Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

IP Trunk

Description, Installation, and Operation

Document Number: 553-3001-363
Document Release: Standard 5.00
Date: July 2006

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Revision history

July 2006

Standard 5.00. This document is up-issued following the removal of outdated content.

August 2005

Standard 4.00. This document is up-issued following removal of regulatory data.

August 2005

Standard 3.00. This document is up-issued for Communication Server 1000 Release 4.5.

September 2004

Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: *IP Trunk: Description, Installation, and Operation* (553-3001-202).

Contents

Provisioning IP Trunk 3.01 (and later) in OTM 2.1 (and later) 375

OA&M using the ITG shell CLI and overlays 489

List of procedures

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This document describes how to engineer, install, configure, administer and maintain an IP Trunk 3.01 system.

IP Trunk 3.01 is an up-issue to the IP Trunk 3.0 and ITG Trunk 2.1 applications. It enhances Voice over Internet Protocol (VoIP) networking capability to and from other Meridian 1 and Business Communication Manager (BCM) systems and Communication Server (CS) 1000 systems.

> ***Note:*** Interoperability with other Nortel products and applications may exist, but has not been verified by the IP Trunk design group; for interoperability with other products, please refer to the customer documentation associated with those products.

IP Trunk 3.01 also enables networking with CS 1000 and CS 1000M systems running CS 1000 Release 4.0. (A CS 1000 system is a server-based, full-featured IP PBX, fully distributed over IP LAN/MAN/WAN networks.)

The IP Trunk 3.01 application, building on the approach in IP Trunk 3.0, provides a clean and easy way for customers to add a Meridian 1 system to a CS 1000 network composed of other Meridian 1 systems, BCM, CS 1000, or other supported endpoints.

IP Trunk 3.01 supports stand-alone Gatekeepers for Meridian 1 IE and BCM nodes when working in an environment that does not include Call Servers and Signaling Servers. It also supports an environment where the Gatekeeper is part of a CS 1000 network.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis (Meridian 1 PBX 11C Chassis)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)
- *Communication Server 1000E: Upgrade Procedures* (553-3041-258)

Conventions

Terminology

In this document, the following systems are referred to generically as “system”:

- Communication Server 1000S (CS 1000S)

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as “Small System”:

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as “Large System”:

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Features and Services* (553-3001-306)
- *Software Input/Output: Administration* (553-3001-311)
- *Software Input/Output: Maintenance* (553-3001-511)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview of IP Trunk 3.01

Contents

This section contains information on the following topics:

Introduction

The IP Trunk 3.01 (and later) software application is an Internet Telephony Gateway (ITG) trunk software application that maintains the functionality of ITG Trunk 2.x using Integrated Services Digital Network (ISDN).

IP Trunk 3.01 (and later) allows networks with Meridian 1 IP-enabled systems to add a CS 1000 system to the existing IP Telephony network. This increases the range of system options to provide enterprise-wide telephony services.

IP Trunk 3.01 (and later) provides call-routing flexibility and survivability. Even with a Signaling Server acting as a centralized authority for routing IP

Telephone calls, IP Trunk can make some call-routing decisions locally. This can be done for one of the following reasons:

- It can maintain at least a minimum level of service in the unlikely event that all Signaling Servers on the network are unreachable.
- It can maintain the existing functionality within a pre-existing ITG Trunk network that was upgraded to IP Trunk 3.01 (and later).

In addition to routing IP Telephony calls with locally configured call-routing options, IP Trunk 3.01 takes advantage of the centralized IP Telephony call routing of an H.323 Gatekeeper residing on a Signaling Server elsewhere on the network.

The H.323 Gatekeeper allows or denies access to IP network gateways. It also provides address analysis to find the destination gateway or device. A gateway is a device that translates circuit-switched signaling into H.323 signaling and translates circuit-switched bit stream user data into packetized user data to enable the data to be delivered across an IP network. IP Trunk 3.01 (and later) provides IP access between the Meridian 1/CS 1000M system and the IP network carrying voice traffic.

IP Trunk 3.01 (and later) interworks with ITG Trunk 2.x, but not with ITG Trunk 1.0. For ITG Trunk 1.0 to interwork with IP Trunk 3.01 (and later), upgrade ITG Trunk 1.0 to ITG Trunk 2.0. See “Upgrade an ITG Trunk 1.0 node to support ISDN signaling trunks” on page 621.

IP Trunk 3.01 (and later) interworks with a CS 1000S and CS 1000M system, which fulfils the role of a Gatekeeper. The Gatekeeper uses directly-routed calls. See “Directly-routed calls” on page 39. Using H.323 Registration and Admission Signaling (RAS), IP Trunk 3.01 (and later) registers with the Gatekeeper, if provisioned to do so. IP Trunk 3.01 (and later) then processes calls by scanning its directory number information and routes unresolved calls to the Gatekeeper.

For a Meridian 1 system to interwork with a CS 1000S or CS 1000M system, the following requirements must be met:

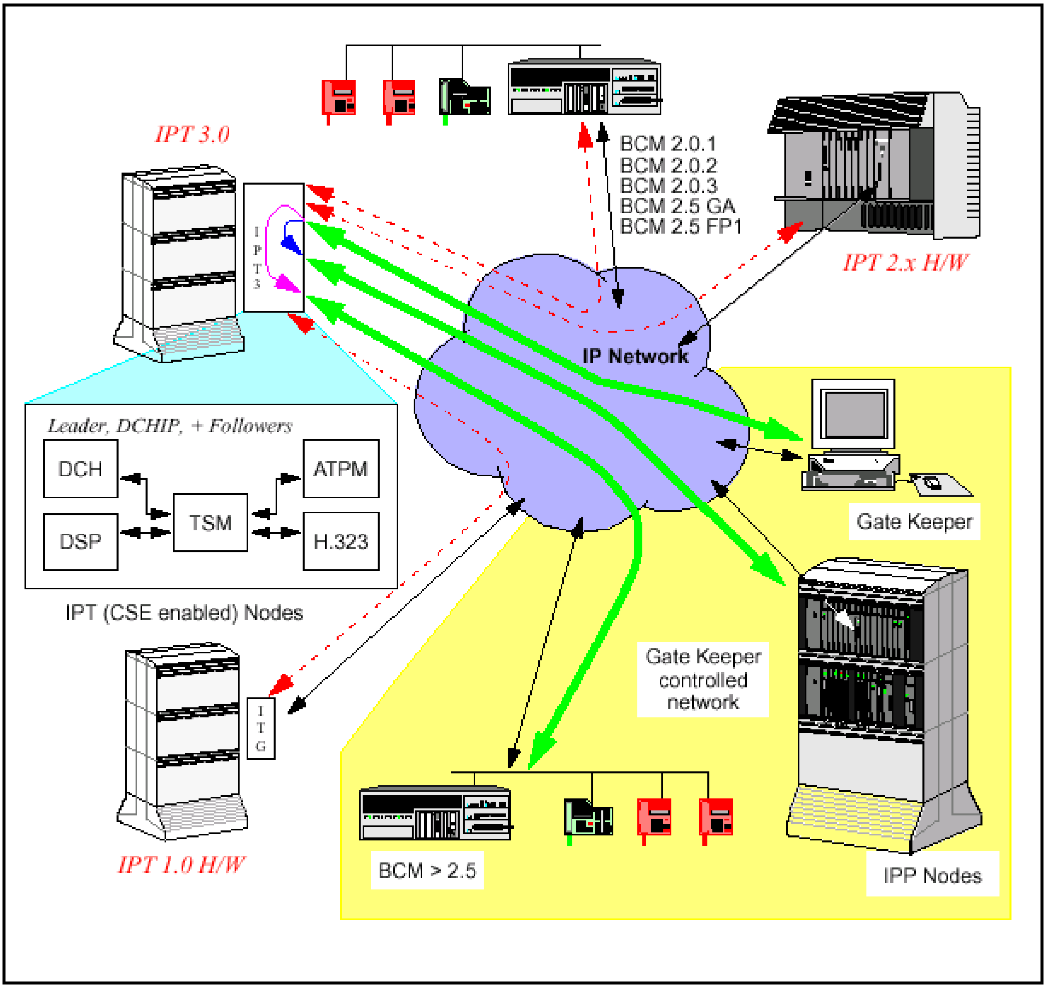
- The ITG-Pentium 24-port trunk card and the Media Card 32-port trunk card must be upgraded to IP Trunk 3.01 (and later) software. This upgrade supports MCDN features and Gatekeeper registration. As well as this document, see *Optivity Telephony Manager: System Administration* (553-3001-330) for more information on installing, upgrading, and upgrading IP Trunk 3.01 (and later) parameters.
- The IP Trunk 3.01 (and later) node must be configured to register with the CS 1000S or CS 1000M Gatekeeper. Refer to "Gatekeeper-resolved endpoints" on page 448 and to *Optivity Telephony Manager: System Administration* (553-3001-330) for more information on how to configure the IP Trunk 3.01 (and later) options.

IP Trunk 3.01 (and later) is subordinate to the Gatekeeper for all calls that require Gatekeeper intervention. This means that the IP Trunk 3.01 (and later) node performs the following actions:

- registers with the Gatekeeper
- requests admission
- accepts the reply
- handles the call based on the return message from the Gatekeeper

IP Trunk 3.01 (and later) accesses additional devices through the Gatekeeper. It is no longer necessary to individually provision the entire mesh at each IP Trunk 3.01 (and later) node. Instead, the calls go to the Gatekeeper, which provides the IP Trunk 3.01 (and later) application with the correct destination for the call. See Figure 1 on page 38.

Figure 1
IP Trunk 3.01 (and later) architecture



IP Trunk 3.01 (and later) uses the Meridian 1/CS 1000M core switch as the primary driver, which sends ISDN messages through the ISDN Signaling Link (ISL) to the IP trunk card for IP Trunk 3.01 (and later) processing. IP

Trunk 3.01 (and later) tandems the Meridian 1/CS 1000M core switch to the IP network, providing point-to-multipoint connection.

Alternatively, depending on the provisioning and the requested destination, if a call cannot be resolved locally, IP Trunk 3.01 (and later) can interwork with the Gatekeeper to identify the destination node before routing directly to that destination.

Two types of calls can be routed through interworking with the Gatekeeper: directly-routed calls and Gatekeeper-routed calls.

WARNING

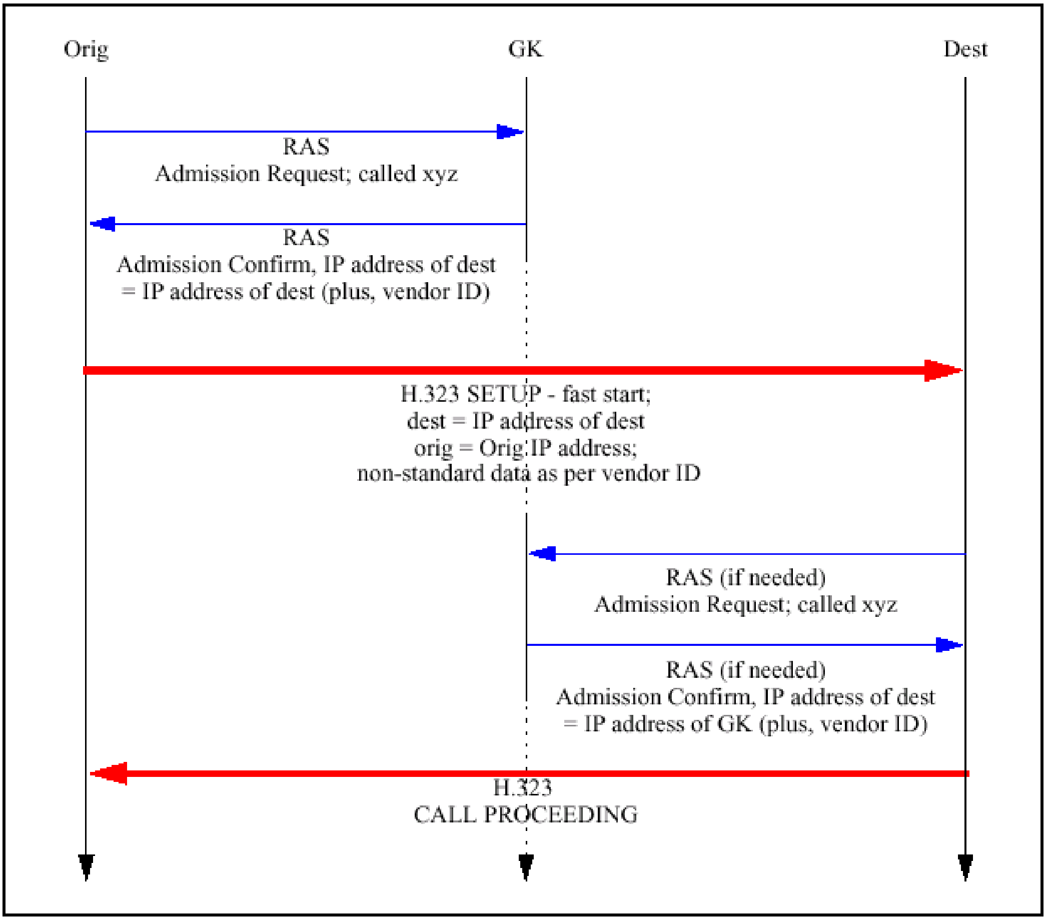
The only Gatekeeper that IP Trunk 3.01 (and later) officially supports is the CS 1000S or CS 1000M Gatekeeper. Gatekeeper calls made between the CS 1000S or CS 1000M system and IP Trunk 3.01 (and later) are directly-routed calls.

Directly-routed calls

In directly-routed calls, the Gatekeeper returns the IP address of the call's actual destination.

Figure 2 on page 40 represents a directly-routed call. Once the destination IP address is obtained, the originator sends the call directly to the destination node.

Figure 2
Directly-routed call

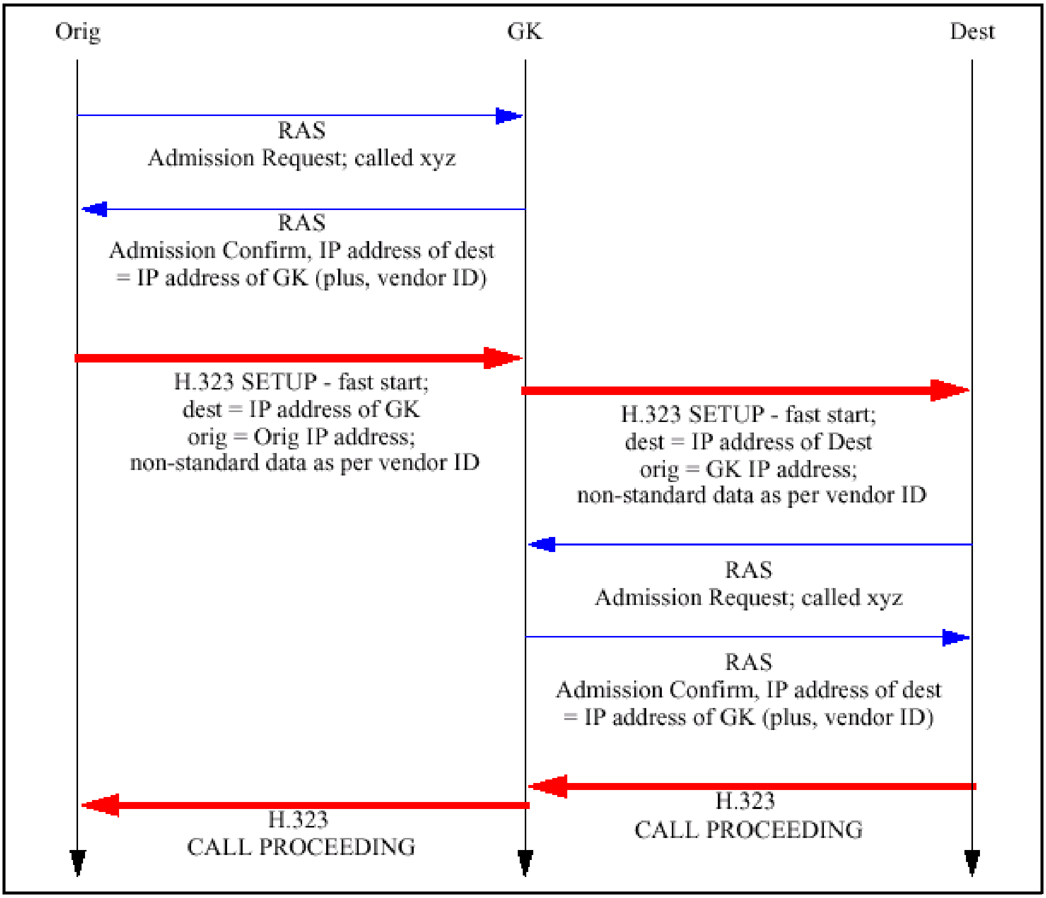

Orig
GK
Dest
RAS
Admission Request; called xyz
RAS
Admission Confirm, IP address of dest
= IP address of dest (plus, vendor ID)
H.323 SETUP - fast start;
dest = IP address of dest
orig = Orig IP address;
non-standard data as per vendor ID
RAS (if needed)
Admission Request; called xyz
RAS (if needed)
Admission Confirm, IP address of dest
= IP address of GK (plus, vendor ID)
H.323
CALL PROCEEDING

Gatekeeper-routed calls

In Gatekeeper-routed calls, the Gatekeeper returns the Gatekeeper's IP address and port as both the destination for the originating call and the originator for the destination, rather than the end-point address and port.

