contains information about a terminal's capability to transmit and receive multimedia streams.	Acknowledge Reject Release (1)
Open Logical Channel	Opens a logical channel for transport and audiovisual and data information.	Acknowledge Reject Confirm
Close Logical Channel	Closes a logical channel between two endpoints.	Acknowledge
Request Mode	Used by a receiving terminal to request particular modes of transmission from a transmitting terminal.	Acknowledge Reject Release (1)
End Session Command	Indicates the end of an H.245 session. After transmission, the terminal will not send anymore H.245 messages.	None
(1) Used in the event of a time-out.		

H.235 protocol

H.235 provides enhancements within the framework of the H.3xx-Series Recommendations to incorporate security services such as authentication and privacy (data encryption). H.235 works with other H Series protocols that use H.245 as their control protocol. H.235 messages are encoded in ASN.1 format.

Configuration procedures

Introduction

This chapter describes the procedures for configuring H.323 in a Communication Server 2100 network. The Communication Server 2100 H.323 provisioning activity provides the ability to configure Gateway Controllers (GWCs) and the Communication Server 2000 Management Tools (CMT) with the appropriate data to support H.323 gateways on the Communication Server 2100. In an H.323 configuration, the Communication Server 2100 core and Gateway Controllers function as an H.323 gatekeeper.

There are two alternatives for provisioning H.323 on the Communication Server 2100 as follows:

- “Communication Server 2000 Management Tools GUI” on page 35
- “XML OSSGate interface” on page 60

Note: The Communication Server H.323 feature involves tasks commonly associated with both the commissioning of new hardware and provisioning of services.

GUI-driven provisioning summary

For the Graphical User Interface (GUI)-driven approach, a simple multiple-step process is required to add the mandatory node and trunk data to the core, Gateway Controller and Communication Server 2000 Management Tools server. The process can be summarized as follows:

1. Start the Communication Server 2000 Management Tools Selector GUI.
2. Add a Gateway Controller node with an H.323 Gateway Controller profile.
3. Associate an H.323 gateway to a previously-added H.323 Gateway Controller with an H.323 gateway profile and configuration data.
4. Manually provision the Computing Module (CM) trunking tables.

XML-driven OSSGate provisioning summary

For XML-driven configuration, perform the following steps:

1. Connect and log into the OSSGate XML system.
2. Add a Gateway Controller node with an H.323 Gateway Controller profile.
3. Associate an H.323 gateway to a previously-added H.323 gateway Controller with an H.323 gateway profile and configuraiton data.
4. Query for the auto-generated endpoints for the new gateway.
5. Provision the trunking tables in the Computing Module using the endpoints from **Step 4**.

Communication Server 2000 Management Tools GUI

This section describes the various sections of the CS2000 Management Tools (CMT) that enable the provisioning of H.323 Gateway Controllers and media gateways and those that are used for reviewing the resulting auto-provisioned data.

FOR MORE INFORMATION

This document does not provide a complete description of the GUI or even the referenced sections. For detailed information about how to launch and use the GUI, see the *CS2000 Management Tools User Guide*.

This section contains the following procedures:

Launching the CS2000 Management Tools GUI

The first provisioning step is to launch the CS2000 Management Tools Graphical User Interface (GUI). The GUI is launched as a web client and is supported on Windows, Solaris and Linux.

Procedure 1
Launch the CS2000 Management Tools GUI

From your management workstation

1 Launch a web browser. Most of the common versions of Netscape and Internet Explorer are supported.

2 Point to URL Http://<sspfs_server>.

- Replace “<sspfs_server>” with the hostname or IP address of the server on which the Succession Server Platforms Foundation Software (SSPFS) software is installed.

3 A screen appears confirming the connection to Nortel tools and shows choices of the various GUIs.

Select “CS2000 Configuration Tools”.

Note: If you are prompted to install any software such as the Sun JRE/JPI or Sun JWS, install it before continuing. The steps for doing this vary depending on the client platform. However, client-specific instructions are provided on screen. Refer to the SSPFS installation instructions for help installing client software off this web page.

4 A small window appears saying that the software is being loaded. The screen shows the files as they are transferred to the client. This process can take a few minutes to complete. When the system is done transferring files, the window displays “Starting Application” and then goes away.

- Depending of the configuration, a screen, or series of screens, may pop up warning about potential security risks. The screen(s) differ depending on the browser being used. Selecting “always accept” or “trust always” enables the computer to always run Nortel code and prevents these screens from re-appearing on that client box during subsequent GUI launches.

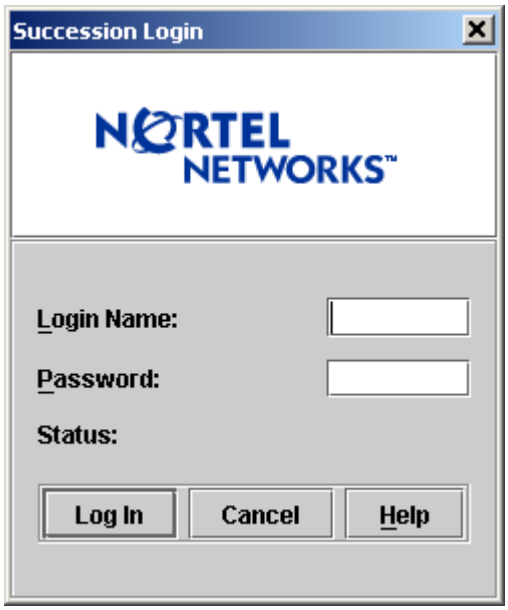
Note: The user should verify with their IT department about internal rules and restrictions before granting “always accept” or “trust always” permission on web applications.

5 A large blank grey screen entitled “CS2000 Management Tools” appears. A smaller screen entitled “Succession Login” appears in front of the “CS2000 Management Tools” screen.

Enter the user name and password to login on this window and click **Log In**.

- If an incorrect username/password is entered, the system displays an error to that effect.

- The user account must be a member of the group “succssn” in order to be allowed to log into the GUI.

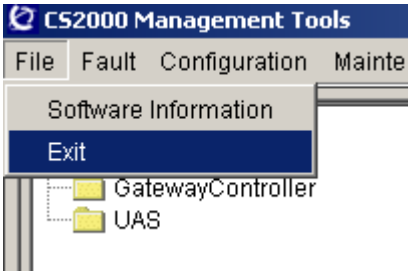


Note: For more information about setting up username and passwords, refer to the *Succession Server Platform Foundation Software Security Installation Manual*. The account name provided must have permission to have read/write access to element managers and trunks in order to be able to perform H.323 provisioning.

6 The small window disappears and the larger window changes into the GUI. This process can take up to a minute or two.

- If the GUI does not appear within two minutes, there is an error. Refer to the “Troubleshooting” section of the *SSPFS and/or CMT User Guide* for more information.

7 To exit the GUI, click on **Exit** from the “File” menu and confirm by clicking the **OK** button.



This procedure is now complete

Adding an H.323 Gateway Controller

Once the GUI has been launched, the next step is to add an H.323 Gateway Controller.

Note: This step may have been pre-completed by a Nortel installation team. To verify whether a Gateway Controller has already been added, single-click on “GatewayController” in the upper-left window on the GUI. A list of all provisioned Gateway Controllers appears in the window in the lower-left side.

There are two profiles that appear in the pull-down menu for the profiles to specify North American and international H.323 Gateway Controllers. The two profiles appear in the menu as follows:

- H.323_NA
- H.323_INTL

Note: Currently, only the H.323_NA profile is supported on the Communication Server 2100.

When these profiles are selected, some read-only fields will change in the window showing the different execs and tone sets. These fields are for information only. While they can have pull-down menus, the selected option does not matter.

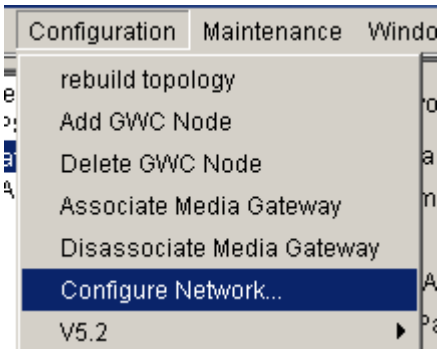
Procedure 2
Add an H.323 Gateway Controller

From the CS2000 Management Tool GUI

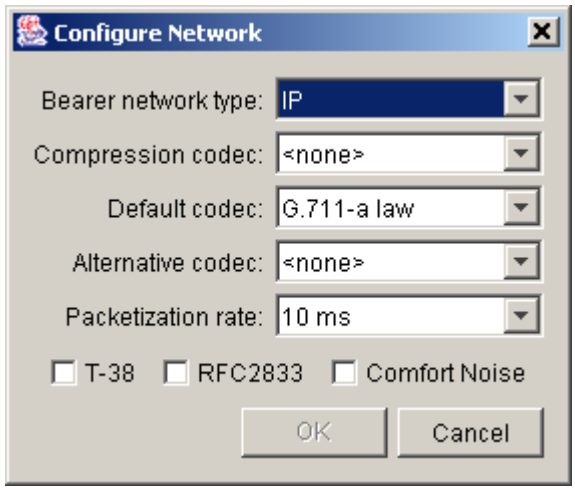
1

If	Do
If this is the first Gateway Controller being added to the system ...	The system must be preconfigured for Gateway Controller addition. Proceed to **Step 1a**.
If this is not the first Gateway Controller being added to the system ...	Proceed to **Step 2.**

a Select **Configure Network ...** from the “Configuration” menu at the top of the screen.



b The “Configure Network” window appears.



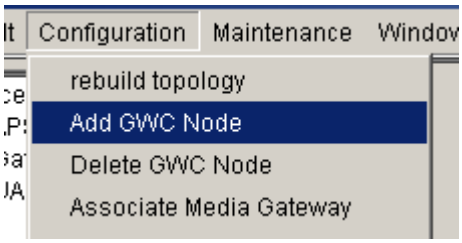
c Select the options needed based on network design/configuration and click on the **OK** button.

CAUTION

If you are unsure about the settings, do not attempt to guess at them as it can cause severe problems once Gateway Controllers and gateways are added to the system.

2 Select “Add GWC Node” from the “Configuration” menu at the top of the screen.

- If the Configuration menu does not list this option, the GUI has not fully loaded. Try again in a minute or two. If the option still does not appear, refer to the “Troubleshooting” section of the *CS2000 Management Tools User Guide*.



3 The “Add Gateway Controller” window appears. This window provides fields for all of the data necessary to add an H.323 Gateway Controller. Enter all of the required information, as described in the following sub-steps, and click on the **OK** button.

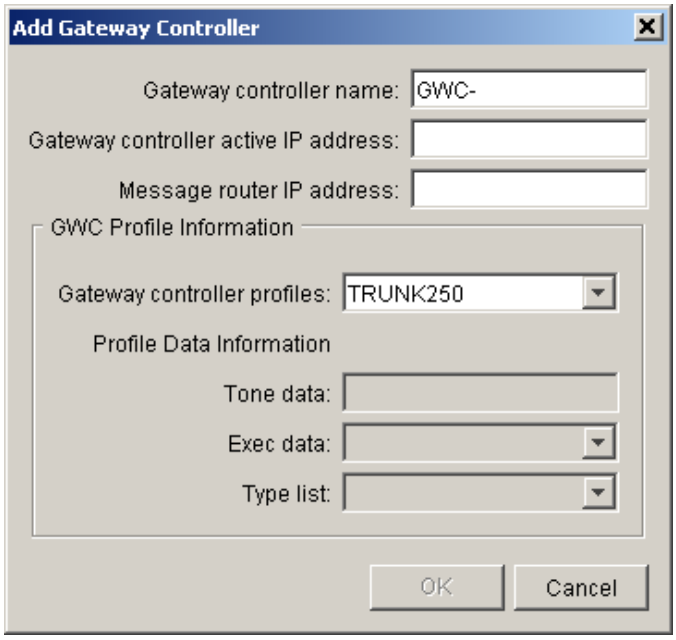
a Select a number for the Gateway Controller. This number must match the one from the SAM21EM GUI and must be of the format “GWC-#”.

b Enter the active unit IP address for the Gateway Controller. This IP address will be the smaller of the IP addresses from the SAM21EM GUI minus 2.

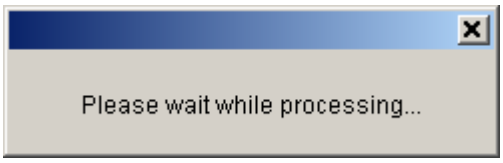
For example, if the IP address from the SAM21EM is 5.15.78.90, the IP address entered here must be 5.15.78.88.

c Enter the IP address of the Computing Module’s message router.

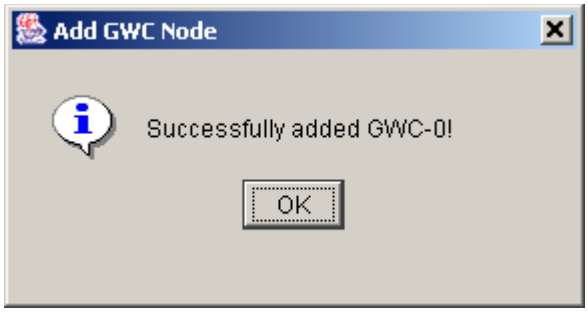
d Select the “H.323_NA” profile. The three greyed-out fields below the profile change to display the exec and tone data for the profile. These cannot be changed.



4 A small “Processing” window appears. Please allow three to five minutes for the addition of the Gateway Controller. This window disappears when the operation is completed and another small window appears displaying the results of the operation.



- If the operation worked correctly, the window displays “Successful”, along with the name of the Gateway Controller as entered previously. If the window displays anything else, the addition of the Gateway Controller failed. The window and server logs will provide more information as to the likely cause of the failure.



5 The new Gateway Controller appears in the list of Gateway Controllers in the bottom left-hand window. The system also adds the Gateway Controller to the core in Table SERVRINV.

To verify that the operation succeeded, click on the Gateway Controller just added and verify that the data displayed on the right-hand side is correct. A background audit will ensure that the Computing Module and the GUI are always synchronized.

This procedure is now complete

Adding a Network Address Translation

Due to the need to conserve IP addresses across enterprises, it is likely that the Communication Server 2100 will be on one IP VPN and the gateways will be in different IP VPNs. Therefore, in order for the Communication Server 2100 to communicate with the gateways, a Network Address Translation (NAT) is needed. As the Network Address Translation needs to be specified during the add media gateway operation, it must be added before the gateway.

FOR MORE INFORMATION

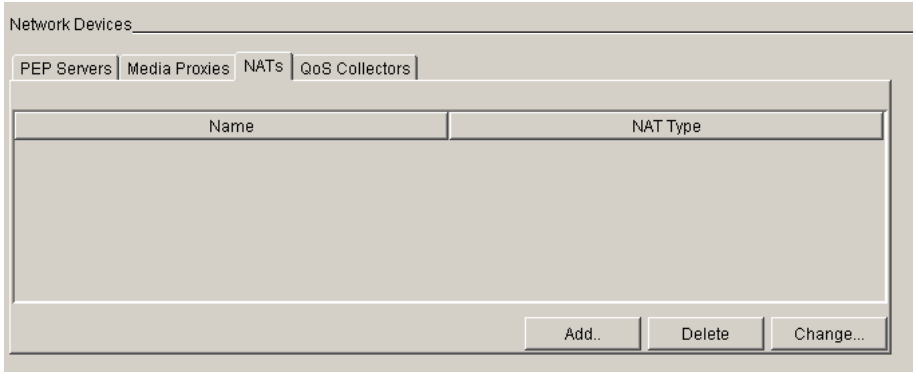
See the *Meridian SL-100/Communication Server 2100 Product Guide, 555-4001-806,* for more information about Network Address Translations.

Procedure 3
Add a Network Address Translation

From the CS2000 Management Tool GUI

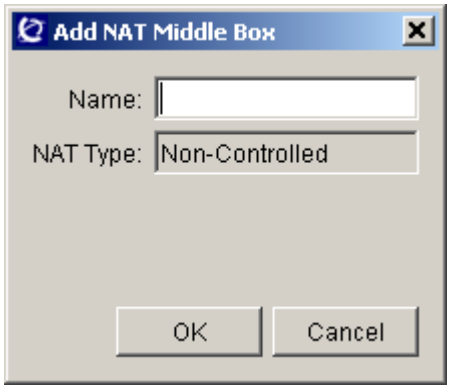
1 Click on the "GatewayController" folder in the upper-left window. Do not select the Gateway Controller added during "Add an H.323 Gateway Controller" on page 39 (or any Gateway Controller for that matter).

2 From the right-hand window, select the "NATs" tab in the middle of the screen. A list of NATs is displayed (the list may be empty at this point).



3 Click the **Add** button to add a Network Address Translation.

4 A small pop-up window displays. Enter the name of the Network Address Translation and select “Non-Controlled”. Then click the **OK** button.



Note: Currently, the only supported type is Non-Controlled. No other option should be selected.

5 The window disappears and the main window displays the Network Address Translation.

6 If an error was made, you can use the **Delete** button to delete the Network Address Translation.

Note: The **Change** button is currently not supported.

This procedure is now complete

Associating an H.323 media gateway

You associate an H.323 media gateway using the Communication Server 2000 Management Tools (CMT) GUI. The following list of media gateway profiles are listed in the pull-down menu used to specify H.323 profiles:

- Nortel Business Communications Manager (BCM)
- Nortel Meridian 1
- Cisco 2600
- Cisco 3600
- Cisco AS5300
- Westell

  The Westell profile contains the setup for the Westell iQ2030 series of gateways. This includes the Q2031 and Q2032. Note that the different gateways vary in maximum sizes so the system adjusts the "max reserved terminations" field accordingly.

Note: This list is provided as a reference only and is subject to change.