Figure 3 represents a Gatekeeper-routed call. The destination IP address provided by the Gatekeeper is the Gatekeeper's IP address. All messages are routed through the Gatekeeper.

Figure 3
Gatekeeper-routed call


Orig
GK
Dest
RAS
Admission Request; called xyz
RAS
Admission Confirm, IP address of dest
= IP address of GK (plus, vendor ID)
H.323 SETUP - fast start;
dest = IP address of GK
orig = Orig IP address;
non-standard data as per vendor ID
H.323 SETUP - fast start;
dest = IP address of Dest
orig = GK IP address;
non-standard data as per vendor ID
RAS
Admission Request; called xyz
RAS
Admission Confirm, IP address of dest
= IP address of GK (plus, vendor ID)
H.323
CALL PROCEEDING
H.323
CALL PROCEEDING

Startup and registration

On system startup, the IP Trunk 3.01 (and later) Leader card is established, based on whether the primary and backup Leaders come up, in what sequence, and how quickly. This operation remains unchanged from prior releases. It provides all necessary information to the follower cards.

Part of the information in the Dial Plan table is the Gatekeeper registration information, which includes three main fields: the local node H.323 identifier (node name), a flag indicating registration handling, and a third field for future development.

The registration handling has two potential flag values as follows:

- 0 – Register the IP addresses of all cards (Leader 0, Leader 1, and Follower cards) in the IP Trunk 3.01 (and later) node.
- 1 – Each card must register individually, if required. When registering with a CS 1000S or CS 1000M Gatekeeper, IP Trunk 3.01 (and later) registers only the node address. No other IP addresses are sent to the Gatekeeper in the Registration Request (RRQ) message.

  Note: The flag value is ignored when the provisioned Gatekeeper is a CS 1000S or CS 1000M Gatekeeper.

On startup, if the IP Trunk 3.01 (and later) Leader is provisioned to use a Gatekeeper, it seeks out and locates the Gatekeeper using RAS signalling and then registers with the Gatekeeper using an RRQ. As part of the registration process, the IP Trunk 3.01 (and later) Leader registers using the registration handling flag to determine how to proceed.

The Gatekeeper and IP Trunk 3.01 (and later) re-register on a regular basis, based on the Time To Live (TTL) configured for the IP path.

> ***Note:*** The Gatekeeper is the final authority on the TTL values. The Gatekeeper can override the provisioned value of IP Trunk 3.01 (and later) and require the IP Trunk 3.01 (and later) gateway to change its TTL value to match that required by the Gatekeeper.

Depending on the Gatekeeper type (for example, Gatekeepers other than CS 1000S or CS 1000M), if the Gatekeeper flag in the dial plan file indicates the need for multiple IP Trunk 3.01 card IP addresses (flag value = 0), the **RRQ** includes all IP addresses for the node. These additional IP addresses are reserved exclusively for calls to the Gatekeeper. By sending all the IP addresses in the RRQ, the Gatekeeper is able to determine the origin of the admission requests. These addresses are used when the Gatekeeper considers the **endpointIdentifier** sent to the gateway in the RRQ confirmation to be insufficient to confirm that the Admission Request (**ARQ**) belongs to a gateway registered with that Gatekeeper. The Gatekeeper rejects any ARQ from an unknown end-point.

> ***Note:*** CS 1000S or CS 1000M require an **endpointIdentifier** match and does not care about the IP addresses. Therefore, the Gatekeeper flag is unnecessary for CS 1000S or CS 1000M.

On startup, the message flow between the IP trunk card serving as the IP Trunk 3.01 (and later) Active Leader and the Gatekeeper is as follows:

1. **Gatekeeper Request (GRQ)** – From the Active Leader to the Gatekeeper, using the provisioned Gatekeeper IP address. The Optivity Telephony Manager (OTM) configuration indicates where the IP Trunk 3.01 (and later) node must look for its Gatekeeper, but this is not necessarily the actual Gatekeeper address the node uses for call processing.

   Some Gatekeepers use a “virtual IP address” to screen the fact that the Gatekeeper with which the gateway registers has internal standby controllers. In this case, the request might go to a Gatekeeper server that determines the correct virtual IP address. The Gatekeeper’s internal Message Forwarding process sends the messages to the current active Gatekeeper node.

   Note: CS 1000S or CS 1000M do not require a Gatekeeper Request from IP Trunk 3.01 (and later); therefore, no Request or Confirm is sent.

2. **Gatekeeper Confirm (GCF) –** From the Gatekeeper to the Active Leader, with the functional Gatekeeper IP address. This address is used for all call control messaging and registration messages between the IP Trunk 3.01 (and later) cards and the Gatekeeper.

3 **Gatekeeper Registration Request (RRQ)** – From the Active Leader to the Gatekeeper, with all of the node's IP addresses.

Note: IP addresses are only sent if required. CS 1000S or CS 1000M do not require all IP addresses, so the IP addresses are not sent.

4 **Gatekeeper Register Confirm (RCF)** – From the Gatekeeper to the Active Leader, providing the TTL prior to a re-registration attempt by the leader and indicating under what conditions admission requests are needed.

Typically, the TTL is in minutes. The default IP Trunk 3.01 (and later) value, if no response from the Gatekeeper is received, is 300 seconds. However, the Gatekeeper can enforce a shorter interval in seconds or tens of seconds. The standards allow seconds from 1 to (2^{32}) –1.

Recommendation

Nortel recommends that the TTL be provisioned in the 30- to 60-second range.

The IP Trunk 3.01 (and later) node must perform a "keep-alive" re-registration prior to the expiry of the timer on the Gatekeeper. When the Gatekeeper timer expires, a full registration is needed.

IP Trunk 3.01 (and later) and CS 1000S/CS 1000M

The CS 1000S or CS 1000M systems use virtual trunking (IP Peer Networking) to inter-operate with the IP Trunk 3.01 (and later) nodes. However, the CS 1000S or CS 1000M can be a Gatekeeper for the system.

When IP Trunk 3.01 (and later) is part of a network with a Signaling Server acting as a central control point, it is able to take partial advantage of a feature known as IP Peer Networking. IP Peer Networking eliminates the multiple conversions between IP and non-IP circuits, increasing call routing efficiency and overall voice quality. Many calls involving an IP Peer endpoint and one or more IP Trunk endpoints can use this capability. However, calls that use only IP Trunk facilities, and a small subset of calls involving both IP Trunk and IP Peer, cannot obtain this benefit.

IP Trunk 3.01 (and later) supports Gatekeeper Registration and Admission Signaling (RAS) and Call Admission Signaling. IP Trunk 3.01 (and later) interworks with CS 1000S or CS 1000M, which fulfills the role of a Gatekeeper. Using H.323 RAS, IP Trunk 3.01 (and later) uses RAS Messaging to register with the Gatekeeper if provisioned to do so. IP Trunk 3.01 (and later) then processes calls by scanning its Directory Number (DN) information. If the call is not resolved using the local Address Translation Protocol Module (ATPM) and IP Trunk 3.01 (and later) is registered with a Gatekeeper, then IP Trunk 3.01 (and later) routes the call to the Gatekeeper.

Administrators use OTM 2.1 (and later) to configure the IP address of a CS 1000S or CS 1000M node with a capability of “CS 1000S” in the ATPM dialing plan table. This enables the IP Trunk 3.01 (and later) node to directly call the CS 1000S or CS 1000M node.

The IP Trunk 3.01 (and later) node is subordinate to the Gatekeeper for all calls requiring the Gatekeeper. The IP Trunk 3.01 (and later) node registers with the Gatekeeper according to H.323 protocol, requests admission, accepts the reply according to H.323 protocol, and handles the call based on the returned message from the Gatekeeper.

A CS 1000S or CS 1000M node consists of two components:

- Call Server – used for call control of CS 1000S or CS 1000M gateways
- Signaling Server – used for protocol analysis

The CS 1000S/CS 1000M Gatekeeper accepts the registration of multiple IP trunk cards implicitly in a single **RRQ**. This means that all Follower cards are registered at the same time as the Leader card, because the CS 1000S/CS 1000M node returns an **endpointIdentifier** assigned by the Gatekeeper to that node. Later, a request to establish a call to a Gatekeeper-controlled endpoint receives in the response the **enpointIdentifier** of the endpoints that was provided at registration.

> ***Note:*** The CS 1000S/CS 1000M gateways interwork with the IP Trunk 3.01 (and later) gateway resident function which generates the FACILITY redirect. The FACILITY redirect is used when calls terminate at an IP Trunk 3.01 (and later) node. The CS 1000S/CS 1000M gateways do not use this redirection themselves.

Other Gatekeepers accept the FACILITY redirect and registration of multiple IP trunk cards in a single RRQ; that is, the Followers are registered with, and at the same time as, the Leader.

IP Trunk 3.01 (and later) interworks with the CS 1000S/CS 1000M systems and IP Peer Networking. As CS 1000S/CS 1000M and IP Peer Networking use MCDN only, the only applicable protocol is MCDN. IP Trunk 3.01 (and later) uses the "interoperability format" of the non-standard data with IP Peer Networking and all other gateways accessible through CS 1000S/CS 1000M.

When IP Trunk 3.01 (and later) inter-operates with itself, with ITG Trunk 2.x.25, or with BCM 2.5 FP1, the IP Peer Networking CS 1000S/CS 1000M Gatekeeper is not required. The existing ITG Trunk 2.1 node-based dialing plan is converted automatically to IP Trunk 3.01 (and later) by OTM 2.1 (and later).

There are no direct media paths between the Meridian 1 telephones and the CS 1000S/CS 1000M telephones. There are direct paths between the IP Trunk 3.01 (and later) IP trunk cards and the CS 1000S/CS 1000M telephones.

Loss plans and pad values

When the IP Trunk card is in a CS 1000 system, it can take advantage of the Dynamic Loss Plan developed for the IP Peer product. This allows the system core to inform the IP Trunk card of the correct pad levels to be used. As with IP Peer, it also allows the creation of a custom table when the environment requires one.

When using Dynamic Loss Plan, the node must be provisioned to have a default loss plan pad of 0 in both the transmit and receive directions. This allows a 0 transmit and receive level when the IP Trunk has a tandem to another trunk device, improving voice quality.

Codec selection

A CS 1000S/CS 1000M network is generally designed for use with a G.711 Codec. In cases where minimizing bandwidth usage in a CS 1000S/CS 1000M network is a consideration, G.729 might be used.

Recommendation

Nortel recommends provisioning G.711 Codec in IP Trunk 3.01 (and later) and in all other network equipment to facilitate communication with CS 1000S/CS 1000M.

IP Trunk 3.01 (and later) requirements

IP Trunk 3.01 requires a minimum of Release 25.15 software. To interwork with the CS 1000S/CS 1000M Gatekeeper, CS 1000 Release 3.0 software (or later) is required.

Package requirements

Table 2 on page 48 lists the package requirements for the IP Trunk 3.01 (and later) application.

Note: Unlike ITG Trunk 2.0, Q-Signaling protocol (QSIG) support is not required in IP Trunk 3.01 (and later), though it is available for Large Systems. CS 1000S, Meridian 1 Option 11C Cabinet, CS 1000M Cabinet, Meridian 1 PBX 11C Chassis, and CS 1000M Chassis do not support QSIG signaling. Therefore, the Multi-purpose Serial Data Link (MSDL), applicable only to Large Systems, is recommended but not mandatory; the earlier D-channel interface cards can provide Meridian Customer Defined Network (MCDN) ISDN Signaling Link (ISL). QSIG and MSDL are incompatible for feature transport. If both QSIG and MSDL are configured on the network, this can cause the loss of features such as Name Display, Ring Again, and Transfer Notification and subsequent path simplification operations.

Table 2
IP Trunk 3.01 (and later) package requirements (Part 1 of 2)

Package Name	Package Number	Package description	Comments
BARS	57	Basic Alternate Route Selection	Package 57 and/or 58 is required.
NARS	58	Network Alternate Route Selection	Package 57 and/or 58 is required.
CDP	59	Coordinated Dialing Plan	Required if Dialing Plan used. If the configuration restricts NARS, use CDP to obtain private network dialing. CDP can also co-exist with NARS.
ISDN	145	ISDN Base	Mandatory. No D-channel can exist without this package.
ISL	147	ISDN Signaling Link	Mandatory. ISL cannot exist without this package. Without ISL, the Meridian 1/CS 1000M to IP Trunk D-channel cannot be provisioned.
NTWK	148	Advanced ISDN Network Services	Required if Networking Services used.

Table 2
IP Trunk 3.01 (and later) package requirements (Part 2 of 2)

Package Name	Package Number	Package description	Comments
FNP	160	Flexible Numbering Plan	Required if Dialing Plan used. When the configuration allows CDP, FNP is recommended, but not mandatory.
MSDL	222	Multipurpose Serial Data Link	Recommended for MSDL on Large systems.

OTM 2.1

OTM 2.1 (or later) is required to configure and maintain IP Trunk 3.01 (and later).

Interoperability with the ITG 8-port trunk card

Telephone calls can be made between IP Trunk 3.01 (and later) and ITG Trunk 2.x.

System description

Contents

This section contains information on the following topics:

IP Trunk 3.01 (and later) application

IP Trunk 3.01 (and later) supports ISDN Signaling Link (ISL) IP trunks on the Media Card 32-port trunk card and the ITG-Pentium 24-port trunk card.

> ***Note:*** The NTCW80 8-port trunk card cannot be upgraded to IP Trunk 3.01 (and later).

An ISDN Signaling Link D-Channel (ISL DCH) provides DCH connectivity to the system and signaling control for the ports on the IP trunk card and any additional ports on other IP trunk cards in the same node. The DCH connection expands the signaling path between the Meridian 1/CS 1000M and the gateway. IP Trunk 3.01 (and later) allows Meridian 1/CS 1000M systems to be networked using ISDN, while transmitting H.323 signaling and voice over a standard IP protocol stack.

IP Trunk 3.01 (and later) compresses voice and demodulates Group 3 Fax. IP Trunk 3.01 (and later) then routes the packetized data over a private IP network.