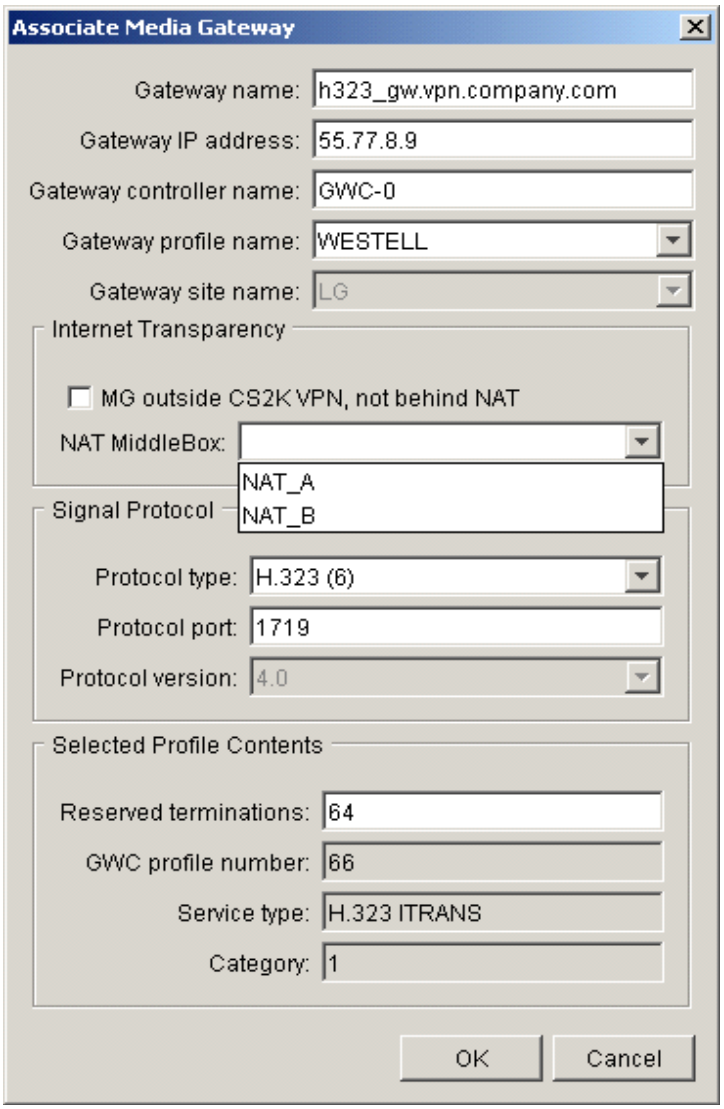
When one of these profiles is selected, the "Internet Transparency" panel appears above the "Signaling Protocol" panel. This panel, as shown in Figure 5 on page 46, contains a checkbox and a text field. If the gateway is behind a Network Address Translation, the checkbox must not be selected and the name of the Network Address Translation must be selected. If the gateway is not on the Virtual Private Network (VPN), but does not use a Network Address Translation, the checkbox must be selected and the text field left empty. If no Network Address Translation is being used and the Gateway is on the customer's VPN, the checkbox must be left unselected and no Network Address Translation selected from the pull-down menu.

The maximum reserved endpoints window changes when a profile is selected to specify the maximum number of endpoints allowed for that profile. This number can be lowered in the GUI if all the endpoints are not being used (0 cannot be entered in this field). This number must always be entered in a power of 32 (for example, 32, 64, 96, 128 etc.). While the code does not enforce this restriction, failure to follow this convention can result in Gateway Controller usability issues if frequent gateway deletions and additions are performed.

The H.323 protocol choice is available from the “Protocol” pull-down menu. The H.323 protocol appears at position number six (last) on the menu and is only valid for the profiles listed above.

When H.323 is selected as the protocol, the “Protocol version” pull-down menu changes to display “4.0” and becomes greyed out so that it cannot be modified. Additionally, the protocol port window changes to display “1719” as the default port. If an H.323 gateway is not behind a Network Address Translator, the H.323 port should be entered in this field. Figure 5 shows an example of the Associate Media Gateway panel.

Figure 5
Associate Media Gateway panel



Attention

ATTENTION

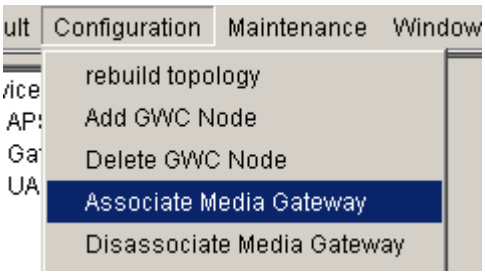
The GUI allows any protocol to be selected for the profiles above and allows for any profile to be selected for the H.323 protocol, even if it is a non-supported configuration. While media gateway addition may respond back as successful, call processing functionality through that media gateway will not function correctly.

Procedure 4
Associate an H.323 media gateway

From the CS2000 Management Tool GUI

1 Select “Associate Media Gateway” from the “Configuration” menu at the top of the screen.

- If the configuration menu does not list this option, the GUI has not fully loaded yet. Try again in a minute of two. If the option still does not appear, refer to the “Troubleshooting” section of the *CS2000 Management Tools GUI User Guide*.



2 The Associate Media Gateway window appears (see Figure 5 on page 46). Use this window to enter all of the necessary data to associate an H.323 gateway. Enter all of the information in the fields as described in the following sub-steps and click the **OK** button:

a Select a name for the new gateway. The only requirements are that the name be less than 32 characters and contains only DNS-querable characters. An example of a proper name is as follows:

gateway1.network.company.com.

b Specify the IP address for the gateway. If the gateway is behind a Network Address Translation, specify the IP address on the Communication Server’s side of the Network Address Translation.

c Specify the number of the H.323 Gateway Controller added earlier.

d Select the appropriate H.323 gateway profile. The three greyed-out fields below the profile will change to display the profile #, service types and category of the profile. These cannot be changed.

- This example uses the Westell H.323 gateway.

e The window expands to display a section on Network Address Translations.

If	Do
If the gateway is behind a Network Address Translation ...	Select a Network Address Translation from the pull-down menu.
If the gateway is not behind a Network Address Translation ...	Select the “not behind NAT” checkbox according to the gateway’s VPN location.

Note: The Network Address Translation name specified must be entered in Procedure 3 on page 43. Otherwise, an error occurs.

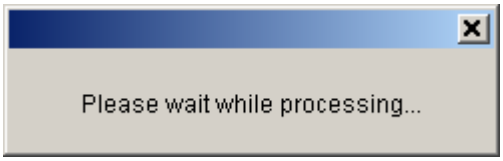
f Select H.323 for the protocol. The protocol version field changes to “4.0” and is greyed out. The default port changes to “1791”.

g Specify the number of endpoints desired.

Note:1 The system generates the number of endpoints based on the number of “reserved terminations”. Endpoint groups are allocated in blocks of 32. The Westell example has a default value of 64 and the system allocates two endpoint groups consisting of 32 endpoints per group. If you specify a value of 33 for the reserved terminations, the system generates two endpoint groups.

Note 2: The three fields in grey at the bottom of the window are for informational purposes only and cannot be changed. These fields are designed for Nortel support and not for end-customer use. The “service type” field should always include both “H.323” and “ITRANS” for H.323 gateways.

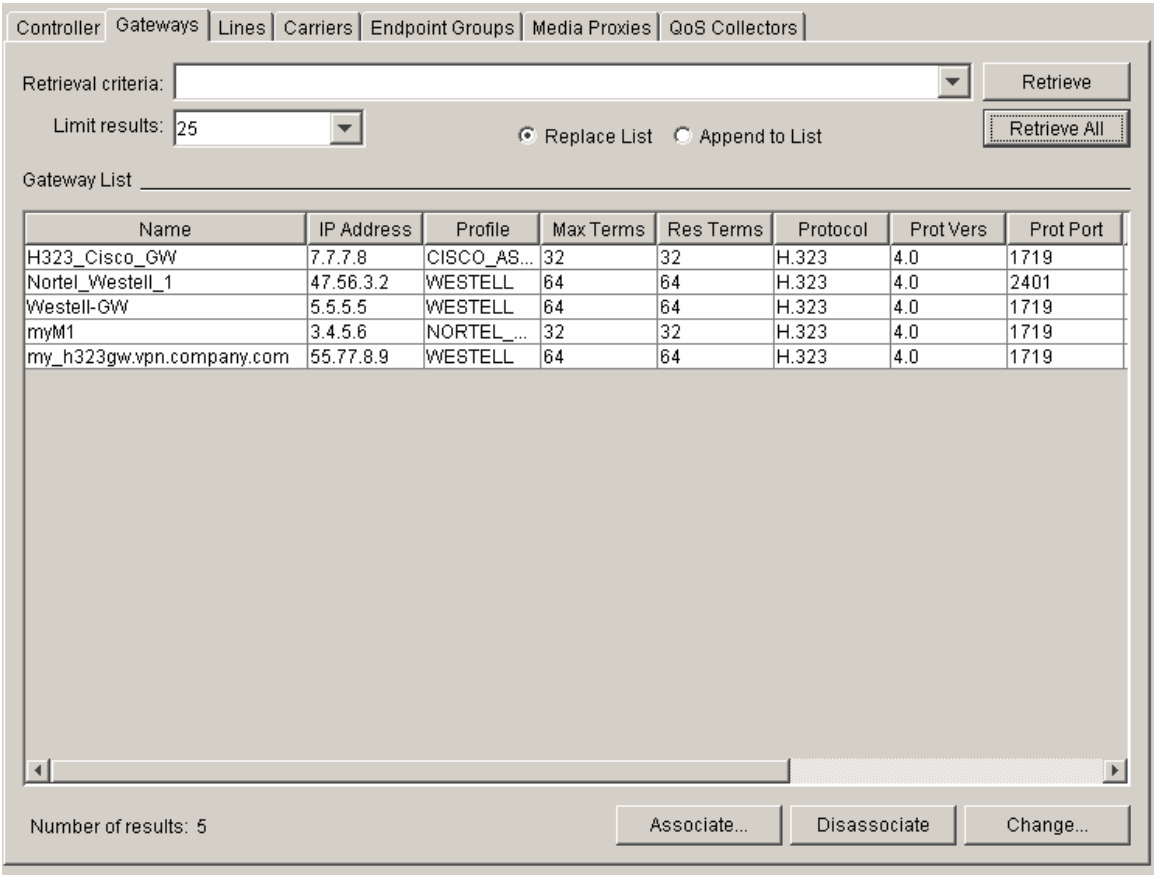
3 The small “Processing” window appears. Please allow three to five minutes for the addition of the gateway. This window disappears when the operation is completed and a new small window appears describing the results of the operation.



- If the operation was successful, the window displays “Successful”. If the window displays anything else, the addition failed. The window and server logs provide more information as to the likely cause of the failure.
- If the processing window does not disappear after five minutes, the window can be closed by clicking the “x” at the upper-right corner (Microsoft Windows) or double clicking the box in the upper-left corner (Solaris/Linux). Also, occasionally, a “Timed Out” window will appear. In both cases, the operation may have succeeded and needs to be verified using the following steps.

4 Verify the addition of the gateway by selecting the “Provisioning” tab from the right-hand side of the GUI screen and then clicking on “Gateways” from the tab in the middle. When “show all” is clicked, the gateway should be displayed. Verify that the data is what was entered.

To aid in readability, the following screen has been expanded from its original size. Due to the amount of data, a scroll-bar is required to display items in the list. The fields are re-arrangeable by grabbing (that is, clicking and holding) on the title and dragging it to another location. Clicking on a title sorts the list by that title (ascending to descending). The size of each field can also be expanded or contracted by clicking on the line between the two fields and moving it to the right or left.



- The newly-created gateway appears as the last item in the list. The list contains all gateways added using both GUI and XML provisioning.

5 Verify that the endpoints were created by clicking on the “Endpoint Groups” tab and clicking on the **Show all** button. The endpoint groups should be displayed.

6 Click on each of the Endpoint Groups (EPGs) associated with that gateway and click on the **Display** button.

Note: The order of the Endpoint Group names is not important. The only important information are the TIDs which are assigned to the gateway. These may be in dis-contiguous blocks of 32 TIDs.

To aid in the following steps, it helps to print this window. To print this window, perform the following sub-steps:

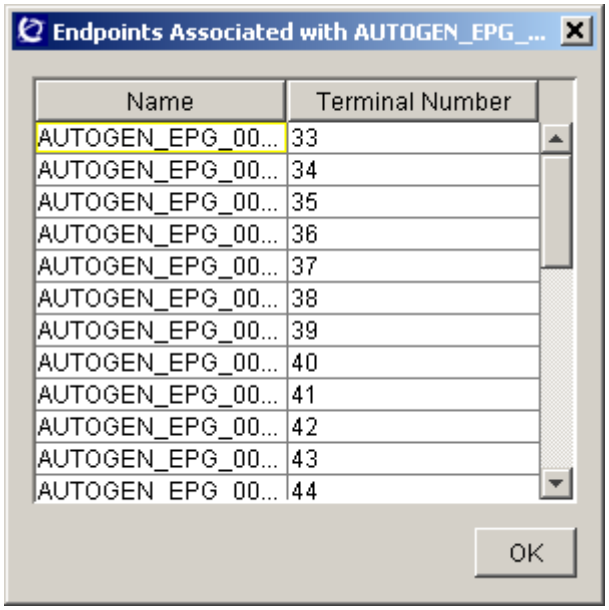
Note: These instructions are for the Windows client OS. Users of Linux or Solaris clients need to follow the screen capture instructions for their OS system.

a Resize the window so that it shows all of the endpoints that are relevant to the operation (that is, grab the window and expand it). If this cannot be done, this operation can be performed multiple times to show all of the relevant endpoints.

b Click **Crtl** + **Alt** + **PrtScrn** (that is, Control/Alternate/ PrintScreen) simultaneously.

It will appear that nothing happened; however, if you are on Windows and are running a clipboard monitor, it may indicate a graphic has been stored.

c Launch Microsoft Paint or other graphics program (for example, Start > Programs > Accessories > Paint). Click **Crtl** + **V** (that is Control/V) to paste the image. You can now print the screen (for example, File > Print).



At this point, the work using the GUI is complete. You can now shut down the GUI.

However, the provisioning process is not yet complete. While the gateway has been added to the system, it cannot yet provide service. To provide service, the endpoint groups must be datafilled manually on the core.

Note: An OSS system generally applies these changes automatically.

From the Core Manager

7 Log into the core. This varies depending on the type of Computing Module hardware and office setup.

8 Datafill the trunk provisioning tables on the Computing Module using the data from the GUI. The example in the following sub-steps uses the name "H.323PRI". Tables are not case sensitive.

Refer to DMS core trunking documentation for additional information.

a Add a trunk group (CLLI) to Table CLLI. The only requirements are that the CLLI and ADMUM field be unique.

Example: `H323PRI 123 64 MY_TRUNKGROUP_INFO`

b Add the trunk group to table TRKGRP. The name must match the one from Table CLLI.

Example: `H323PRI PRA 0 NPDGP NCRT MIDL N $$`

c Add the trunk group to table TRKSGRP. The name must match the one from Table CLLI.

Example: `H323PRI 0 DS1SIG ISDN 20 20 87Q931 2 N STAND NETWORK PT-PT USER N UNEQ 160 N DEFAULT` **`GWC 0`** `29 1 64K HDLC $$`

- The Gateway Controller specified must be the Gateway Controller entered in **Step 2c** (this appears in **bold** type in the example above). The Gateway Controller must be the same for all tuples.
- The Terminal Number (TN) for the single D-channel of the H.323 PRI trunk group must be mapped to the first endpoint/TN of the first endpoint group that the system generated for the respective H.323 gateway.

  Note: The first TN of the first endpoint group allocated for the H.323 gateway cannot be the integer "1".

- H.323 interfaces do not support backup D-channels.
- There is a required one-to-one relationship for an H.323 gateway and an H.323 PRI trunk group. The system supports only one H.323 PRI trunk group per H.323 gateway.

d Add the H.323 PRI trunk members to Table TRKMEM. The name must match the one from Table CLLI. There will be many of these tuples to enter (that is, one for each endpoint in the endpoint group[s]). Each endpoint from the GUI, requires a tuple specifying the TID.

- The Gateway Controller specified must be the Gateway Controller entered in **Step 2c** (this appears in **bold** type in the example below). The Gateway Controller must be the same for all tuples.
- The TID consists of two numbers: a node and a Terminal Number (this appears in *italic* type in the example below). This will be from the endpoint.

  Note: Do not enter a tuple in this table using the TID used from **Step 7c** (Table TRKSGRP). Start with the second TN of the first endpoint group allocated for the H.323 gateway.

- For an H.323 gateway with 64 endpoints/TNs, there can be up to 63 TRKMEM tuples. For an H.323 gateway with 32 endpoints there can be up to 31 tuples.

Example 1: First TRKMEM tuple from this range.

```
H323PRI 1 0 GWC 0 29 2
```

Example 2: Last TRKEM tuple from this range.

```
H323PRI 63 0 GWC 0 29 64
```

A lower number of TRKMEM tuples can be added (for example, only 60 trunk members).

Example: `H323PRI 60 0 GWC 0 29 61`

e Create a logical terminal group in Table LTGRP.

- The group name must be unique. It will be used in Tables LTDEF, LTMAP, LTDATA and LTCALLS.
- The group number must be unique.

Example: Using ISDN as the name.

```
ISDN 902 (SAPI16) $
```

f Define a PRI LTID in Table LTDEF.

Example: `ISDN 902 B PRA 63 NTNAPRI V1 NIL (NOPMD) $`

g Map the LTID to the H.323 PRI trunk group in Table LTMAP.

Example: `ISDN 902 CLLI H323PRI (TEI 0) $`

h Add the H.323 option in Table LTDATA.

Example: `ISDN 902 SERV SERV Y Y SCREENED ALWAYS (PRI_IP_PROT H323) $`

i Add the PRI routing data to Table LTCALLS.

Example: `ISDN 902 PUB XLALEC 4 919_IBN1_4 NLCA_LATA1_0 $", "ISDN 902 PVT XLAIBN 4 919_IBN1_4 NLCA_LATA1_0 CUSTOMER_GROUP 0 0 $`

This procedure is now complete

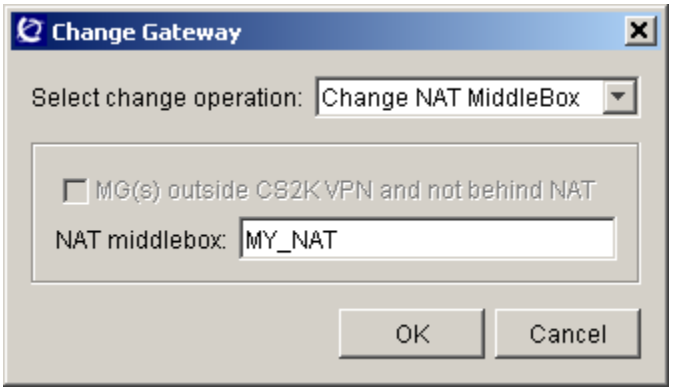
Editing/changing an H.323 media gateway

The process for changing an H.323 media gateway, for the most part, is identical to the process for changing non-H.323 media gateways.

When a gateway is selected in the “Gateways” tab in the Gateway Controller Element Manager section of the GUI, clicking on the **Change ...** button opens up a dialog box allowing the modification of the various fields associated with a gateway.