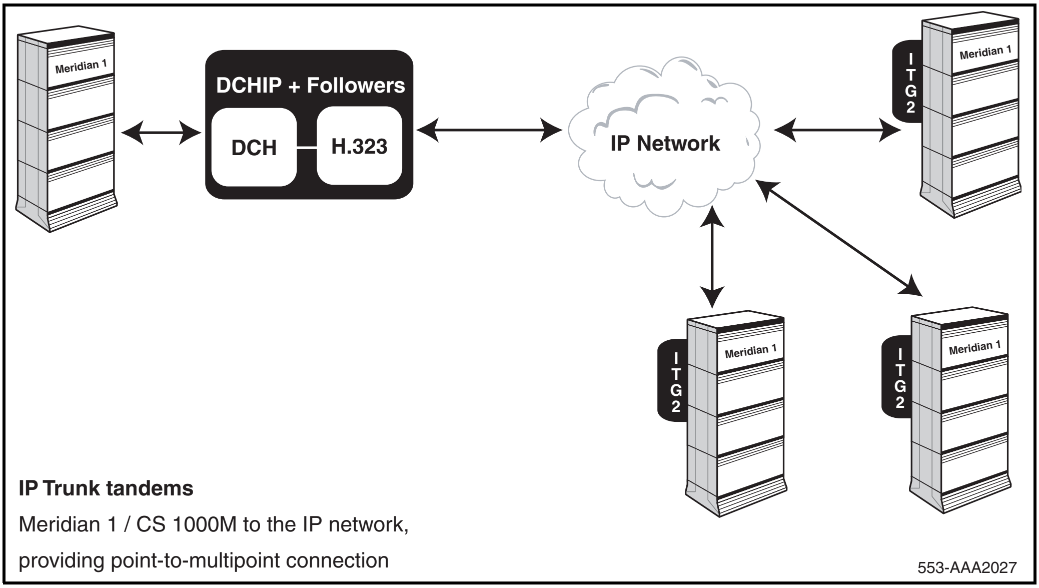
IP Trunk 3.01 (and later) delivers an ISDN signaling interface between the Meridian 1 and the Voice (and fax) over IP (VoIP) interface. The high signaling bandwidth of this ISDN interface expands the feature functionality for VoIP trunks. It provides, for example, Calling Line Identification (CLID) and Call Party Name Display (CPND).

To install IP Trunk 3.01 (and later), the customer must have a corporate IP network with managed bandwidth capacity, and routers available for WAN connectivity between networked Meridian 1/CS 1000 systems. The best VoIP performance is obtained with a QoS-managed network.

The LAN connection of IP Trunk 3.01 (and later) requires 10BaseT or 100BaseTX Ethernet network interfaces for voice (TLAN network interface) and 10BaseT for management and D-Channel signaling (ELAN network interface). There is no restriction on the physical medium of the WAN. Non-compressing G.711 codecs require 100BaseT Ethernet network connectivity. A 10/100BaseT auto-sensing Ethernet network interface routes the voice traffic from the IP trunk cards (TLAN subnet). Signaling between cards and communication with the Optivity Telephony Manager (OTM) 2.1 PC is transmitted over a 10BaseT Ethernet connection (ELAN subnet). The OTM 2.1 (and later) application manages IP Trunk 3.01 (and later).

Figure 4 shows an IP Trunk 3.01 (and later) configuration example.

Figure 4
IP Trunk 3.01 (and later) connectivity



> ***Note:*** In this document, TLAN subnet refers to the Telephony LAN subnet that transmits the ITG voice and fax traffic. ELAN (Embedded LAN) subnet refers to the management and signaling LAN subnet for the system site.

IP Trunk 3.01 (and later) depends on the managed IP network, not the internet, because the managed IP network can provide adequate latency, jitter, and packet loss performance to support VoIP with an acceptable voice quality.

System requirements

The Media Card 32-port trunk card and the ITG-Pentium 24-port trunk cards are able to reside in any of the following Meridian 1/CS 1000M systems running CS 1000 Release 4.0 software:

- Small Systems
- Large Systems

IP Trunk 3.01 requires OTM 2.1 (and later).

Customers must have the NTAK02BB (minimum vintage) SDI/DCH card (Small Systems) or MSDL card (Large Systems) for ISDN Signaling capability. If the customer does not have either of these cards, or does not have an available DCH port on them, the customer must order these cards to support ISDN functionality. Earlier vintages are not supported, as the level of MCDN functionality required to support ITG-compatible ISL is not available on earlier vintages.

Install a modem router on the ELAN subnet to provide remote support access for IP Trunk 3.01 (and later) and other IP-enabled Nortel products. The Nortel Netgear RM356 modem router integrates the functions of a V.90 modem, a PPP remote access server, an IP router, and a 4-port 10BaseT Ethernet hub, and provides a range of security features that must be configured to comply with the customer's data network security policy. The Netgear RM356 modem router can be ordered through many electronic equipment retail outlets.

Table 3 lists the required software packages.

Table 3
Software packages for Meridian 1/CS 1000M IP Trunk 3.01 (and later)

Package	Package number	Notes
Basic Alternate Route Selection (BARS) or Network Alternate Route Selection (NARS)	57 or 58	Required
ISDN Base (ISDN)	145	Required
ISDN Signaling Link (ISL)	147	Required
MSDL	222 (Large Systems)	Required
QSIG Interface (QSIG) (see Note)	263 (Large Systems)	Optional
QSIG GF Transport (QSIG GF) (see Note)	305 (Large Systems)	Optional
Advanced ISDN Network Services (NTWK)	148	Optional
Coordinated Dialing Plan (CDP).	59	Optional
Flexible Numbering Plan (FNP)	160	Optional
Note: Nortel recommends that MCDN, not QSIG, be used on all IP Trunk 3.01 (and later) systems. Only MCDN is supported for interworking with CS 1000S and CS 1000M		

Hardware components for IP Trunk 3.01 (and later)

New installations use the Media Card 32-port trunk card. Table 4 lists the hardware components required for new installations.

Table 4
Hardware components for the Media Card 32-port trunk

Component	Product code
The package includes the following: • NTVQ90 – Media Card 32-port trunk card • NTVQ83 ITG EMC Shielding Kit • NTAG81 PC Maintenance cable • NTAK19 Shielded 4-port SDI/DCH cable for NTAK02 card • NTND26 DCHI Interface cable for MSDL • NTCW84 Meridian 1 Backplane to 50-pin I/O Panel Mounting connector with IP Trunk-specific filtering • 50-pin I/O connector – A0852632 • NTVQ80 DCHIP kit for Media Card 32-port trunk card which includes the following; – NTWE07 C7LIU D-Channel PC Card – NTMF29 DCHIP to SDI card assembly cable – NTWE04 Inter Cabinet cable (1 ft) – Support Bracket Retaining Cable and screws • NTMF405 IP Trunk 3.01 (and later)/Voice Gateway Compact Flash • Shielded 50-pin key telephone to 9D Sun and Twin RJ-45 Adapter • NTVQ61 IP Trunk 3.01 (and later) NTP CD-ROM – Multilingual	NTVQ91BA

IP Trunks with the D-Channel PC Card kit require NTAK11xD Cabinets or the Cabinet Upgrade Kit NTDK18AA.

For extra components, such as longer cables required for a Large System, see Table 5 on page 58, which lists all extra components used by both IP trunk cards. See Appendix A on page 571 for more information on some of the cables and connections.

> ***Note 1:*** OTM 2.1 (and later) is a prerequisite and must be ordered separately.
>
> ***Note 2:*** Nortel Netgear RM356 Modem Router or equivalent is required for remote support and must be ordered separately from retail outlets.
>
> ***Note 3:*** Inspect the IPE module to determine if it is equipped with non-removable Molded Filter Connectors on the I/O Panel. For Large Systems manufactured during the period of 1998-1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon cable assembly with a non-removable Molded Filter Connector. If the TLAN subnet connection is 10BaseT use the NT8D81BA Backplane to I/O Panel ribbon cable assembly, for a 100BaseT connection use the NT8D81AA ribbon cable.

Table 4 lists the hardware components included in the IP Trunk 3.01 (and later) packages for new installations.

Table 5 lists the extra components used by both the Media Card 32-port trunk card and the ITG-Pentium 24-port trunk cards.

Table 5
Extra components for IP Trunk 3.01 (and later) trunk cards (Part 1 of 2)

Component	Product codes
MSDL DCH cable (included in Large System package): 6 ft 18 ft 35 ft 50 ft	 NTND26AA NTND26AB NTND26AC NTND26AD
50 ft MSDL DCH Extender cable	NTMF04AB
10 ft Inter cabinet cable NTCW84KA to SDI/DCH cable	NTWE04AC
1 ft Intra cabinet cable NTCW84KA to SDI/DCH cable	NTWE04AD

Table 5
Extra components for IP Trunk 3.01 (and later) trunk cards (Part 2 of 2)

Component	Product codes
Shielded four-port SDI/DCH cable for the NTAK02BB SDI/DCH card (included in Small System package)	NTAK19FB
PC Maintenance cable (for faceplate RS-232 maintenance port to local terminal access)	NTAG81CA
Maintenance Extender cable	NTAG81BA
Large Systems filter connector	
50 pin I/O Panel Filter Connector Block with ITG specific filtering for 100BaseTX (included in Large Systems package)	NTCW84JA
Backplane to I/O Panel ribbon cable assembly compatible with NTCW84JA I/O Panel Filter Connector Block with ITG-specific filtering for 100BaseTX TLAN subnet connection (replaces NT8D81BA Backplane to I/O Panel ribbon cable assembly equipped with non-removable Molded Filter Connectors)	NT8D81AA
Documentation	
IP Trunk 3.01 (and later) NTP CD-ROM – Multilingual	NTVQ61BA
PC Cards	
C7LIU DCH PC Card with Layer 2 DCH Software	NTWE07AA

Ordering rules and guidelines

IP Trunk 3.01 (and later) can be ordered as a VoIP trunk gateway with 32 ports, or as a software upgrade on an existing VoIP trunk gateway on the Media Card 32-port trunk card or ITG-Pentium 24-port trunk card. One IP Trunk card in the system must be equipped with a D-Channel PC Card kit. One kit supports 12 Media Card 32-port trunk or 16 ITG-Pentium 24-port trunk card with a maximum of 382 total ports.

Ordering rules for an IP Trunk 3.01 (and later) node

Initial configuration of an IP Trunk 3.01 (and later) node requires one NTVQ01BB IP Trunk 3.01 Small and Large Systems 32-port package with DCHIP as appropriate for the system. These packages include all components needed for a single-card node, except for the cables that provide interface to the MSDL and SDI/DCH cards. The following DCH interface cables are included:

- NTND26AA (Large Systems)
- NTAK19FB and NTWE04AD (Small Systems)

The following packages are required for IP Trunk 3.01 (and later):

- ISDN Base (ISDN) package 145
- ISDN Signaling Link (ISL) package 147

OTM 2.1 (and later) is required and must be ordered separately.

For MSDL and DCHIP cards that reside in the same Large System UEM equipment row, order:

- NTND26 MSDL DCH cable in sufficient length to reach from the MSDL to the I/O Panel of the IPE module that contains the DCHIP

For MSDL and DCHIP cards that reside in different Large System Universal Equipment Modules (UEM) equipment rows in a multi-row Large System, order:

- NTMF04BA MSDL DCH Extender (50 ft.) cable to reach between the I/O Panels of the two UEM equipment rows

For SDI/DCH and DCHIP cards that reside in different Small System cabinets, order:

- NTWE04AC Inter-cabinet cable (NTCW84KA to SDI/DCH cable-10 ft)

If IP trunk cards are being installed in IPE modules equipped with NT8D81BA Backplane to I/O Panel ribbon cable assembly with Molded Filter Connectors, on a 100BaseTX TLAN subnet connection, order:

- NT8D81AA Backplane to I/O Panel ribbon cable assembly compatible with NTCW84JA Filter Connector Block with ITG-specific filtering for 100BaseTX TLAN subnet connection

  Note: Inspect the IPE module to determine if it is equipped with Molded Filter Connectors on the I/O Panel. Molded Filter Connectors were shipped in North America during a period from 1998 to 1999. Molded Filter Connectors can be used with 10BaseT TLAN subnet connections.

Ordering rules for IP Trunk 3.01 (and later) node expansion

To expand an IP Trunk 3.01 (and later) node, the following are required:

- For each additional non-DCHIP card:
  - — one NTVQ92AA IP Trunk 3.01 (and later) Small and Large Systems 32-port expansion package (without DCHIP)
- For each additional DCHIP card:
  - — one IP Trunk 3.01 (and later) Small and Large Systems 32-port package with DCHIP

Sparing ratios for IP Trunk 3.01 (and later) components

Sparing ratios for selected components are listed in Table 6.

Table 6
Sparing ratios (Part 1 of 2)

Component	Sparing ratio
NTVQ92AA IP Trunk 3.01 (and later) Small and Large Systems 32-port expansion package (without DCHIP) (for repair only -- no RTU license)	10:1

Table 6
Sparing ratios (Part 2 of 2)

Component	Sparing ratio
“NTVQ91VA IP Trunk 3.01 (and later) Small and Large Systems 32-port package with DCHIP	10:1
I/O cable assemblies	20:1

IP trunk card description

The Media Card 32-port trunk card and ITG-Pentium 24-port trunk card provide a cost-effective solution for high-quality voice and fax transmission over an IP network.

The IP Trunk cards are an IPE-based assembly designed for installation in a Meridian 1/CS 1000M IPE shelf.

A Media Card 32-port trunk card occupies one slot and can have a maximum of 32 ports. The ITG-Pentium 24-port trunk card is a two-slot trunk card and can have a maximum of 24 ports. On the ITG-Pentium 24-port trunk card, a Peripheral Component Interconnect (PCI)-based Digital Signal Processing (DSP) daughterboard provides voice processing and supplies the packets to the IP Trunk 3.01 (and later) network using a Pentium host processor. The Media Card 32-port trunk card has the DSP connected to the main assembly. This main assembly is what compresses speech into packets and supplies the packets to the IP Trunk 3.01 (and later) network using an Intel StrongARM (SA) processor.

The IP trunk cards monitor the IP network for delay (latency) and packet loss between other IP trunk cards. The card re-routes new calls to the alternate circuit-switched trunk routes if the Quality of Service (QoS) of the data network is not acceptable. Customers can configure QoS parameters on the IP trunk cards to ensure that the IP Trunk 3.01 (and later) trunk route is not used for new calls if the network QoS degrades below an acceptable level. QoS monitoring is not available for Gatekeeper-routed endpoints such as the CS 1000S and CS 1000M.

8051 XAController firmware

The XAController firmware is delivered through the following formats:

- ITGPFW57.BIN - 8051 XAController firmware for the ITG-Pentium 24-port trunk card
- SMCFW67.BIN - 8051 XAController firmware for the Media Card 32-port trunk card NTVQ01BA

Table 7 gives the firmware compatibility for the Media Card 32-port trunk card.

Table 7
Firmware compatibility matrix for the Media Card 32-port trunk card

Firmware version	NTVQ01BA	NTVQ01BB
6.7	Compatible	Not compatible
8.0	Not compatible	Compatible

NTVQ01BB Media Card 32-port trunk cards are factory-programmed with Release 8.0 firmware. Any firmware feature upgrades are available on the Nortel website.

Download this firmware from the Customer Support Software page. Go to www.nortel.com. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support

Card roles

The Media Card 32-port trunk card and ITG-Pentium 24-port trunk card can have one or more of the following roles:

- Follower
- Active Leader
- Backup Leader
- D-channel IP gateway (DCHIP)

The card roles identify which systems are active systems/standby systems and which are client systems. The Active Leader has a Node IP address on the voice interface. This node IP is an alias IP which is added to the original IP address on the voice interface. Other machines in the network use the Node IP to keep track of the Active Leader.

Each Meridian 1/CS 1000M is usually configured with the following:

- one IP trunk card that acts as an Active Leader
- one IP trunk card that acts as a Backup Leader
- at least one IP trunk card that provides DCHIP functionality
- one or more IP trunk cards identified as Followers

In the OTM 2.1 (and later) ITG application, the term Leader 0 refers to the IP trunk card initially configured to perform the role of the Active Leader. The term Leader 1 refers to the IP trunk card that is initially configured to perform the role of Backup Leader. The Active Leader and Backup Leader exchange the Node IP address when the Active Leader goes out-of-service. The term Active Leader indicates the Leader 0 or the Leader 1 card that is performing the Active Leader role.