There are several editing options. Currently, only changing the Network Address Translation name is supported. When the Network Address Translation is selected from the menu, the box expands to show the Network Address Translation setting (see below).

Note: Other options may be presented for changing. However, if any of these options are selected for changing, the system presents an error message indicating that these cannot be changed for the H.323 gateway(s). If non-H.323 gateways were selected at the same time, the system also will change the options for the non-H.323 gateways.



Disassociating an H.323 media gateway

WARNING

Before a gateway can be deleted you must remove all the datafill from the Computing Module. The GUI will not verify that this datafill is removed. Removing datafill is similar to steps 7 and 8 in Procedure 4 on page 47, but in reverse order.

If the datafill is not removed, the gateway can still be removed. However, this removal results in inconsistent data between the CS2000 Management Tools and the Communication Server 2100 which is not recommended, because this may not be detected by an audit.

WARNING

Before a gateway can be deleted, it is important to verify that it is not in use to avoid taking down active calls. All associated trunks must be in an INB state to make sure that no calls can originate during the deletion process. Failure to do this can result in the system denying the delete request.

Once all the Computing Module datafill is removed, the gateway can be deleted using the GUI.

To delete an H.323 media gateway, either disassociate the media gateway from the “Configuration” menu and type the name of the gateway to be deleted or select the gateway from the “Gateway” tab on the Gateway Controller data table and click on the **Delete** button.

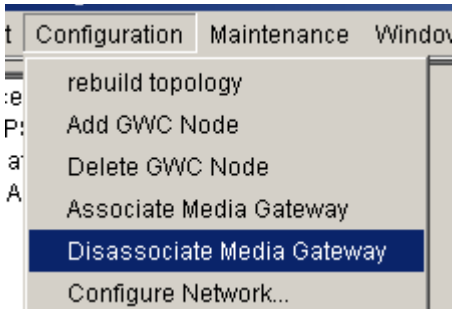
If the operation is successful a confirmation window appears. If there was an error during the deletion, the window describes the reason for the deletion failure

Procedure 5 on page 55 describes the easiest way to disassociate an H.323 gateway.

Procedure 5
Disassociate an H.323 gateway

From the CS2000 Management Tool GUI

1 Select “Disassociate Media Gateway” from the “Configuration” menu.



2 A small Disassociate Media Gateway dialog box appears. It has only one text field.

3 Enter the name of the gateway to be deleted and click the **OK** button.

4 A small “Processing” window may appear. Please allow two to three minutes for the deletion of the gateway. The window disappears when the operation is completed and a new window appears displaying the results of the operation as follows:

- If the operation is successful, the window displays “Successful”. If the window displays anything else, the disassociation failed. The window and server logs provide more information about the likely cause of the failure.
- If the processing window does not disappear after five minutes, the window can be closed by clicking the “x” at the upper-right corner (Microsoft Windows) or double clicking the box in the upper-left corner (Solaris/Linux). The operation may have succeeded.

5 Verify the gateway is deleted by following **Step 4** in Procedure 4 on page 47. The gateway should no longer be displayed.

Note: The endpoint groups associated with this gateway will also be deleted.

Fore more information about the CS2000 Management Tools GUI and the “DisassociateMG” window, see the *CS2000 Management Tools User Guide*.

This procedure is now complete

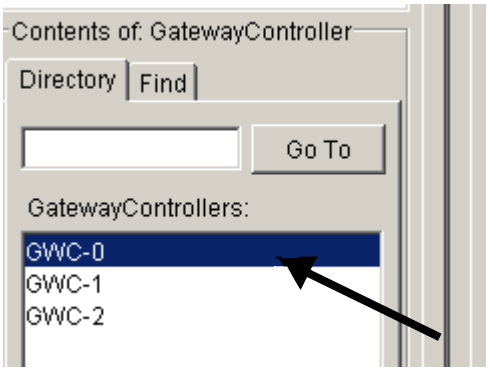
Deleting an H.323 Gateway Controller

There are multiple ways of removing Gateway Controllers as described in the *CS2000 Management Tools User Guide*. Procedure 6 describes the easiest way to delete an H.323 Gateway Controller.

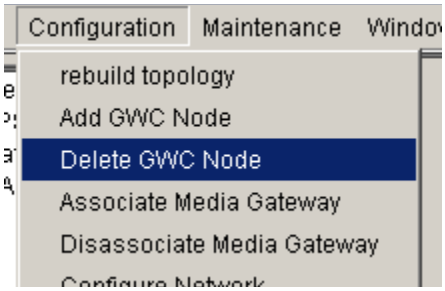
Procedure 6
Delete an H.323 Gateway Controller

From the CS2000 Management Tool GUI

1 Select the Gateway Controller to be deleted from the bottom-left window. This example deletes GWC-0.

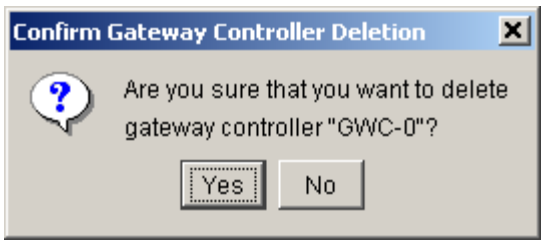


2 Select “Delete GWC Node” from the Configuration menu.

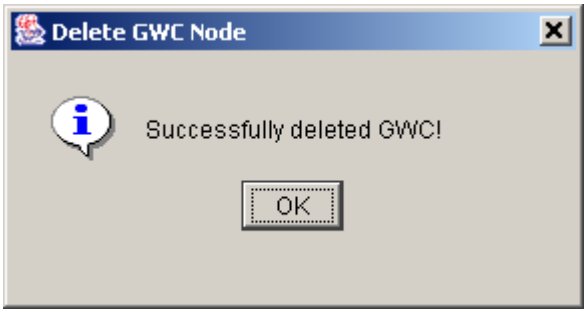


3 The “Confirm Gateway Controller Deletion” window appears. Confirm the deletion by clicking on the **Yes** button.

- If an error occurs, a window displays providing information about the reason(s) for the failure to delete. The most common reason is gateways still subtending off the Gateway Controller.

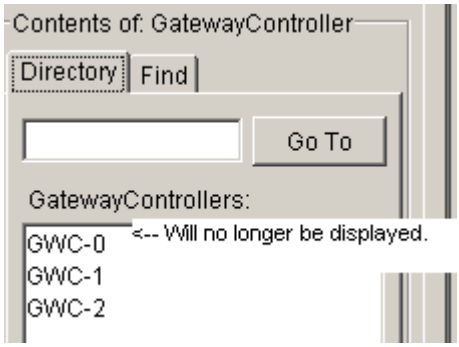


If successful, a window displays acknowledging the deletion.



4 Verify that the Gateway Controller is on longer displayed in the bottom-left window.

Sometimes the Gateway Controller may still be displayed. In this case, click on APS (or another element) in the upper-left window and then click on GatewayController in that same window and then look in the bottom-left window and it should be removed.