Leader 0 or Leader 1 can have Active Leader status. On system power-up, Leader 0 normally functions as the Active Leader and Leader 1 as the Backup Leader. At other times, the Leader card functions reverse, with Leader 1 working as the Active Leader and Leader 0 working as the Backup Leader.

The Leader, Backup Leader, Follower, and DCHIP cards communicate through their ELAN network interfaces. For more information, see “Internet Protocols and ports used by IP Trunk 3.01 (and later)” on page 179.

Follower

A Follower card is a Media Card 32-port trunk card and/or an ITG-Pentium 24-port trunk card which converts telephone signals into data packets and data packets into telephone signals. For outgoing calls, Follower cards provide dialed number-to-IP address translation.

Active Leader

The Active Leader card is an IP trunk card that acts as a point of contact for all other Meridian 1/CS 1000 systems in the network.

The Active Leader card is responsible for the following:

- distributing incoming H.323 calls to each registered Follower card in its node and balancing load among the registered cards for incoming IP calls
- IP addresses for other cards in its node (see "Interactions among card functions" on page 70)
- serving as a time server for all IP trunk cards in its node
- performing network monitoring for outgoing calls in its node
- voice processing

All calls from a remote VoIP gateway node are first presented to the Active Leader card. The Leader card maintains a resource table of all the IP trunk cards in its node. The Active Leader card consults its internal IP trunk card resource table to determine which card has the most idle channels and is the least busy. Based on that information, the Active Leader card selects the card to receive the new call.

In a multi-card IP Trunk 3.01 (and later) node, the Active Leader is busier than the Follower cards. As a result, the channels on the Follower cards are used first. Only after most of the channels on the Follower cards and Backup Leader card are in use does the Active Leader card assign an incoming call to itself.

After a channel on a card has been selected, the Active Leader sends a message to the selected IP trunk card telling it to reserve a channel for the new call. The Active Leader redirects the call to the selected IP trunk card. All subsequent messages are sent directly from the remote VoIP gateway node to the selected card.

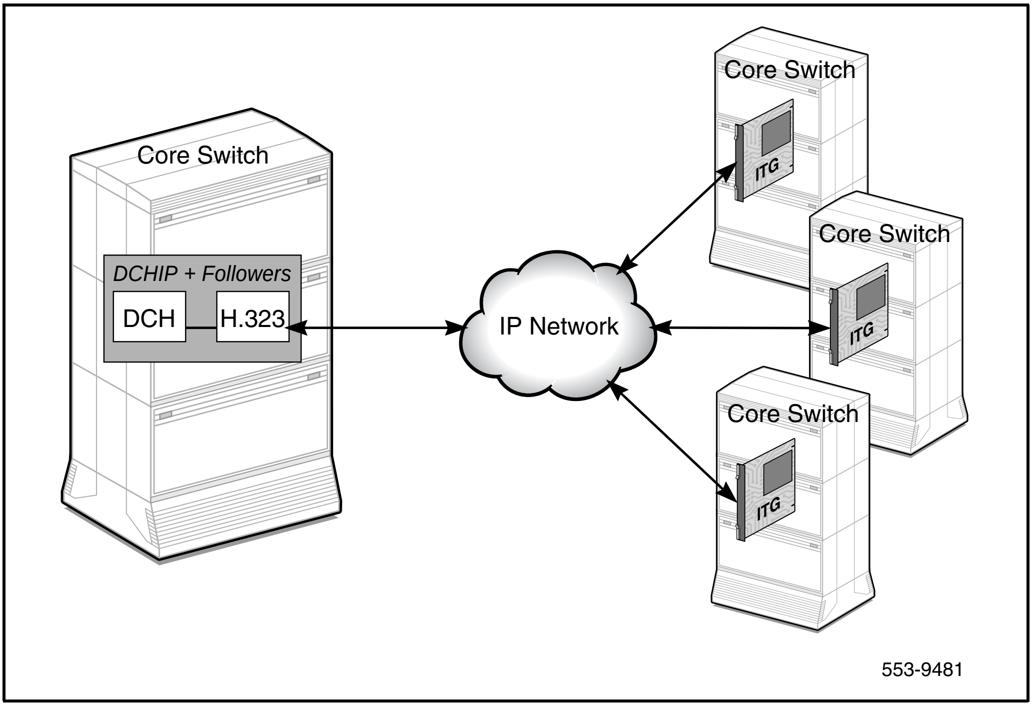
Backup Leader

The Backup Leader card steps in when the Leader is out-of-service. This minimizes service interruptions.

D-channel IP gateway

The ITG-Pentium 24-port or Media Card 32-port trunk card with D-channel IP gateway (DCHIP) functionality (DCHIP card) is connected by the RS-422 cable to the Multi-purpose Serial Data Link (MSDL) card on the Meridian 1/CS 1000M Large Systems. It connects to the SDI/DCH Card on Small Systems. The DCHIP Card is equipped with a DCH PC Card. The DCH PC Card provides the RS-422 and LAPD functionality that is required for the D-channel (DCH) interface to the system. The DCHIP Card is the network side of the system ISL D-channel connection. The card is a tandem node in the switch network, providing a single-to-multi-point interface between the Meridian 1/CS 1000M and the IP Trunk 3.01 (and later) network. See Figure 5.

Figure 5
IP Trunk 3.01 (and later) architecture

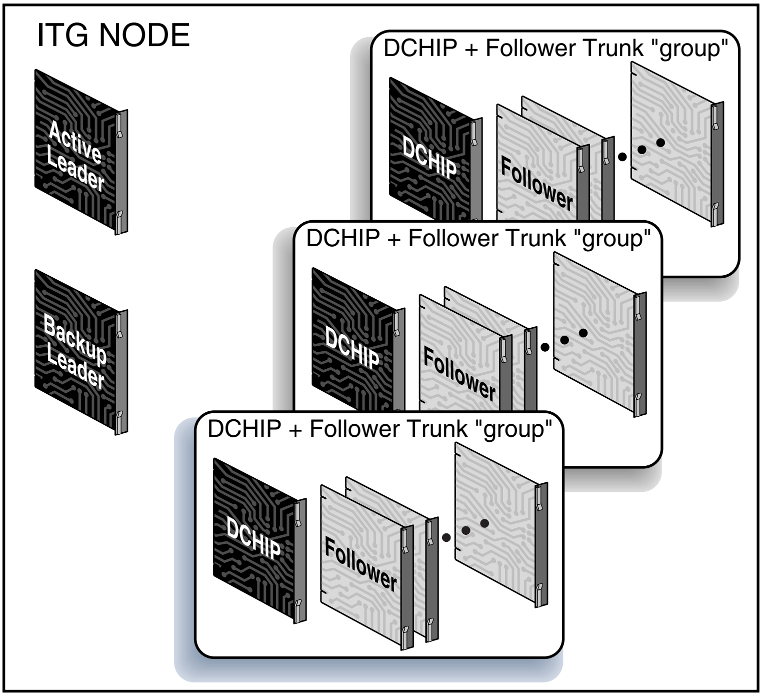


The ISL connection to the Meridian 1/CS 1000M functions as it does in a normal ISDN network. The ISL controls the call processing for calls over analog ISDN Signaling Link (ISL) TIE trunks. With IP Trunk 3.01 (and later), these ISL TIE trunks are located on the IP trunk cards. The IP Trunk 3.01 (and later) D-channel only controls IP trunk cards in the same IP Trunk 3.01 (and later) node. OTM administration relates the cards with trunks to the DCHIP IP trunk card.

The IP trunk card uses ISDN messages for call control and communicates with the Meridian 1/CS 1000M through the PC Card, using the RS-422 link. On the Meridian 1, the MSDL provides the ISL DCH interface. The DCHIP IP trunk card software performs the tandeming of DCH call control to the H.323 protocol.

Each DCHIP trunk card can be associated with up to 382 trunks. The trunks reside on all IP Trunk 3.01 (and later) IP trunk cards (ITG-Pentium 24-port trunk cards and Media Card 32-port trunk cards) in the node. This creates a functional grouping of IP trunk cards with the DCHIP trunk card providing the DCH connectivity. If more than 382 trunks are required, additional DCHIP trunk card groups are configured, each with a maximum of 382 related trunks. See Figure 6 on page 68.

Figure 6
Leader, DCHIP, and trunks in an IP Trunk 3.01 (and later) node


ITG NODE
Active Leader
Backup Leader
DCHIP + Follower Trunk "group"
DCHIP
Follower
DCHIP + Follower Trunk "group"
DCHIP
Follower
DCHIP + Follower Trunk "group"
DCHIP
Follower

Card combinations

The Leader and DCHIP, or Follower and DCHIP, functions can reside on a single IP trunk card or multiple IP trunk cards. If a Follower card is equipped with a DCH PC card, it can function as a DCHIP trunk card. As an IP Trunk 3.01 (and later) node becomes larger with more trunk traffic, load balancing should be configured. When load balancing is required, the Leader and DCHIP functionality are placed on separate cards which are assigned the least call traffic. For the largest IP Trunk 3.01 (and later) nodes and networks, the Leader and DCHIP cards can be partially configured with trunk ports or have no trunk ports at all.

An example configuration that allows for redundancy and backup is the following:

- **Card 1:** Leader and DCHIP #1
- **Card 2:** Backup Leader and DCHIP #2
- **Card 3:** Follower #1 – 24 trunks connected with DCHIP #1
- **Card 4:** Follower #2 – 24 trunks connected with DCHIP #2

To support more trunks, more DCHs can be added. Each DCHIP card can support a maximum of 15 NT0961AA ITG-Pentium 24-Port Follower cards or 11 NTVQ90BA Media Card 32-port Follower cards. This limit is due to the maximum limit of 382 trunks in an ISL route.

> *Note:* Each DCHIP card controls a separate group of Follower cards. If a DCHIP card fails, its associated Followers are removed from service as well. For very large nodes, it is recommended that Follower cards be spread across multiple DCHIPs, in order to provide some resiliency by allowing the IP Trunk 3.01 (and later) node to continue handling calls when one DCHIP card fails.

A DCHIP card and all of the IP trunk cards connected with it belong to one Leader card. This means that the cards also belong to a single customer. The group of IP trunk cards connected with one Leader is referred to as an IP Trunk 3.01 (and later) node. If a single Meridian 1/CS 1000M system has multiple customers requiring IP Trunk 3.01 (and later) connectivity, a separate IP Trunk 3.01 (and later) node is required for each customer. Multiple DCHIPs can be configured for each node.

> *Note:* All DCHIPs in an IP Trunk 3.01 (and later) node must be configured with the same DCH protocol. If the user wants to use multiple DCH protocols, the user must configure multiple IP Trunk 3.01 (and later) nodes.

Each customer requires one or more dedicated IP Trunk 3.01 (and later) nodes. Trunks on the same IP Trunk 3.01 (and later) node share the same dialing plan and IP network connectivity. IP Trunk 3.01 (and later) trunks cannot be shared between customers that have independent numbering plans and IP networks.

It is possible to configure multiple IP Trunk 3.01 (and later) nodes for one customer. This configuration allows load balancing among multiple Leaders for systems with more traffic than a single Leader card can support. The configuration of multiple IP Trunk 3.01 (and later) nodes on one customer requires splitting the dialing plan among the Leaders. Each Leader must have a distinct range of the dialing plan. This restriction exists so that a remote gateway can relate a DN with a single IP address.

> *Note:* For information about engineering an IP Trunk 3.01 (and later) node, refer to "ITG engineering guidelines" on page 125.

Interactions among card functions

Active Leader and Follower card interaction

The Active Leader card controls the assignment of IP addresses for all new ITG-Pentium 24-port and Media Card 32-port trunk cards in its node. If a new IP trunk card is added as a Follower, the new Card Configuration data, as programmed in OTM, is downloaded only to the Active Leader card. When it boots up, the new Follower card requests its IP address from the Active Leader card through the bootp protocol. When the Follower cards boot up, they receive their IP address and Active Leader card IP address from the Active Leader card.

Follower cards continuously send Update messages to the Active Leader card. These messages inform the Active Leader card of the Followers' most recent status and resources. The Active Leader sends Update messages to the Follower cards, informing them of the updated dialing number to IP address translation information. Also the Active Leader card continuously sends messages about changes in the network performance of each destination node in the dialing plan.

If a Follower card fails (for example, DSP failure), it reports to the Active Leader that its failed resources are not available. The trunk ports involved are considered faulty and appear busy to the Meridian 1/CS 1000M. Call processing is maintained on the remaining IP Trunk 3.01 (and later) trunks.

If a Follower card loses communication with the Active Leader, all its ports appear busy to the Meridian 1/CS 1000M. Alarms are raised by sending an Simple Network Management Protocol (SNMP) trap to the IP addresses in the SNMP manager list.

Active Leader and Backup Leader interaction

When a Leader card reboots into service, it sends bootp requests to check whether an Active Leader card is present. If it receives a bootp response, this indicates the presence of an Active Leader card and the rebooting Leader becomes the Backup Leader. If it does not receive a bootp response, this indicates the absence of an Active Leader and the rebooting Leader becomes the Active Leader.

The Backup Leader monitors the heartbeat of the Active Leader by pinging the Active Leader’s Node IP. In the event of the Active Leader’s failure (that is, the Active Leader is not responding to the pinging of the Node IP address by the Backup Leader), the Backup Leader takes over the Active Leader role, in order to avoid service interruption. The Backup Leader assigns the Node IP to its voice interface and announces its new status to all the Follower cards. The Followers re-register with the new Active Leader and, as a result, a new Resource Table is built immediately.

The Leader 0 and Leader 1 cards keep their node properties synchronized. The Backup Leader receives a copy of the bootp.1 file, containing the bootp table, from the Active Leader on bootup and when Node Properties are downloaded to the Active Leader.

Critical synchronized data includes the following:

- the card index:
  - index 1 indicates Leader 0

  - index 2 indicates Leader 1
  - index 3 or greater indicates Follower
- the Management MAC address (motherboard Ethernet address)
- the Node IP address
- the individual card IP addresses and card TNs for all IP trunk cards in the IP Trunk 3.01 (and later) node
- D-Channel number, card density and First CHID

In the event of a Backup Leader failure, the Leader card generates an SNMP trap to the OTM management station, indicating this failure.

If the Active Leader and Backup Leader are reset, removed, or disconnected from the LAN at the same time, the entire IP Trunk 3.01 (and later) node is put out-of-service. If this situation occurs, manual intervention is required to recover the system.

Active Leader/Backup Leader and DCHIP card interaction

The Active Leader checks the status of the DCHIP card. The DCHIP card must constantly inform the Leader of its DCH status and its card status.

When a DCHIP trunk card failure occurs, the associated trunks' states appear busy to the Meridian 1/CS 1000M, so the trunks will not be used for calls. This blocks the normal software action of reverting to analog signaling when an ISL DCH fails. If either end's DCHIP or DCH connection fails, ISDN protocol features across the IP network do not function. When a DCHIP card fails, its associated Followers are also removed from service.

In the case of a DCH failure, established calls are maintained; however, no new calls can be made. Calls in a transient state are dropped.

ITG-Pentium 24-port trunk card (NT0961AA)

The ITG-Pentium 24-port trunk card was introduced as part of ITG Trunk 2.0. During the installation of the IP Trunk 3.01 loadware, the application on the ITG-P 24-port card(s) (ITG-P) must be upgraded. It is essential to ensure the latest software is loaded on the ITG-P card(s).

Description

The NT0961AA ITG-Pentium 24-port trunk card plugs into an Intelligent Peripheral Equipment (IPE) shelf. Each ITG-Pentium 24-port trunk card occupies two slots. ITG-Pentium 24-port trunk cards have a ELAN network interface (10BaseT) and a TLAN network interface (10/100BaseT) on the I/O panel. The ITG-Pentium 24-port trunk card has a DIN-8 serial maintenance port connection on the faceplate and an alternative connection to the same serial port on the I/O backplane.

Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

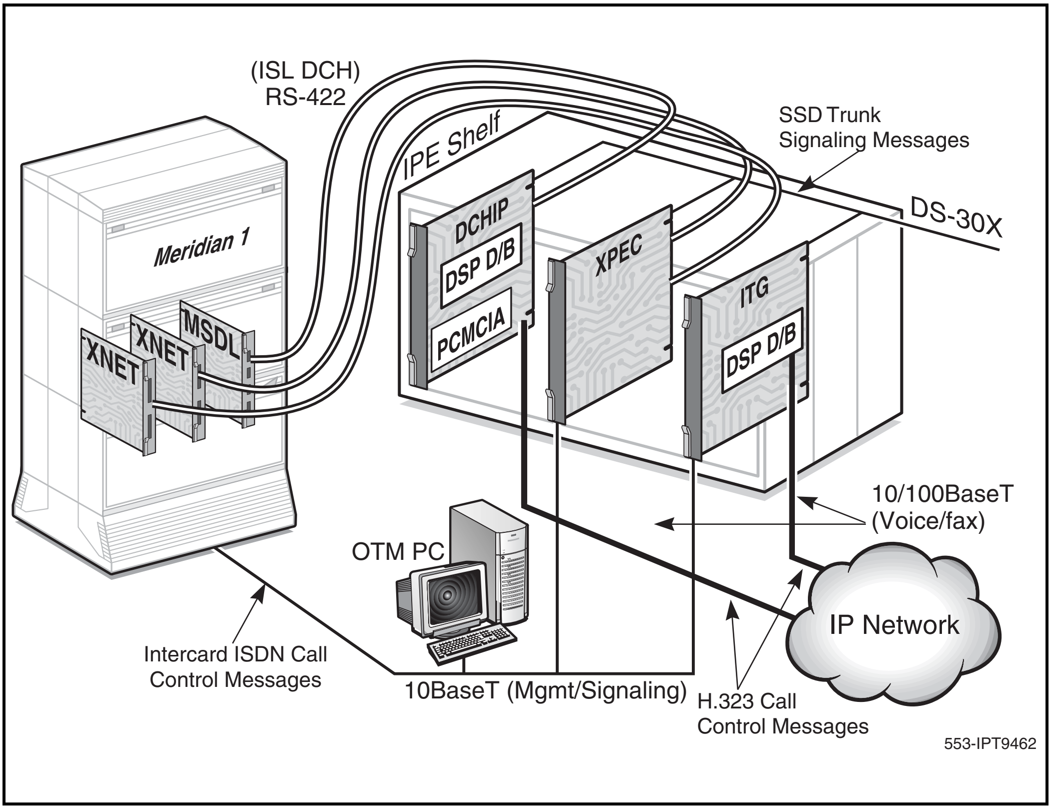
The NT0961AA ITG-Pentium 24-port trunk card supports 24 ports per card.

The core ITG processor is an Intel Pentium II (266 Mhz).

The ITG-Pentium 24-port trunk card is responsible for converting the 64 kbit/s Pulse Code Modulation (PCM) speech from the DS-30X backplane interface into packetized speech for transmission over the IP network. On the daughterboard, the DSPs compress speech and feed the resulting packets to the IP network.

Figure 7 on page 74 shows ITG-Pentium 24-port trunk card system connectivity.

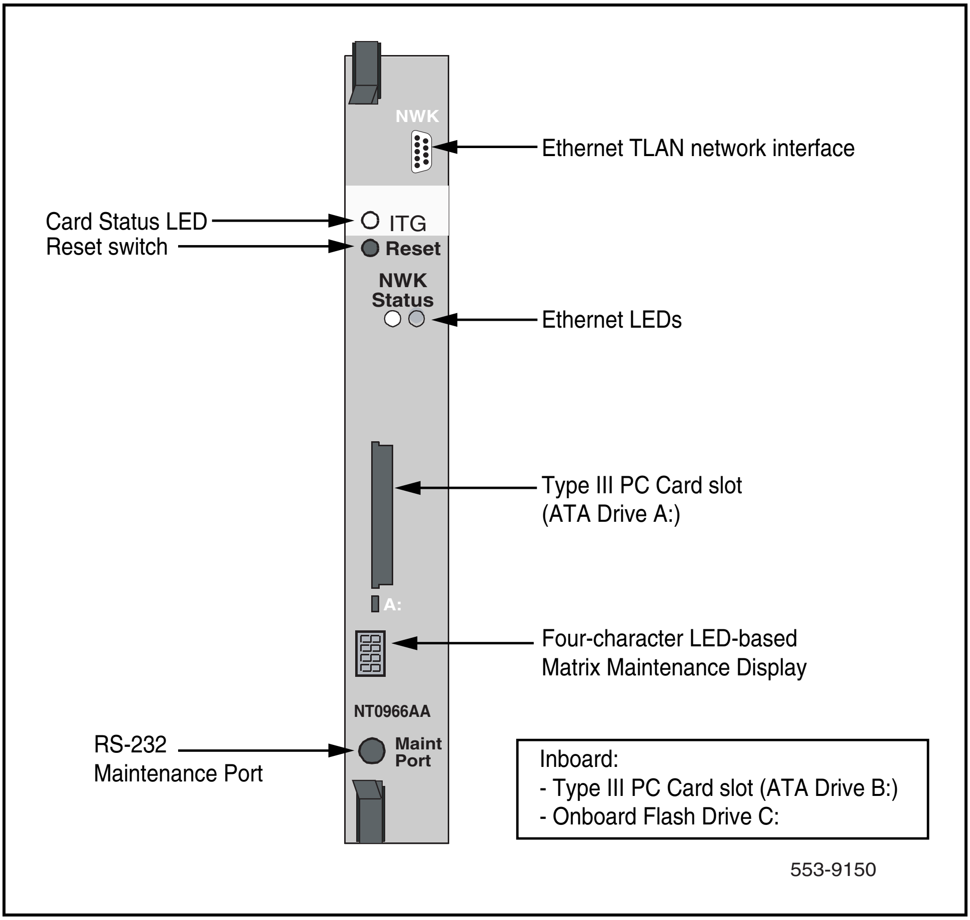
Figure 7
ITG-Pentium 24-port trunk card system connectivity and messaging



Faceplate indicators, controls, and interfaces

The NT0961AA ITG-Pentium 24-port trunk card has a double width faceplate using the shortened lock latches, as shown in Figure 8.

Figure 8
NT0961AA ITG-Pentium 24-port trunk card


NWK
Ethernet TLAN network interface
Card Status LED
Reset switch
ITG
Reset
NWK Status
Ethernet LEDs
Type III PC Card slot (ATA Drive A:)
A:
Four-character LED-based Matrix Maintenance Display
NT0966AA
RS-232 Maintenance Port
Maint Port
Inboard:
- Type III PC Card slot (ATA Drive B:)
- Onboard Flash Drive C:
553-9150

Card Status LED

A single red, card status LED on the faceplate indicates the enabled/disabled status of the 24 ports on the card. The LED is lit (red) during the power-up or reset sequence. The LED remains lit until the card correctly boots and assumes its role (that is, Leader, Backup Leader, Follower or DCHIP). If the LED remains on, one of the following has occurred:

- the self-test has failed (the Faceplate Maintenance Display indicates the cause F:xx)
- the card has rebooted
- the card is active, but there are no trunks configured on it (for example, the card is a Leader or DCHIP)
- the card is active and has trunks, but the trunks are disabled (that is, the trunks must be enabled in LD 32)

  Note: During configuration, the error message "F:10" can appear. This error indicates a missing Security Device. It occurs because Security Devices are not implemented on ITG Trunk 2.0. Ignore this message.

See "ITG-Pentium 24-port trunk card faceplate maintenance display codes" on page 563 for a complete list of faceplate codes.

Ethernet status LEDs

Ethernet status LEDs for the voice interface on the daughterboard display the Ethernet activity as follows:

- Green is always on if the carrier (link pulse) is received from the TLAN Ethernet hub.
- Yellow flashes when there is data activity on the TLAN Ethernet hub.
- During heavy traffic, yellow can stay continuously lit.

  Note: There are no Ethernet status LEDs for the ELAN network interface on the motherboard.

Reset switch

A reset switch on the faceplate allows an operator to manually reset the card without having to cycle power to the card. This switch is normally used following a software upgrade to the card or, alternatively, to clear a fault condition.

PC Card socket

There are two PC Card sockets. The faceplate socket accepts either a Type I, a Type II, or a Type III PC Card and is designated ATA device A:. The internal socket is reserved for the NTWE07AA C7LIU DCH PC Card on the DCHIP.

Maintenance display

This is a four character, LED-based dot matrix display. It shows the card boot sequence and is labeled with the card role as follows:

- LDR = Active Leader
- BLDR = Backup Leader
- FLR = Follower

> ***Note:*** A properly-functioning IP trunk card displays one of the above codes. If an IP trunk card encounters a problem, a fault code is displayed. For more information, see “Media Card 32-port trunk card faceplate maintenance display codes” on page 560 and “ITG-Pentium 24-port trunk card faceplate maintenance display codes” on page 563.

RS-232 maintenance port

The ITG-Pentium 24-port card has a DIN-8 (RS-232) maintenance port (DCE) connection on the faceplate and an alternative connection to the same serial port on the I/O backplane. Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

Ethernet TLAN network interface

The faceplate Ethernet TLAN network interface is a 9-pin, sub-miniature D-type connector. The Ethernet TLAN network interface on the daughterboard is identified as “lnPci1” in the ITG shell.

> **WARNING**
>
> Do not connect a TLAN cable to the faceplate 9-pin Ethernet TLAN network interface NWK. Connect the TLAN cable to the I/O cable.

Backplane interfaces

The following interfaces are provided on the backplane connector:

DS-30X voice/signaling

This carries PCM voice and proprietary signaling on the IPE backplane between the IP trunk card and the Intelligent Peripheral Equipment Controller (XPEC).

Card LAN

This carries card polling and initialization messages on the IPE backplane between the IP trunk card and the Intelligent Peripheral Equipment Controller (XPEC).

RS-232 serial maintenance port

This provides an alternative connection to the serial maintenance port that exists on the I/O backplane. Use the NTCW84KA or NTMF94EA I/O panel breakout cable to access the port. A DIN-8 serial maintenance port connection exists on the faceplate. Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

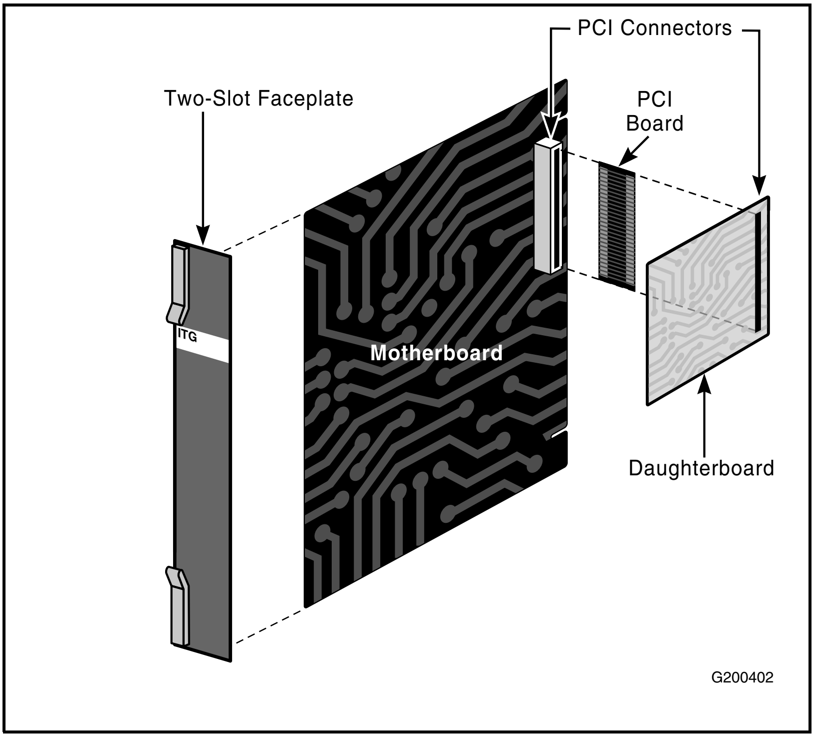
Assembly description

The ITG-Pentium 24-port trunk card assembly consists of a two-slot motherboard/daughterboard combination, as shown in Figure 9 on page 79. A PCI interconnect board connects the motherboard and the DSP daughterboard.

CAUTION — Service Interruption

The ITG-Pentium 24-port trunk card is not user-serviceable. Figure 9 on page 79 is for information purposes only. Do not remove the daughterboard from the motherboard.

Figure 9
Mechanical assembly



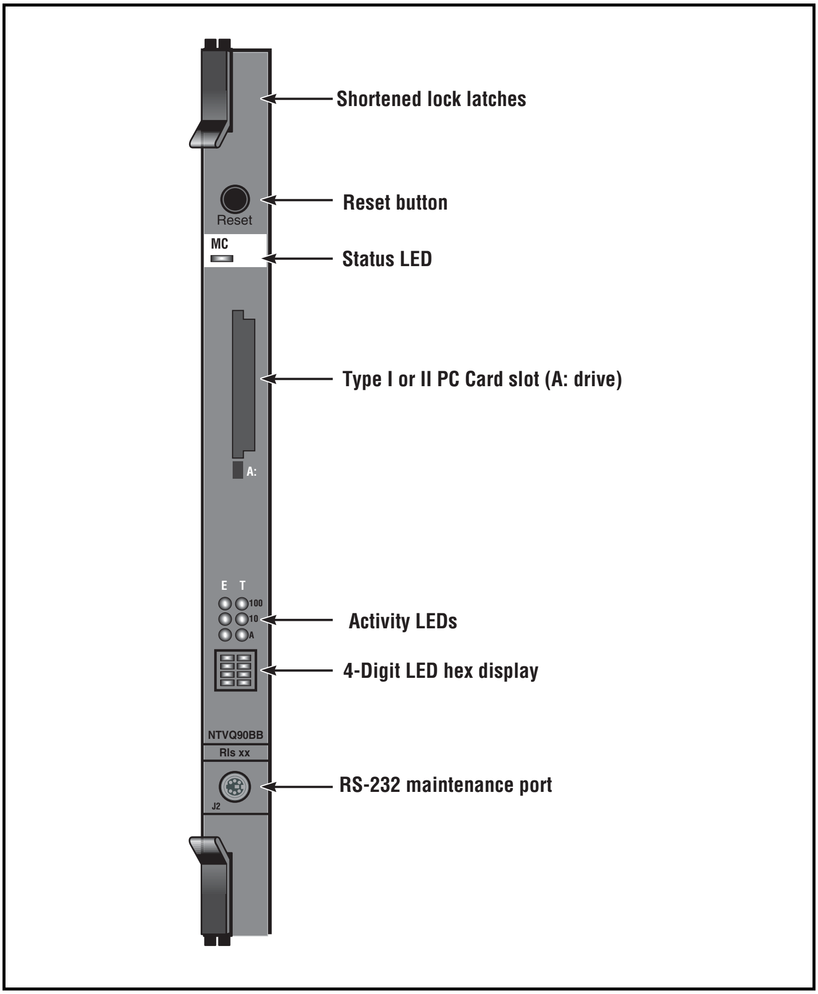
Media Card 32-port trunk card (NTVQ01BB)

The NTVQ01BB Media Card 32-port trunk card provides a single slot implementation in an IPE shelf for Large and Small Systems. During the installation of the IP Trunk 3.01 loadware, the application on the Media Card(s) must be upgraded. It is essential to ensure the latest software is loaded on the Media Card(s).

Description

The Media Card 32-port trunk card is based on an integrated hardware platform that delivers a single-slot ITG solution, with an increase in port density from 24 ports to 32 ports. The Media Card 32-port trunk card faceplate is shown in Figure 10.