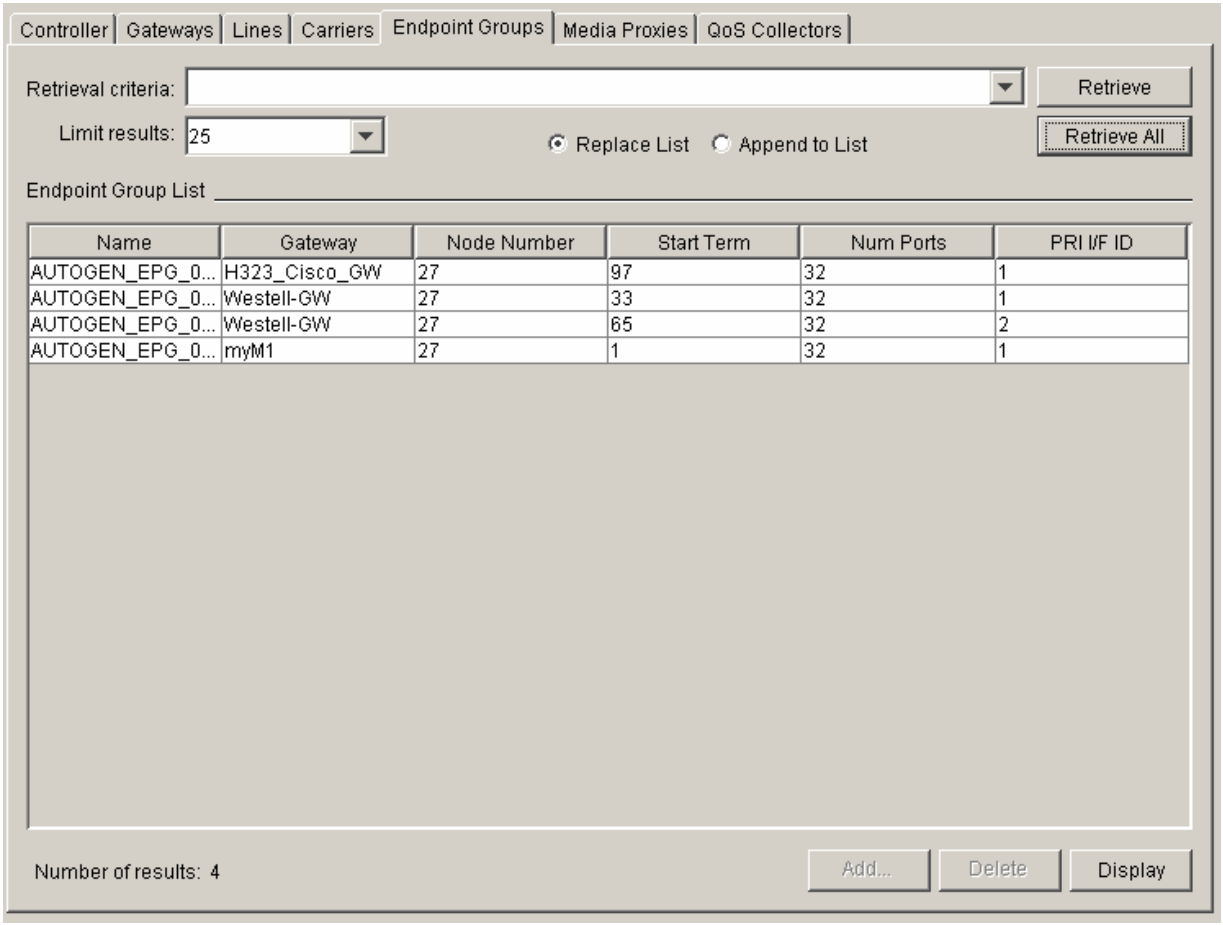


5 Verify that the Gateway Controller is no longer listed in the Computing Module Table SERVRINV. If it is still displayed, this will be caught by the periodic audit which will allow the deletion of it.

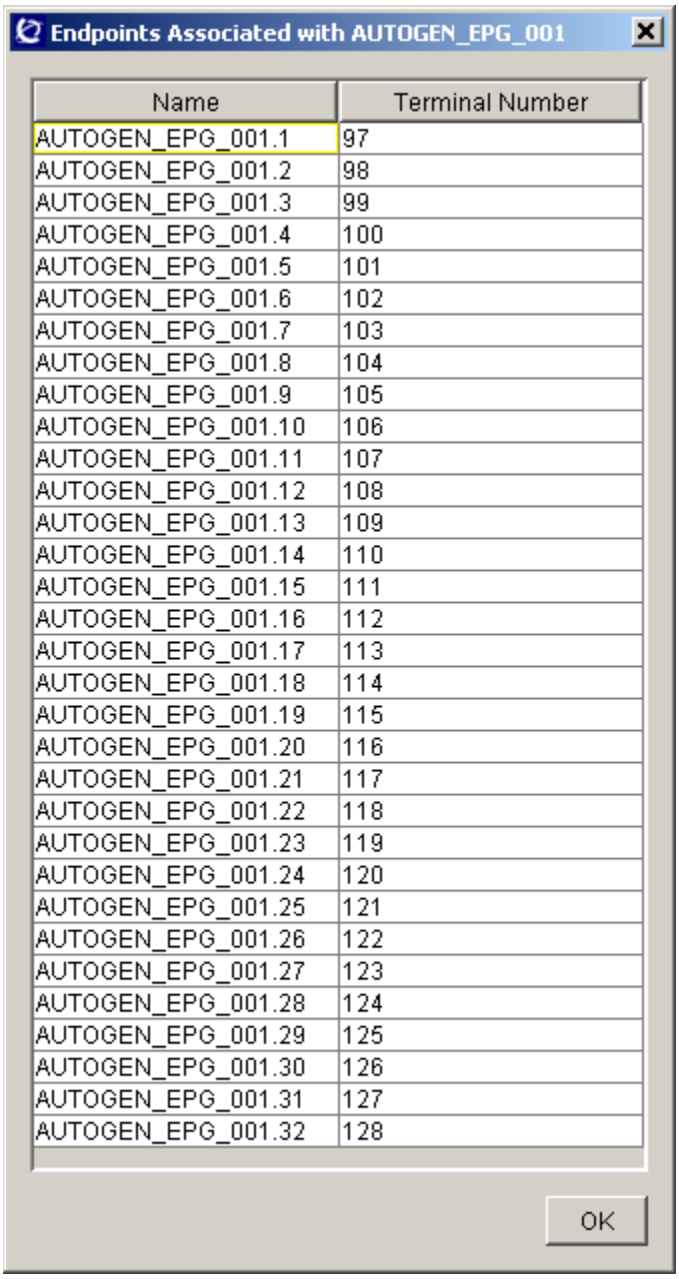
This procedure is now complete

Endpoint Group tab on Gateway Controller table

The H.323 application introduces a new tab on the Gateway Controller table of the CS2000 Management Tools GUI. The Endpoint Groups tab displays the endpoints that are created by the addition of H.323 media gateways. When an H.323 media gateway is being added, the system automatically provisions one or more carriers against the gateway. For this reason, the Endpoint Group tab is read-only. When a gateway is deleted, the associated endpoints are removed with it.



When you click on the **Display** button, the following pop-up window appears showing endpoint to TID mappings:



XML OSSGate interface

This section describes how to provision H.323 Gateway Controllers and media gateways from an Operations Support System (OSS). For the most part, the Extensible Mark-up Language (XML) commands mirror the GUI equivalents and provide similar functionality.

This section only describes the changes and additions to the commands due to supporting H.323 and is not intended to be a complete XML user guide or even to fully explain how to use the modified commands. Refer to the *OSSGate Users Guide* for detailed instructions about using these commands.

The section describes the following H.323 XML OSSGate commands:

Adding an H.323 Gateway Controller

The process for adding an H.323 Gateway Controller using XML is similar to adding a non-H.323 Gateway Controller. The only difference is that one of the new H.323 GWC profiles must be specified. These two profiles are the same ones listed in the add Gateway Controller window on the GUI and are as follows:

- H.323_NA
- H.323_INTL (not currently supported on the Communication Server 2100)

The following is an example XML message used to add a Gateway Controller (the H.323 tag [NA in this case] appears in **bold)**:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
   <Command>
      <Interface>cs2kCfgMgrIf</Interface>
         <Methods>
            <addGWCtoCS usn="1" version="1.0">
               <Parameters>
              <csUIName>MY_CALLSERVER</csUIName>
                  <gwcUIName>GWC-0</gwcUIName>

<profileName>H.323_NA</profileName>

<gwcActvIp>47.142.128.36</gwcActvIp>
                  <gwcSnmpPort>161</gwcSnmpPort>

<msgRouterIp>47.142.128.24</msgRouterIp>

<msgRouterIpPort>4684</msgRouterIpPort>
               </Parameters>
            </addGWCtoCS>
         </Methods>
   </Command>
</CommandList>
```

The responses returned for adding an H.323 Gateway Controller are identical to the responses for adding non-H.323 Gateway Controllers and are not discussed here. Refer to the *OSSGate Users Guide* for a list of all possible error and success responses and recommended courses of action for each.

Associating an H.323 media gateway

Associating an H.323 media gateway using XML is similar to adding a non-H.323 media gateway. The only differences are the additional media gateway profiles.The following is an example of an associate H.323 media gateway XML command. H.323-specific data appears in **bold**. In this example, a Cisco 3600 series H.323 GW is selected.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
   <Command>
      <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
         <assocMG usn="1" version="1.0">
            <Parameters>

<mgUIName>gateway.company.com</mgUIName>

<mgProfileName>CISCO_3600</mgProfileName>
                <mgIpAddr>69.143.34.1</mgIpAddr>
              <mgProtocolType>6</mgProtocolType>

<mgProtocolVersion>4.0</mgProtocolVersion>

<mgProtocolPort>1720</mgProtocolPort>
                <gwcUIName>GWC-0</gwcUIName>
                <NATname>MY_NAT</NATname>
            </Parameters>
         </assocMG>
      </Methods>
   </Command>
</CommandList>
```

Note: Note that the method name is “assocMG”, not “associateMG” as it is in the GUI.

One thing to point out is that, unlike in the GUI, when adding a gateway using XML, there is no option to select no NAT or no auto provisioning. If the NATname field is excluded from the XML message, no NAT will be associated with this gateway.

Please refer to the *OSSGate Users Guide* for a list of all possible error and success responses and recommended courses of action for each. If one of these errors is received, the gateway will not be added to the system (and the endpoint groups will not be created).

Note: After the OSS system adds the new gateway (which auto-provisions the endpoint group[s]), it needs to add the necessary CM datafill to Tables LTGRP, LTMAP, LTDATA, CLLI, TRKGRP, TRKSGRP, and TRKMEM, among potentially others, to bring the gateway into service. This process is identical to the process the OSS follows after completion of an `addCarrier` XML command and is not discussed here.

Querying for a media gateway's endpoints (TIDs)

An XML method is used for the querying of endpoints (TIDs) based on the gateway name. This method is used by OSS systems during data-sync operations.

The XML client (OSS system) sends in a request to list all the endpoints, optionally specifying the name of a gateway. The system responds with an XML message listing all of the endpoints (TIDs) on the system, or, if a gateway was specified, only the ones subtending off that gateway. The response in the latter case is similar to the one returned during the add H.323 media gateway operation from the previous section.

This is a read-only method as it only allows for the querying of the endpoints and not for modifying them. For this reason, it is assigned to the trkro security permission group. In order to use this method, the OSS technician must log into OSSGate using an account containing trkro access.