Figure 10
Media Card 32-port trunk card



The base hardware (known as the Media Card) enhances cabling arrangements for installation and maintenance.

NTVQ01BB Hardware

NTVQ01BB Media Card 32-port trunk card is an improved version of NTVQ01BA Media Card 32-port trunk card.

The main hardware enhancements in NTVQ01BB Media Card 32-port trunk card are:

- The DSP daughter board has been removed and the DSP design is implemented on the motherboard.
- The onboard FPGAs are changed to the advanced family of device architecture.
- A new Compact Flash Drive is used for onboard C: Drive.
- The faceplate has been re-designed for better ergonomics.
- New firmware is developed to implement the above design enhancements.

Table 8 provides a comparison of the design features for the two versions of the Media Card 32-port trunk card.

Table 8
Media Card 32-port trunk card comparison

	NTVQ01BA	NTVQ01BB
MC Firmware	Release 6.7	Release 8.0
Onboard DSP	1	4
DSP Module	1	Nil
Compact Flash Drive	Compact Flash Drive with lock Pin Retention	Compact Flash Drive with Retaining Clip

Assembly description

The Media Card 32-port trunk card assembly comes with a pre-installed SDRAM Module. The IP Trunk Application is installed on the C:/ drive.

Faceplate indicators and interfaces

The Media Card 32-port trunk card has a single slot faceplate. It uses shortened lock latches to lock it in place. Refer to Figure 10 on page 80.

Status LED

A single red LED indicates the enabled/disabled status of the card and the status of the power-on self-test.

> ***Note:*** Where a DCHIP PC Card is installed in the Media Card 32-port trunk card A:/ drive, the LED does not indicate the status of the DCHIP PC Card or the DCHIP.

Reset button

The reset button enables the operator to manually reset the card without cycling power to it. Use the reset button to reboot the card after a software upgrade, or to clear a fault condition.

PC Card slot

This slot (designated as Slot A:) accepts a Type I or II PC Card. It also supports a DCHIP interface PC Card (D-Chip) to the system through the NTMF29Bx cable.

Ethernet activity LEDs

The LEDs indicate 100BaseT, 10BaseT, and activity on both the ELAN and TLAN network interfaces.

Maintenance display

The maintenance display is a 4-character LED-based dot-matrix display. It displays the IP trunk card boot sequence and displays the card role as follows:

- LDR = Active Leader
- BLDR = Backup Leader
- FLR = Follower

Note: A properly-functioning IP trunk card displays one of the above codes. If an IP trunk card encounters a problem, a fault code is displayed. For more information, see “Media Card 32-port trunk card faceplate maintenance display codes” on page 560 and “ITG-Pentium 24-port trunk card faceplate maintenance display codes” on page 563.

RS-232 maintenance port

The Media Card 32-port trunk card has a DIN-8 (RS-232) maintenance port (DCE) connection on the faceplate and an alternative connection to the same serial port on the I/O backplane.

CAUTION — Service Interruption

Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

Backplane interfaces

The Media Card 32-port trunk card provides the following interfaces on the backplane connector:

- DS-30X voice/signalling
- card LAN
- one RS-232 serial COM port for the Command Line Interface (CLI)
- ELAN 10BaseT and TLAN 10/100BaseT network interfaces

Installation guidelines

Use the following guidelines when installing the Media Card 32-port trunk card:

- Ensure CS 1000 Release 4.0 software is installed and running.
- Ensure that the NTVQ01BB Media Card Firmware is version 8.0 (or later)
- Order the Alarm and Notification application package separately.

- For all MCDN features, the SDI/DCH NTAK02 card (Small Systems) or the MSDL NT6D80 card (Large Systems) is required. These cards must be ordered for each system.
- For Large Systems which include the NT8D81AB moulded Tip/Ring Backplane cable, replace it with the NT8D81AA non-moulded version cable for 100BaseT operation. For more information on installation of the new filter block, refer to page 261.
- A security dongle and keycode mechanism are not required on the Media Card 32-port trunk card.
- The new Option11C Cabinet door and grill (which allows more space between the door and the cards) is required due to the space needed by the DCHIP faceplate assembly. A cabinet upgrade kit, NTDK18AA, is available for the following cabinets: NTAK11xC or earlier, and NTDK50.
- A maximum of ten Media Card 32-port trunk cards can be installed in a Large System cabinet for Class B compliance (EN55022:1998 and EN55024:1998). There are no limitations on the number of Media Card 32-port trunk cards that can be installed in other Meridian 1/CS 1000M systems.

Software delivery

The IP Trunk 3.01 software application is provided on the onboard CompactFlash card for the Media Card 32-port trunk card.

A programmed CompactFlash (NTM405AB) card is shipped along with every IP Trunk 3.01 system package card. The CompactFlash must be installed on the Media Card 32-port trunk card.

IMPORTANT!

The software is downloadable from the Nortel website and is available to IP Trunk customers free of charge.

The Media Card 32-port trunk card package is shipped with the following two major components, as well as other items:

- Media Card 32-Port Assembly (NTVQ01BB)
- CompactFlash card (NTM405AB)

IMPORTANT!

The CompactFlash card must be installed on the Media Card before installing the Media Card assembly in the IPE shelf.

Card upgrades

Media Card 32-port trunk cards running on previous ITG Trunk Releases can be upgraded by replacing the CompactFlash with the NTM405 IP Trunk 3.01 (and later) application upgrade CompactFlash. ITG-Pentium 24-port trunk cards and older Media Card 32-port trunk cards can both be upgraded as outlined in “Software upgrade” on page 88.

Replacing a CompactFlash PC Card (C:/ drive)

If it is necessary to remove the CompactFlash PC (CFlash) card, follow the steps in Procedure 1 on page 86. Then, follow the steps in Procedure 2 on page 87 to install the new CFlash card.

WARNING

The Media Card 32-port trunk card does not require file transfers to or from the A:/ drive for normal operation. If a CFlash ATA card is to be used for file transfers to or from the A:/ drive, to C:/ drive, Nortel recommends that the CFlash ATA card be formatted on the Media Card 32-port trunk card before use.

CAUTION — Service Interruption

When replacing the CFlash, contact the Nortel Technical Support Center.

CAUTION WITH ESDS DEVICES

Use ESDS precautions when handling the Media Card 32-port trunk card.

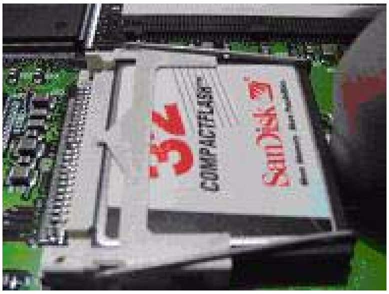
WARNING

Be sure to remove the Media Card 32-port trunk card from the system before replacing the CFlash ATA card.

Procedure 1
Removing the CFlash card on NTVQ01BB

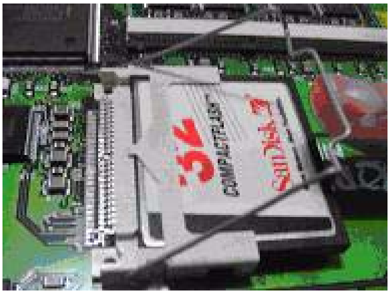
1 Gently pull the clip from its latched position. See Figure 11.

Figure 11
CFlash card with clip latched



2 Move the clip up. The CFlash card can now be removed from the drive.

Figure 12
CFlash card with clip up



End of Procedure

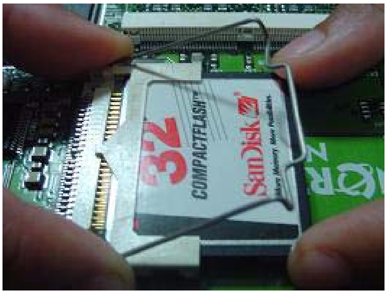
Procedure 2
Installing the CFlash card

1 Follow ESD precautions to protect the card.
Place the Media Card 32-port trunk card horizontally on a clean bench.

2 The metal clip should be pulled up and the new CFlash card should be kept in the right position (see Figure 13).

3 Ensure that force is applied equally at both ends of the CFlash card before pushing it in (see Figure 13).

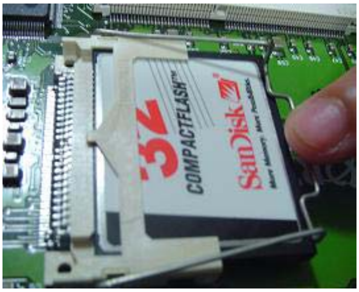
Figure 13
CFlash card with metal clip up



4 Gently insert the CFlash, so that the flash is fully in contact with the connectors on the drive.

5 Push the metal clip down so that the CFlash is locked in (see Figure 14).

Figure 14
CFlash card with metal clip down



End of Procedure

> **WARNING**
>
> The Media Card 32-port trunk card requires the IP Trunk 3.01 (and later) application software (exec file) to be present on the C:/ drive (CFlash card) in order to run the IP Trunk 3.01 (and later) application.

Software upgrade

IP Trunk 3.01 (and later) software upgrades can be performed in three ways:

- by FTP from OTM 2.1 (and later)
- by FTP from the CLI
- from a PC Card

Note: The application (exec) file for the Media Card 32-port trunk card contains a different CPU type definition from other IP trunk card types. When performing an upgrade on an IP trunk node containing a mixture of Media Card 32-port trunk cards, ITG-Pentium 24-port trunk cards, and ITG 8-port trunk cards, each card type must be upgraded with its corresponding image file. It is important that all cards in a node are using the same software release, which means that a node upgraded to IP Trunk 3.01 (and later) can no longer have an ITG 8-port trunk card in that node.

IMPORTANT!

IP Trunk 3.01 (and later) does not support the ITG 8-port trunk card.

Follow the steps in Procedure 3 to upgrade to IP Trunk 3.01 (and later) software.

Procedure 3
Upgrading IP Trunk 3.01 (and later) software

1 Download the latest software upgrade information from the Nortel website to the OTM PC or to an FTP server. Go to www.nortel.com. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support.

2 See “Check and download IP trunk card software in OTM 2.1 (and later)” on page 361 for information on how to upgrade the software by FTP from OTM 2.1 (and later).

See “Transfer files through the Command Line Interface” on page 501 and “Upgrade IP trunk card software using FTP” on page 504 for information on how to upgrade the software by FTP from the CLI.

A CompactFlash PC Card containing the latest software version can be obtained from Nortel. See “Upgrade IP trunk card software by PC Card” on page 505 for information on how to perform the upgrade.

3 When the upgrade file has been downloaded, install the new IP Trunk 3.01 (and later) application software onto the IP trunk card. Follow the application software upgrade procedure as described in “Transmit card properties and dialing plan” on page 554 or in “Transfer files through the Command Line Interface” on page 501.

End of Procedure

Media Card application identification labels

Media Card application identification labels (see Figure 15) are provided with every Media Card 32-port trunk card package. Affix the appropriate label to the Media Card's faceplate (see Figure 16).

Figure 15
Media Card identification labels

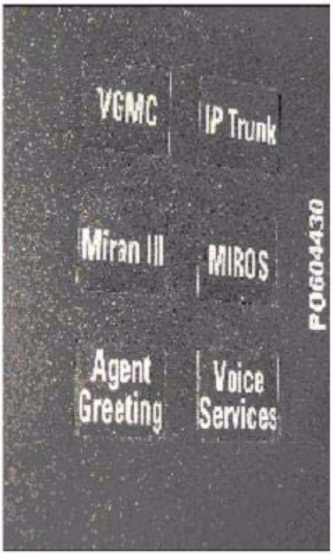
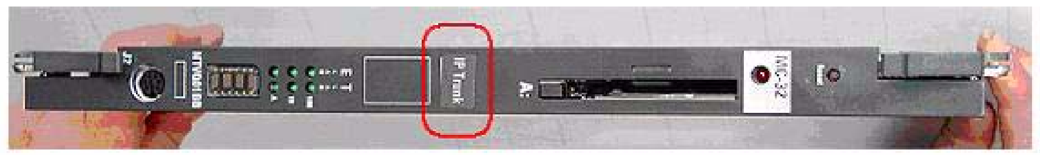


Figure 16
Labeled Media Card



Interoperability with earlier versions of ITG Trunk

When Media Card 32-port trunk cards are implemented in existing networks with nodes comprised of ITG Trunk 2.xx, Release 19 or earlier, fax calls do not work because of protocol incompatibility. Voice calls between ITG Trunk 2.1 and ITG Trunk 2.0 or ITG Trunk 1.0 operate without restrictions.

> ***Note:*** If an upgrade from ITG Trunk 2.xx, Release 19 or earlier, is projected to take several days and fax support is needed during this time, first upgrade the individual nodes to ITG Trunk 2.xx Release 23. When the network is upgraded to ITG Trunk 2.xx Release 23, upgrade again to the latest software release. The interim upgrade step is only required if fax support is needed during the upgrade process.

When the Media Card 32-port trunk cards are upgraded to or installed with IP Trunk 3.01 (and later), fax calls do not work to nodes running ITG Trunk 2.xx Release 19 or earlier. This limitation is due to the same protocol incompatibility that exists between ITG Trunk 2.1 and ITG Trunk 2.xx and earlier.

Fax Tone Detection Configuration

For IP Trunk 3.01 (and later) fax operation, the V.21 Tone detection check box must be selected in OTM 2.1 (and later) in the Configuration window, under the DSP profile tab. For more information, see “Configure DSP profiles for the IP Trunk 3.01 (and later) node” on page 326.

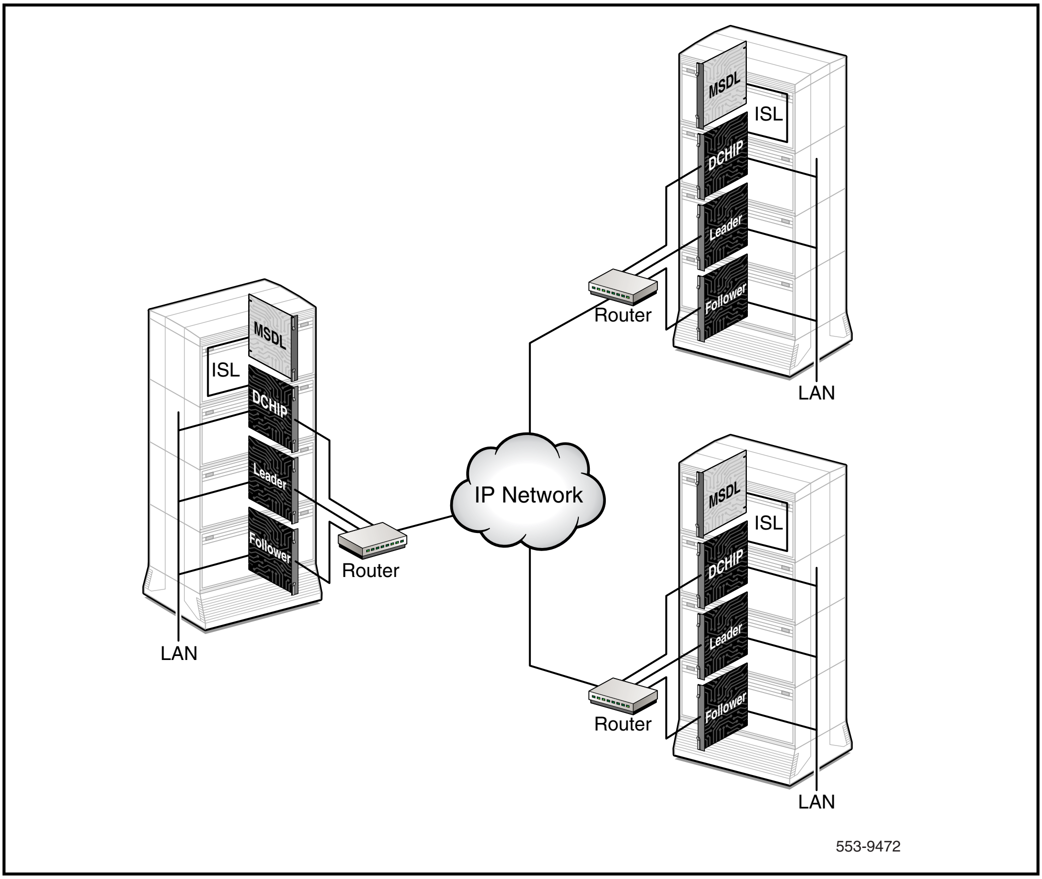
ISDN Signaling Link

ISDN Signaling Link (ISL) provides the capability of replacing conventional analog trunk signaling with out-of-band ISDN D-channel signaling.