The following is an example of the method, "queryEndpointGroups", in the existing Node Provisioning XML interface, "cs2kCfgMgrIf":

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

<mgName>gateway.company.com</mgName>
              </FILTER_MG>
            </Parameters>
         </queryEndpointGroups>
      </Methods>
   </Command>
</CommandList>
```

The previous example demonstrates querying for the endpoints only on the gateway gateway.company.com due to the line in bold. If that line was removed from the XML message and "ALL" were used, all of the endpoint groups on all of the gateways in the system would be returned. If the line were replaced with `<gwcName>gwc-2</gwcName>`, for example, all the endpoint groups on GWC-2 would be displayed.

Note: Only one Gateway Controller, endpoint, or media can be specified. If more then one entry is specified, an error is returned.

After processing, the OSSGate will respond with the following message listing the endpoints. If a gateway is specified, this should take less then a minute. If a Gateway Controller is specified, this operation can take a couple of minutes. If a system-wide query is done, this operation can take upwards of 10 minutes or more depending on the number of endpoint groups and the load on the system.

Note: Due to performance reasons, it is recommended that system-wide queries only be done during off-peak times when no other provisioning is ongoing.

```
<?xml version="1.0" encoding="UTF-8" >
   <CommandList>
      <Response>
         <Interface>EndptGrpProvIf</Interface>
         <Methods>
            <queryEndpointGroups usn="1" version="1.0">
              <ReturnData>
                 <gwc name="GWC-8">
                    <mg name="gateway.company.com">
                       <endpointGroup name="AUTOGEN_EPG_001">
                          <svcData>
                            <service>PRI</service>
                            <IID>1</IID>
                          </svcData>
                          <endptList>
                            <endPt name="AUTOGEN_EPG_001.1">
                              <tid>27 257</tid>
                            </endPt>
                                        <...>
                           <endPt name="AUTOGEN_EPG_001.32">
                              <tid>27 288</tid>
                           </endPt>
                          </endptList>
                       </endpointGroup>
                    </mg>
                 </gwc>
                 <RC>0</RC>
                 <MsgTxt> Retrieval...Completed.</MsgTxt>
              </ReturnData>
            </queryEndpointGroups>
         </Methods>
      </Response>
   </CommandList>
```

If the line in **bold** from the first message was removed or replaced with a `gwcName` tag (and multiple H.323 gateways exist on the system), there would be more than one `<gateway>` tag, each with a series of `<endpoint>` tags under them in the response above.

Note: If a gateway exists on the system, but does not have any endpoints associated with it, it will not be considered an error by this method even though it is likely the result of an error during media gateway association. It is displayed, but there will be no `<endpoint>` tags under it.

Disassociating an H.323 media gateway

The process for disassociating an H.323 media using XML is identical to the process for deleting other kinds of gateways.

To delete an H.323 media gateway, use the disassociate media gateway XML command. This command, unchanged by this feature, is described fully in the *OSSGate Users Guide*.

Note: Deleting H.323 gateways can take considerably longer than deleting non-H.323 gateways. The reason for this is that when an H.323 gateway is removed from the system, associated datafill in the core and associated endpoints on the Gateway Controller are also removed. Therefore, a minute or two delay should be expected and this should not be viewed as an error.

WARNING

Before a gateway can be deleted you must remove all the datafill from the Computing Module. This process is identical to the process followed by the OSS systems, before the deleteCarrier command and can vary by OSS vendor.

WARNING

Before a gateway can be deleted, it is important to verify that it is not in use to avoid taking down active calls. All associated trunks must be in an INB state to make sure that no calls can originate during the deletion process. Failure to do this can result in the system denying the delete request.

Deleting an H.323 Gateway Controller

The process for deleting a H.323 Gateway Controller using XML is identical to the process for deleting other kinds of gateways.

To delete a H.323 Gateway Controller, use the delete Gateway Controller XML command. This command, unchanged by this feature, is described fully in the *OSSGate Users Guide*.

Logs

Introduction

A log report is a message about important conditions or events related to the performance of a component in a Communication Server 2100 network. Log reports include, but are not restricted to, the following information:

- state and activity reports
- changes in state
- hardware or software errors
- test results
- other events or conditions that affect performance

When H.323 is configured, the Communication Server 2100 can generate the following logs to help technicians monitor system performance and troubleshoot problems:

- GWC506 – An H.323 GWC unit has lost the connection to an H.323 gateway.
- GWC507 – The connection between a GWC and an H.323 gateway has been restored.
- GWC600 – Generates an information log about an H.323 failure.

Note: This chapter only describes H-323-specific logs. For more information about Communication Server 2100 logs, see the *Succession Fault Management Logs Reference*, NN10275-909.

GWC506

Log report GWC506 indicates that an H.323 Gateway Controller unit has lost the connection to an H.323 gateway. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Note: This log report is generated only for H.323 gateways that contain fewer than 64 endpoints.

Format

The format for log report GWC506 is as follows:

```
RTPG GWC11 GWC600 MAY21 14:54:47 <sequence number> PBSY Gateway
State Change
Category: Communication
Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
Specific Problem: H323 Connection lost to gateway <gateway name>
Description: <reason for problem>
```

Selected field descriptions

Table 4 explains selected fields in the log report.

Table 4
Log GWC506 fields

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	Alphanumeric text label	Identifies the Gateway Controller node and unit affected by the failure.
gateway name	Alphanumeric text label	Identifies the gateway connected to the Gateway Controller card affected by the failure condition. *Example:* BCM_RTPG1
reason for problem	Text description	Describes the specific reason for the failure.

Action

Table 5 describes the actions the user can take when a Gateway Controller experiences a loss of connection to an H.323 gateway.

Table 5
Actions associated with a loss of connection to an H.323 gateway

Description	Action
Gateway Unregistration by Communication Server 2100 Successful	No action required. The technician has busied the D-channel for the H.323 gateway, or the CS 2100 has busied the D-channel for H.323 gateway due a maintenance action such as Gateway Controller cold SWACT, CS 2100 restart reload, etc.
Time to Live Expired	The H.323 gateway failed to refresh the 30-second keepalive timer in the CS2000 Gateway Controller. Verify communication between the gateway and the Gateway Controller. If necessary, check the H.323 gateway itself, since the CS 2100 Gateway Controller unregistered the H.323 gateway, because the Time-To-Live value has expired.
Gateway Initiated Unregistration	The H.323 gateway initiated the unregistration from the CS 2100 for some reason. Action on the H.323 gateway side may be warranted if the unregistration was unplanned.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC507

Log report GWC507 indicates that the connection between a Gateway Controller and an H.323 gateway has been restored.

Note: This log report is generated only for H.323 gateways that contain fewer than 64 endpoints.

Format

The format for log report GWC507 is as follows:

```
RTPG GWC4 GWC507 AUG02 14:15:28 <sequence number> RTS Gateway
State Change
Category: Communication
Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
Specific Problem: H323 Connection restored to gateway <gateway
name>
Description: Gateway Registration Successful
```

Selected field descriptions

Table 6 explains selected fields in the log report.

Table 6
Log GWC507 fields

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	Alphanumeric text label.	Identifies the Gateway Controller node and unit affected by the failure. *Example:* GWC-11-UNIT-0
gateway name	Alphanumeric text label	Identifies the gateway connected to the Gateway Controller card affected by the failure condition. *Example:* BCM_RTPG1

Action

No action is required.

You can verify that the D-channel has gone in service (INSV) at the MAPCI;MTC:TRKS; TTP; PRADCH; POST GD <trkname >. If any trunk members are provisioned and you wish to be able to make calls, check the trunk members to see that they are also idle (IDL).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC600

Log report GWC600 is an information log for an H.323 failure. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Format

The format for log report GWC600 is as follows:

```
RTPG GWC11 GWC600 MAY21 14:54:47 <sequence number> INFO GWC
Protocol Event
Category: Communication
Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
Specific Problem: <specific problem>
Description: <reason for problem>
```

Selected field descriptions

Table 7 explains selected fields in the log report.

Table 7
Log GWC600 fields

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	Alphanumeric text label	Identifies the Gateway Controller node and unit affected by the failure. *Example:* GWC-11-UNIT-0
gateway name	Alphanumeric text	Identifies the gateway connected to the Gateway Controller card affected by the failure condition. *Example:* BCM_RTPG1
specific problem	Text description	Identifies the H.323 failure condition.
reason for problem	Text description	Describes the specific reason for the failure.

Action

Table 8 table describes the actions the user takes when an H.323 failure condition occurs.

Note: GRQ = Gatekeeper request
RRQ = Registration request
ARQ = Admission request
URQ = Unregistration request
DRQ = Disengage request
RAS = Registration, admission and status

Table 8
Actions associated with an H.323 failure (Sheet 1 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Name Not Provisioned ***Note:*** A log with the same description is generated for an RRQ received with an invalid gateway name.	Ensure that the H.323 gateway name provisioned on the CS 2100 Gateway Controller Manager matches exactly with the gateway name provisioned using the H.323 Gateway Controller provisioning tool.
H323 GRQ rejected	Gateway IP Address Invalid ***Note:*** A log with same description is generated for an RRQ received with an invalid source gateway IP address. In this case, the source IP address is the IP address in the Ethernet frame. So, for gateways behind the NAT, the source IP address will be the NAT IP address. The RAS IP address is not part of the H.323 payload. If the H.323 gateway is not behind a NAT, the source IP will be the IP address of the H.323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway IP address provisioned on the CS 2100 Gateway Controller Manager matches exactly the IP address of the NAT box. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2100 Gateway Controller Manager matches exactly the IP address of the H323 gateway.
H323 GRQ rejected	Gateway Port Invalid ***Note:*** A log with same description is generated for an RRQ received with an invalid source gateway port. In this case, the source port is the source port address in the Ethernet frame. So, for gateways behind a NAT, the source port is the port entry of the static bind at the enterprise NAT for the H.323 gateway. It is not the RAS port which is part of the H.323 payload. If the H323 Gateway is not behind a NAT, the source port will be the RAS port of the H323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway port provisioned on the CS 2100 Gateway Controller Manager matches exactly the port entry of the static bind at the enterprise NAT for the H.323 gateway. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2100 Gateway Controller Manager matches exactly the IP address of the H.323 gateway.

Table 8
Actions associated with an H.323 failure (Sheet 2 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Missing Mandatory RAS Address	No action needed. This log report is for information only.
H323 RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 keepAlive RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 RRQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 ARQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 RRQ rejected	D-Channel Not Provisioned	Ensure that the trunk datafill is provisioned correctly on the CS 2100 XA-Core and CS 2100 Gateway Controller.
H323 ARQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 RRQ rejected	D-channel Not Provisioned	Ensure that the trunk datafill is provisioned correctly on the CS 2100 XA-Core and CS2000 Gateway Controller Manager.
H323 RRQ rejected	D-channel Out Of Service	Ensure that the D-channel associated with the H.323 gateway is in LO state at the MAPCI, mtc, ttp, trks, pradch level on the CS 2100 Core, before the H.323 gateway registers. This log can be cleared with a BSY/RTS of the D-channel associated with the H.323 gateway on the CS 2100 Core. ***Note:*** Trunk logs are also generated which are similar to PRI trunk logs. *For example:* H.323 gateway BCM_RTPG" appears on the XA-Core as trunk name "RTPG_BCM_LOCAL".
H323 RRQ rejected	Table LTDATA Needs H323 Option	Check the datafill in Table LTDATA on the CS 2100 Core. The option PRI_IP_PROT H323 should be present for the D-channel associated with the H.323 gateway.

Table 8
Actions associated with an H.323 failure (Sheet 3 of 4)

Specific problem	Description	Action
H323 RRQ rejected	Max Gateways Registered	No action needed. This log report is for information only. The CS 2100 Gateway Controller has reached the maximum limit for the number of H.323 gateways it can have registered simultaneously.
H323 ARQ rejected	B-channel Resource Unavailable	Ensure that B-channels associated with the gateway are idle (IDL) at the MAPCI, mtc, ttp, trks level on the CS 2100 XA-Core. This log can be cleared with a BSY/RTS of the B-channels associated with the H.323 gateway on the CS 2100 XA-Core. If all the B-channels associated with the H.323 gateway are call processing busy (CPB) at the MAPCI, mtc, ttp, trks level on the CS 2100 XA-Core, no action is needed. There is no B-channel available for the call. This log report is for information.
H323 RRQ rejected	No GWC Unit Active Running ***Note:*** A log with the same description will be generated if any RAS message (GRQ, RRQ, ARQ, URQ, DRQ) is received when the Gateway Controller unit is not actively running. This log can be cleared with a BSY/RTS of GWC unit.	Ensure that the CS 2100 Gateway Controller is in active running state. This log can be cleared with a BSY/RTS of GWC unit.
H323 DRQ rejected	Request to Drop Non Existent Call	No action needed. This log report is for information only. This reports a disengage request for a call which is not active or non-existent.
H323 URQ rejected	Endpoint Not Registered	A RAS request is received from a H.323 gateway which is not registered on the CS 2100 Gateway Controller. Verify that the H.323 gateway is provisioned on the CS 2100 Gateway Controller.
H323 Call rejected	Codec Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H.323 gateway matches the codec for the CS 2100 provisioned at the CS2000 Gateway Controller Manager.

Table 8
Actions associated with an H.323 failure (Sheet 4 of 4)

Specific problem	Description	Action
H323 Call rejected	Codec/Payload Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H.323 gateway matches the codec for the CS 2100 provisioned at the CS 2100 Gateway Controller Manager. Ensure that the payload (packetization) time on the H.323 gateway matches the payload (packetization) for the CS 2100 provisioned at the CS 2100 Gateway Controller Manager.
H323 Call rejected	H245 Tunneling Not Enabled On Gateway	Ensure that H.245 tunneling is enabled on the H.323 gateway.

Associated OM registers

This log report has no associated OM registers.

Additional information

This section provides examples of XA-Core logs relevant to the following:

- Specific problem: H323 RRQ rejected
- Description: D-Channel Out Of Service

The following are examples of XA-Core logs when the D-channel is manually busied (BSY):

```
RTPG * ISDN105 JUN16 21:45:44 2311 FLT PRA Sync Loss
   ISP = 0 GWC 11 PORT 0 CHNL 0

RTPG *** ISDN112 JUN16 21:45:44 2412 INFO PRA D-CHANNEL
   CRITICAL ALARM RTPG_BCM_LOCAL DCH=GWC 11 120 1: OOS

RTPG *** TRK103 JUN16 21:45:49 2917 FLT GROUP_ALARM
   RTPG_BCM_LOCAL 100% BUSY
```

Operational Measurements

The H.323 application uses the existing TRK2NET1 and TRKNET2 Operational Measurements (OMs). Use these TRK Operational Measurements to evaluate the performance of the H.323 application.

For more information, see the *Succession Performance Management Operational Measurements References,* NN10264-709.These manuals contain Operational Measurement (OM) descriptions for OM groups and registers applicable to Communication Server 2100 offices.

OM Group summary

The following sections provide a brief overview of the TRK2NET OM groups:

TRK2NET1

OM group Trunk to Network Group 1 (TRK2NET1) measures trunk group traffic for each bearer network. Registers in TRK2NET1 measure the following events for each trunk group:

- routing and seizure attempts
- seize failures
- total trunk use
- busy use

TRK2NET2 contains registers that are extensions of a subset of registers in TRK2NET1. OM groups TRK and TRNK2 provide traffic data summaries on a per-trunk group basis for all trunk groups in an office. TRK2NET1 and TRK2NET2 provide similar traffic data summaries with further refinement on a per-bearer network basis for each trunk group for all trunks groups in an office.

TRK2NET2

OM group Trunk to Network Group 2 (TRK2NET2) measures trunk group traffic for each bearer network. The group contains registers that are extensions of a subset of registers in TRK2NET1.

As with OM group TRK2NET1, set new office parameter MULTINET_DISPLAY_ACTIVE to “Y” to display TRK2NET2.

List of terms

APDU	Application Protocol Data Unit
API	Application Programming Interface
APM	Application Transport Mechanism
ARQ	AdmissionRequest (RAS message)
ASN.1	Abstract Syntax Notation 1
ASPEN	Automatic System for Performance Evaluation of the Network
BCM	Business Communications Manager (former name of Communication Server 200 or 400)
BRQ	BandwidthRequest (RAS message)
CallP	Call Processing
CLLI	Common Language Location Identification
CM	Computing Module
CMT	Communication Server 2000 Management Tools
CPE	Customer Premises Equipment
CS	Communication Server
CS 200	Communication Server 200 (previously called the Business Communications Manager)
CS 1000	Communication Server 1000
CS 2100	Communication Server 2100
CS LAN	Communication Server LAN
CSeq	Call Sequence
DNS	Domain Name System
DPT	Dynamic Packet Trunk
DRQ	DisengageRequest (RAS message)
DTMF	Dual-tone Multifrequency
EM	Element Manager

EMS	Element Management System
EPG	Endpoint Group
FTP	File Transfer Protocol
GCF	Gatekeeper Confirmation message
GRQ	Gatekeeper Request message
GUI	Graphical User Interface
GWC	Gateway Controller
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol, Secure
IEC	International Engineering Consortium
IE	Information Element
IEMS	Integrated Element Management System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCM	IP CLient Manager
IPSec	IP Security Protocol
IRQ	InfoRequest (RAS message)
IRR	InfoRequestResponse (RAS message)
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISUP	Integrated Services Digital Network User Part
ITU	International Telecommunication Union
JRE	Java Runtime Environment
JPI	Java Platform Interface
JWS	Java Web Start
LAN	Local Area Network. A network that connects computers to share data storage devices and printers.
MAP	Maintenance and Administration Position
MAPCI	Maintenance and Administration Position Command Interpreter
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
OAM&P	Operations, Administration, Maintenance and Provisioning

OM	Operational Measurement
OSS	Operations Support System
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
PRI	Primary Rate Interface
QoS	Quality of Service
RAS	Registration, Admission and Status
RFC	Request For Capability
RIP	Request in Progress (RAS message)
RRQ	RegistrationRequest (RAS message)
RTCP	Real-Time Control Protocol
RTP	Real-Time Protocol
SAM21	Service Application Module 21
SERVORD	Service Order
SFTP	Simple File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSPFS	Succession Server Platform Foundation Software
SWACT	Switch Activity
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TID	Terminal Identifier
TN	Terminal Number
TSAP	Transport Service Access Point
UDP	User Datagram Protocol
UUI	User-to-User Information
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

WAN	Wide Area Network
XML	Extensible Mark-up Language

Nortel Communication Server 2100

H.323

Service Implementation Guide

Publication number: 555-4031-904
Product release: SE08
Document release: Standard 01.03
Date: May 2005
Printed in the United States of America.

NORTEL