The ISL interface makes available the flexibility of using ISDN signaling to analog facilities. When no Primary Rate Interface (PRI) exists between two Meridian 1/CS 1000M systems, ISL operates in dedicated mode. A dedicated point-to-point signaling link is established between the two systems. The signaling information for the selected analog trunks is transported over the ISDN signaling link. The analog ISL TIE trunks are for user voice transport. If the D-channel link is down, call control returns to normal in-band analog trunk signaling.

The ITG is similar to the existing ISL configuration where there is a Virtual Private Network (VPN) between Meridian 1/CS 1000M systems. Instead of a one-to-one connection, multiple switches can be networked through a single ISL interface at each site. Figure 17 on page 93 shows an IP Trunk 3.01 (and later) trunk configuration with three Meridian 1/CS 1000M systems. The IP Trunk 3.01 (and later) trunk simulates an analog facility. The ISL interface is connected to a DCHIP PC Card which provides ISDN to VoIP tandeming. All IP Trunk 3.01 (and later) IP trunk cards (DCHIP, Leader, and Follower) are connected through the ELAN subnet. The IP trunk cards communicate with remote switches through the IP network.

Figure 17
ITG configuration



ISDN signaling between the Meridian 1 and IP Trunk 3.01 (and later) supports the delivery of Calling Line Identification (CLID) and feature messaging. ISL DCH signaling provides the necessary signaling connection over which data, including CLID and feature-specific messaging, can be passed.

On Large Systems, the DCH interface to the Meridian 1/CS 1000M uses the MCDN or QSIG GF protocols and their variants to transmit call and feature control messages to the DCHIP card. Small Systems use only MCDN because the NTAK02BB SDI/DCH card does not support QSIG protocols for ISL. The DCH interface uses these protocols and their variants, as they have the following advantages:

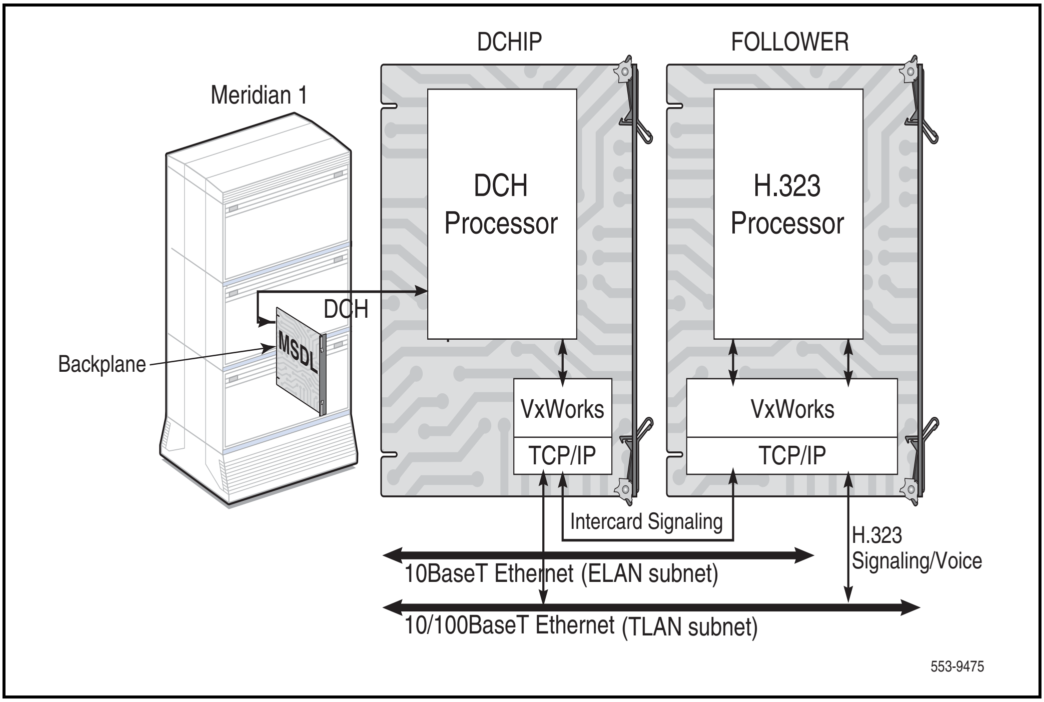
- ISL configuration support
- symmetry (incoming and outgoing call messaging is the same)
- near H.323 standard

QSIG GF Name Display is the only supported QSIG supplementary service.

The ITG feature complies with H.323 Basic Call Q.931 signaling. This part of the H.323 standard (H.225) defines the messaging used to setup and release basic calls. A mechanism is implemented to enable the passing of ISDN messaging through the IP network between the two endpoints. The call is set up using the H.323 standard signaling with encapsulated ISDN-specific information. This mechanism allows interworkings with other gateways.

The DCHIP card provides the tandem between the ISDN signaling and the H.323 protocol. If the DCHIP functionality is combined with the Follower card, messages are sent between the DCH Processor and the H.323 Processor. Most configurations split this functionality between the DCHIP and Follower cards. Figure 18 on page 95 shows the signal flow from the DCH to the H.323 stack.

Figure 18
Signal flow from the DCH to the H.323 stack

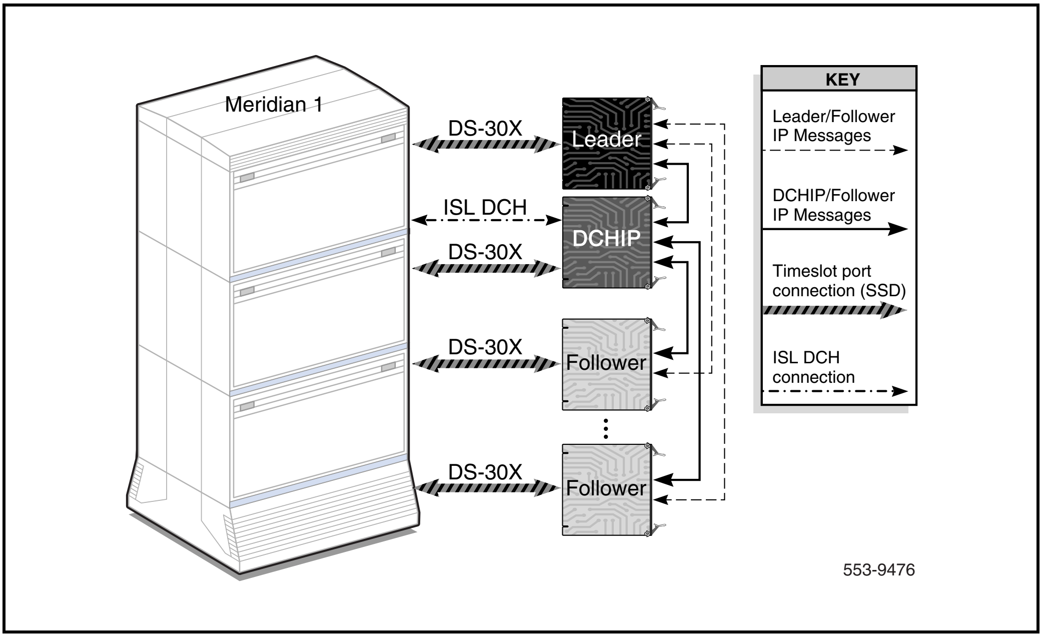


Note: For further information on ISDN Signaling Link (ISL), refer to *System Management* (553-3001-300)*, ISDN Primary Rate Interface: Installation and Configuration* (553-3001-201)*,* and *ISDN Primary Rate Interface: Maintenance* (553-3001-517).

Inter-card signaling paths

The Leader, DCHIP, and Follower cards communicate using their ELAN network interface IP addresses. Figure 19 on page 96 illustrates the IP signaling paths used inter-card and between the cards and the system in the ITG offering.

Figure 19
IP Trunk 3.01 (and later) card signaling paths



In Figure 19, the DS-30X connection is part of the IPE shelf's backplane. The ISL DCH connection is a cable that runs from the "octopus" breakout cable, on the back of the IPE cabinet, to one of the MSDL's RS-422 ports. The Leader/Follower card messages normally travel over the TLAN subnet. The DCHIP messages travel over the ELAN subnet - a 10BaseT LAN connected to each IP trunk card and the OTM PC. A separate 10/100BaseT LAN transmits the voice/fax data to the remote VoIP systems.

Dialing plans

Dialing plan configuration allows customers to set up routing tables to route calls to the appropriate destination, based on dialed digits. The dialing plan is configured through the Electronic Switched Network (ESN) feature, using OTM or overlays in the system. With ESN configuration, the system can route outgoing calls to the IP trunk card. Address translation allows the IP trunk card call processing to translate the called party number to the IP address of the terminating IP Trunk 3.01 (and later) node and to deliver calls to the destination through the IP network.

The ITG-Pentium 24-port and Media Card 32-port trunk cards support the following dialing plans:

- North American dialing plan
- Flexible Numbering Plan

Customer-defined Basic Automatic Route Selection (BARS) and Network Alternate Route Selection (NARS) Access Codes are used to access the dialing plans.

The IP Trunk 3.01 (and later) dialing plan supports a single customer per IP Trunk 3.01 (and later) node and multiple IP Trunk 3.01 (and later) nodes per Meridian 1/CS 1000M system. A customer can have multiple IP Trunk 3.01 (and later) nodes in a system, but each node can only support the dialing plan of a single customer. Multiple customers will require multiple nodes per system.

Multi-node configuration

The following example explains a possible configuration between two Meridian 1/CS 1000M switches to achieve both resiliency into the IP network and load balancing.

Meridian 1/CS 1000M switch A has two IP Trunk 3.01 (and later) nodes, A1 and A2, for the destination NPA 613. A Route List Block (RLB) is created, in order to have two route entries (one for each IP Trunk 3.01 (and later) node). If the trunks of node A1 are all in use or node A1 is down, call traffic is routed to node A2. This provides resiliency by preventing failure of a single IP Trunk 3.01 (and later) node (for example, DCH failure or Leader subnet fails) from completely eliminating VoIP service for a Meridian 1/CS 1000M system.

It is desirable to distribute calls to multiple nodes at a remote destination Meridian 1/CS 1000M. The configuration of multiple dialing plan entries at the local IP Trunk 3.01 (and later) node allows routing based on the dialed digits.

For example, Meridian 1/CS 1000M switch B node B1 has two entries for NPA 408 and 4085, which point to nodes A1 and A2 of Meridian 1/CS 1000M switch A, respectively. Calls from B1 with dialed digits 408-5xx-xxxx are routed to the IP Trunk 3.01 (and later) node A1 while all other 408-xxx-xxxx calls are routed to IP Trunk 3.01 (and later) node A2.

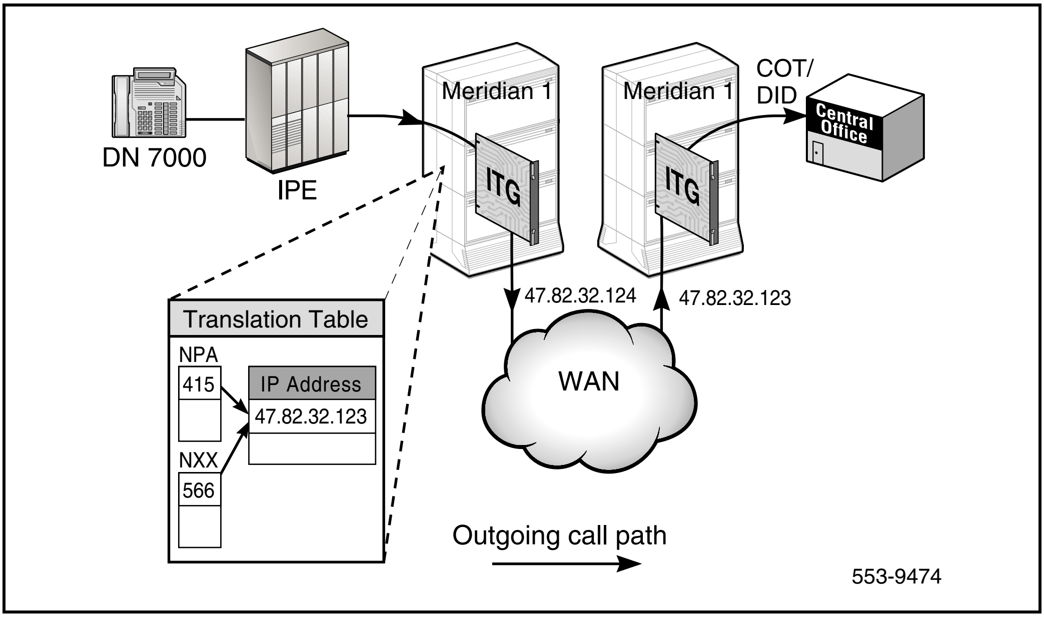
North American dialing plan

The North American dialing plan is used to make public network calls through the private IP network. However, calls are not directly routed to the Central Office (CO) through the LAN connection. Instead, a tandem switch with voice trunk connections, including T1 ISDN PRI, serves as the gateway to route voice calls coming through the LAN to the voice trunk.

Figure 20 on page 99 shows DN 7000 placing a public call, through the private LAN, by dialing 1-415-456-1234 or 566-1234. The IP trunk card with IP address 47.82.32.124 searches for the Numbering Plan Area (NPA) or Local Exchange Code (NXX) tables with the matched NPA or NXX entries. When an entry is found, the corresponding IP address is used to send H.323 call setup messages to the gateway (a Meridian 1/CS 1000M with an IP address of 47.82.32.123), which routes the call to the PSTN through a regular CO or DID trunk.

The translation table is expanded to allow extended, three-to six-digit NPA codes. For example, DNs, such as 1-415-456-XXXX and 1-415-940-XXXX, can have different destination IP addresses.

Figure 20
North American dialing plan — call flow



Flexible Numbering Plan

A Flexible Numbering Plan (FNP) allows the length of Location Codes (LOCs) to vary from node to node. As well, the total number of digits dialed to reach a station can vary from station to station. It also allows flexibility for the length of the location codes from node to node. An FNP can be used to support country-specific dialing plans. FNP also allows users to dial numbers of varying lengths to terminate at a destination. Flexibility of the number of digits which can be dialed is achieved using Special Numbers (SPNs).

Electronic Switched Network (ESN5) network signaling

IP Trunk 3.01 (and later) and ITG Trunk 2.x support a mixed network of remote nodes with ESN5 and standard (that is, non-network) signaling. ESN5 is an extension of MCDN signaling which can be used by IP Trunk 3.01 (and later), ITG Trunk 2.x, and IP Peer (CS 1000S and CS 1000M).

ESN5 inserts the Network Class of Service (NCOS) prefix ahead of the dialed numbers. Make sure that, if ESN5 is to be used, it is provisioned on both the IP trunk cards and the Route Data Block (RDB) for that node. If ESN5 is provisioned for an IP Trunk 3.01 (and later) node, all remote ITG 2.x and IP Trunk 3.01 (and later) node must have that node provisioned as "SL1ESN5" in the dialing plan. If this is not done, a default NCOS is inserted by the ESN5 node receiving the call from the non-ESN5 VoIP gateway. Fore more information, see "ESN5 network signaling" on page 308.

Echo cancellation

All telephony voice services now in use reflect some level of echo back to the user. The term "echo" refers to the return of a signal's reflection to the originator.

Packet voice networks introduce sufficient latency to cause what a caller would consider an audible echo. The echo path is round-trip. Any speech coding, packetization, and buffering delays accumulate in both directions of transmission, increasing the likelihood of audibility.

Echo cancellation reduces feedback sounds and background noise for clearer voice quality. Some less advanced IP telephony products do not include echo cancellation circuitry, resulting in voice quality of a level below business communications standards. Without echo cancellation, the talking parties can hear varying levels of echo as they speak.

Echo canceller tail delay

Early versions of ITG Trunk DSPs and DSP firmware had a maximum echo canceller (ECAN) tail delay of 32 ms. More recent cards and firmware support higher tail delays, with the ITG-P and the Media Card 32-port card supporting up to 128 ms. However, when the capability was added, the default in OTM remained unchanged at 32 ms, even though the ECAN performance was significantly better with 128 ms. This problem has been resolved in OTM, but ITG Trunk and IP Trunk nodes defined by customers with the original OTM software still use the incorrect default value.

Recent releases of OTM that are properly configured, with all applicable patches and the fix integrated, have the default for new systems set to 128 ms. This results in all new nodes being given the correct default value. However, it will not change the value on systems that are already configured unless the user deliberately changes the value.

IP Trunk 3.01 includes an enhancement to accommodate this issue. Since a 32-ms ECAN tail delay is usually only provisioned "by default" and not by deliberate user programming, the IP Trunk 3.01 application maps an ECAN tail delay of 32 seconds to the corrected default of 128 ms. This addresses the vast majority of users who want the optimum available ECAN performance. However, a small number of users, for various reasons, may want the 32-ms tail delay.

Users that can accept poorer echo performance and really want a 32 ms delay can use a value of 8 ms, which the IP Trunk application maps to 32 ms. A delay of 8 ms is completely unacceptable to end users, so this does not result in any loss of user capabilities. In addition, a value of 16 ms, which is also unsatisfactory, is mapped to a delay of 64 ms, maintaining the same two-to-one ratio with the next lower value in both the OTM and IP Trunk environment. (In this case, the 8 ms value is half the 16 ms, and the 32 ms value is half the 64 ms value.)

Table 9 shows the mapping between the delay value configured in OTM and the actual delay value used in IP Trunk 3.01. The actual configured delay value can be displayed using the CLI command **itgCardShow**. If the OTM value is mapped, "Default - xxx" is displayed, where "xxx" is the mapped value. If the OTM value is 64, 96, or 128 ms, "Value from OTM - xxx" is displayed.

Table 9
Echo canceller tail delay mapping from OTM to IP Trunk 3.01
(Part 1 of 2)

Provisioned in OTM (in ms)	Value used by IP Trunk 3.01
8	32
16	64
32 (default value in IP Trunk 3.01 and earlier)	128 (default value in IP Trunk 3.01)
64	64

Table 9
Echo canceller tail delay mapping from OTM to IP Trunk 3.01
(Part 2 of 2)

Provisioned in OTM (in ms)	Value used by IP Trunk 3.01
96	96
128 (default value in IP Trunk 3.01)	128 (default value in IP Trunk 3.01)

Speech Activity Detection

Speech activity detection reduces the IP bandwidth used by typical voice conversations. When Speech Activity Detection is enabled, no voice samples are sent during periods of silence (from one side of the conversation or the other). When a caller stops speaking, instead of a “dead” line, the listener hears “comfort noise” generated to match the previous background noise level when the caller was speaking.

> ***Note:*** Coders can send silence frames before the end of transmission during a period of silence. Coders might omit sending audio signals during periods of silence after sending a single frame of silence, or send silence background fill frames, if these techniques are specified by the audio codec in use.

This background white noise keeps the telephone from sounding like the line has gone dead - the listener can tell that the call is still up, and that the person at the other end has merely stopped speaking. This technique allows pauses during calls to sound almost the same as they would on a standard telephone line. The primary benefit of Speech activity detection is that it allows the IP Trunk to use bandwidth only when it needs to send voice samples, thereby saving expensive WAN bandwidth for data traffic or other voice and fax calls. Since normal telephone conversations include pauses, and only one side is normally speaking, Speech activity detection reduces the bandwidth used on a call by more than half.

For applications that send no packets during silence, the first packet after a silence period is distinguished by setting a marker bit in the Real Time Protocol (RTP) data header. Applications without Speech Activity Detection set the bit to zero.

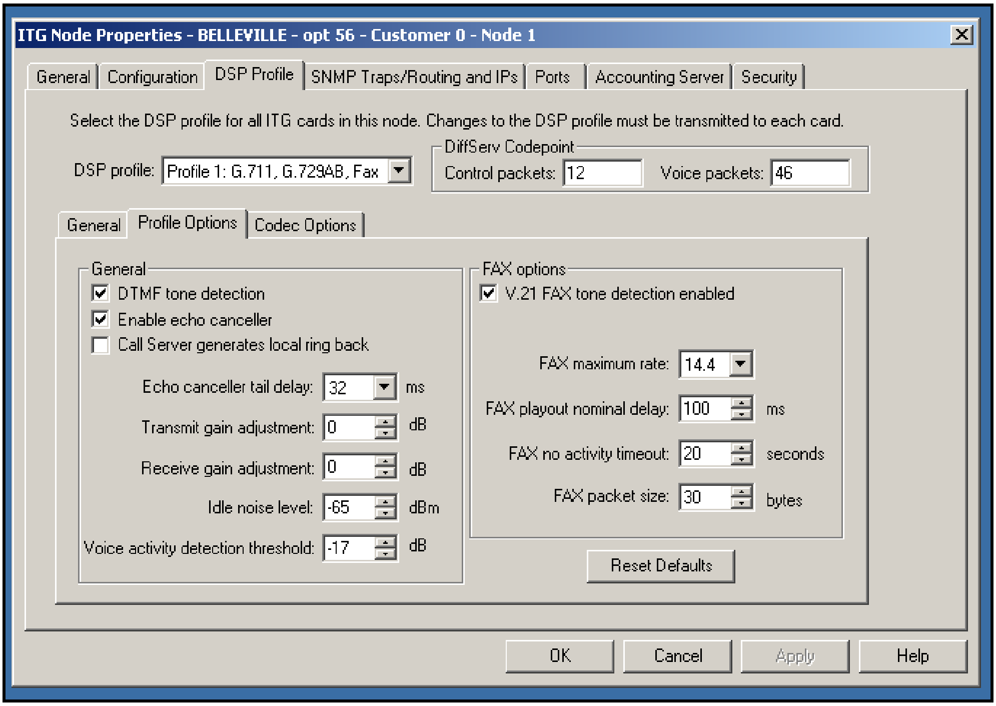
DTMF Through Dial

Preservation and transport of tones through the IP Trunk 3.01 (and later) network is critical for Interactive Voice Response (IVR) services. IP Trunk 3.01 (and later) can be configured to ensure that DTMF tone information is included in the packets that are sent through the IP Trunk 3.01 (and later) network and that the tones are re-transmitted by the far-end gateway. The duration information for DTMF signals is not transmitted; that is, long DTMF bursts are reduced to a short standard duration.

Callers can access traditional Voice Mail or IVR services (for example, “Press 1 for more information” or “Press 2 to be connected to our customer service department”). Services that depend on long DTMF bursts cannot be accessed.

In order to ensure that DTMF tones are being transmitted properly, the DSP must be configured correctly in OTM 2.1 (and later). If the IP Trunk 3.01 (and later) node is configured to use a voice codec other than G.711, “DTMF Tone Detection” **must** be selected (checked) in OTM 2.1 (and later). See Figure 21 on page 104. For more information on how to configure the IP Trunk 3.01 (and later) DSP, see “Configure DSP profiles for the IP Trunk 3.01 (and later) node” on page 326. If the IP Trunk 3.01 (and later) node is using G.711 without “DTMF Tone Detection” checked, there is no guarantee that DTMF tones will be properly transmitted to the far end, due to the possibility of latency or packet loss.

Figure 21
DTMF tone detection



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 12
Voice packets: 46

General
☑ DTMF tone detection
☑ Enable echo canceller
☐ Call Server generates local ring back

Echo canceller tail delay: 32 ms
Transmit gain adjustment: 0 dB
Receive gain adjustment: 0 dB
Idle noise level: -65 dBm
Voice activity detection threshold: -17 dB

FAX options
☑ V.21 FAX tone detection enabled

FAX maximum rate: 14.4
FAX playout nominal delay: 100 ms
FAX no activity timeout: 20 seconds
FAX packet size: 30 bytes

Quality of Service

Quality of Service (QoS) is the gauge of quality of the IP network between two nodes. As QoS degrades, existing calls suffer from poor voice and fax quality. New calls will not be initiated if transmissions degrade below an acceptable level.

Behavioral characteristics of the IP network depend on the following:

- Round Trip Time (RTT)
- latency
- queuing delay in the intermediate nodes
- packet loss
- available bandwidth

The Type of Service (ToS) bits in the IP packet header can affect how efficiently data is routed through the network. For further information on ToS, see “Type of Service” on page 112.

Packet jitter related to latency affects the quality of real-time IP transmissions. For good voice quality, the IP trunk card reassembles the voice packets in an ordered continuous speech stream and plays them out at regular intervals despite varying packet arrival times.

The user configures a required QoS for the IP Trunk 3.01 (and later) node in OTM. The QoS value determines when calls fallback to alternate facilities due to poor performance of the data network. The QoS value is between 0.0 and 5.0, where 0.0 means never fallback to alternate facilities and 5 means fallback to alternate facilities unless the voice quality is perfect. When the QoS for outgoing calls, as measured by the Leader card, falls below the configured value, calls fallback to alternate facilities. Once the QoS rises above the configured value, all new outgoing calls are routed through the IP network.

> ***Note:*** QoS is measured for each remote gateway. For example, if a given Leader has three remote leaders in its dialing plan table, it performs three QoS measurements and calculations (one per remote gateway).

Since IP trunks use the same port for both voice and fax, the same QoS thresholds apply for both voice and fax calls. Network requirements for fax are more stringent than for voice. Fax protocols, such as T.30, are more sensitive to transmission errors than the human ear.

Quality of Service parameters

Quality of Service for both voice and fax depends on end-to-end network performance and available bandwidth. A number of parameters determine the ITG voice QoS over the data network.

Packet loss

Packet loss is the percentage of packets sent that do not arrive at their destination. Packet loss is caused by transmission equipment problems and congestion. Packet loss can also occur when packet delays exceed configured limits and the packets are discarded. In a voice conversation, packet loss is heard as gaps in the conversation. Some packet loss, less than five percent, can be acceptable without too much degradation in voice quality. Sporadic loss of small packets can be more acceptable than infrequent loss of large packets.

Packet delay

Packet delay is the time between when a packet is sent and when it is received. The total packet delay time consists of fixed and variable delay. Variable delay is more manageable than fixed delay, as fixed delay is dependent on network technology. Variable delay is caused by the network routing of packets. The IP Trunk 3.01 (and later) node must be as close as possible to the network backbone (WAN) with a minimum number of hops, in order to minimize packet delay and increase voice quality. ITG provides echo cancellation, so that a one-way delay up to 200 milliseconds is acceptable. For more information about Echo Cancellation, see “Echo cancellation” on page 100.

Delay variation (jitter)

The amount of variation in packet delay is referred to as delay variation or jitter. Jitter affects the ability of the receiving IP trunk card to assemble voice packets into a continuous stream when the packets are received at irregular intervals.

Latency

Latency is the amount of time it takes for a discrete event to occur.

Bandwidth

Bandwidth is a measure of information carrying capacity available for a transmission medium. The greater the bandwidth the more information that can be sent in a given amount of time. Bandwidth is expressed in bits per second (bps).

Network performance utilities

Two common network performance utilities, Packet InterNet Groper (PING) and Traceroute, are described in this section. Other utilities can be used to gather information about IP Trunk 3.01 (and later) network performance.

> ***Note:*** These descriptions are for reference purposes only. Traceroute is not part of the IP Trunk 3.01 (and later) product.

Because network conditions can vary over time, collect performance data over a period of at least four hours. Use performance utilities to measure network performance from each IP Trunk 3.01 (and later) node to every other IP Trunk 3.01 (and later) node in the network.

Packet InterNet Groper (PING)

Packet InterNet Groper (PING) sends an Internet Control Message Protocol (ICMP) echo request message to a host, expecting an ICMP echo reply. This allows the measurement of the round-trip time to a selected host. By sending repeated ICMP echo request messages, the percentage of packet loss for a route can be measured.

Traceroute

Traceroute uses the IP Time-To-Live (TTL) field to forward router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. It must, instead, discard the packet and return an ICMP “time exceeded” message to the originating IP address. Traceroute uses this mechanism by sending an IP datagram with a TTL of 1 to the specified destination host. The first router to handle the datagram returns a “time exceeded” message. This identifies the first router on the route. Traceroute sends out a datagram with a TTL of 2. This causes the second router on the route to return a “time exceeded” message, and so on, until all hops have been identified. The Traceroute IP datagram has a port number unlikely to be in use at the destination (usually >30,000). This causes the destination to return a “port unreachable” ICMP packet which identifies the destination host. Traceroute can be used to measure round-trip times to all hops along a route, identifying bottlenecks in the network.

E-Model

IP Trunk 3.01 (and later) uses the E-Model, a method similar to the ITU-T Recommendation G.107, to determine voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating, R, for the network transmission quality. IP Trunk 3.01 (and later) uses a simplified version of the model to correlate the network QoS to the subjective Mean Opinion Score (MOS).

MOS is a numerical scale used to rate voice quality. When MOS is equal to 5.0, voice quality is good. When MOS is equal to 0.0, voice quality is bad.

For packet loss over 16%, the MOS value is set to 0, and the remote node is considered to be in fallback mode.

End-to-end latency

IP Trunk 3.01 (and later) network end-to-end latency consists of several components: routing delay on the IP Trunk 3.01 (and later) network, frame duration delay and jitter buffer delay on the codec, and delay on the circuit-switched network. The determination of end-to-end delay depends on the dynamics of the IP Trunk 3.01 (and later) network and the detailed service specification.

MOS values are calculated based on the routing delay and frame duration and jitter buffer delay on the codec. These latencies must be taken into consideration during the engineering of the total network’s latency. If the end-to-end latency of the network is specified and the latency of the PSTN circuit-switched components is removed, the remainder is the latency available for the IP trunks. This latency value plays a large role when configuring IP Trunk 3.01 (and later) node QoS values in OTM.

For instance, assume the end-to-end network latency is 300 milliseconds (ms) and the part of that latency which the IP network contributes is 180 ms. Furthermore, assume the network has low packet loss. Using the G.711 codec, this means the configured QoS can be a minimum of 4.3. If the latency in the IP network increases, the configured QoS is not met and fallback to alternate facilities occurs.

Equipment Impairment factor

Equipment Impairment factors are important parameters used for transmission planning purposes. They are applicable for the E-Model.

> ***Note:*** For information on QoS engineering guidelines, refer to "ITG engineering guidelines" on page 125.

Fallback to alternate facilities

IP Trunk 3.01 (and later) continuously monitors and analyzes QoS data. When IP Trunk 3.01 (and later) detects IP network congestion, and the QoS is below a pre-defined value, new calls routed to the remote gateway are rejected. Instead, the Meridian 1/CS 1000M routes them over non-IP facilities. The Stepback on Congestion over ISDN feature provides fallback to alternate facilities functionality.

Triggering fallback to alternate trunk facilities

A key background activity of IP Trunk 3.01 (and later) is to monitor the network's QoS between itself and each remote IP gateway configured in the dialing plan. When the QoS is below the defined acceptable level for a given IP Trunk 3.01 (and later) destination node, all outgoing calls from the near-end Meridian 1/CS 1000M to the far end Leader are re-routed through alternate circuit-switched trunk facilities. All calls that the switch is trying to set up are re-rerouted; established calls cannot fall back.

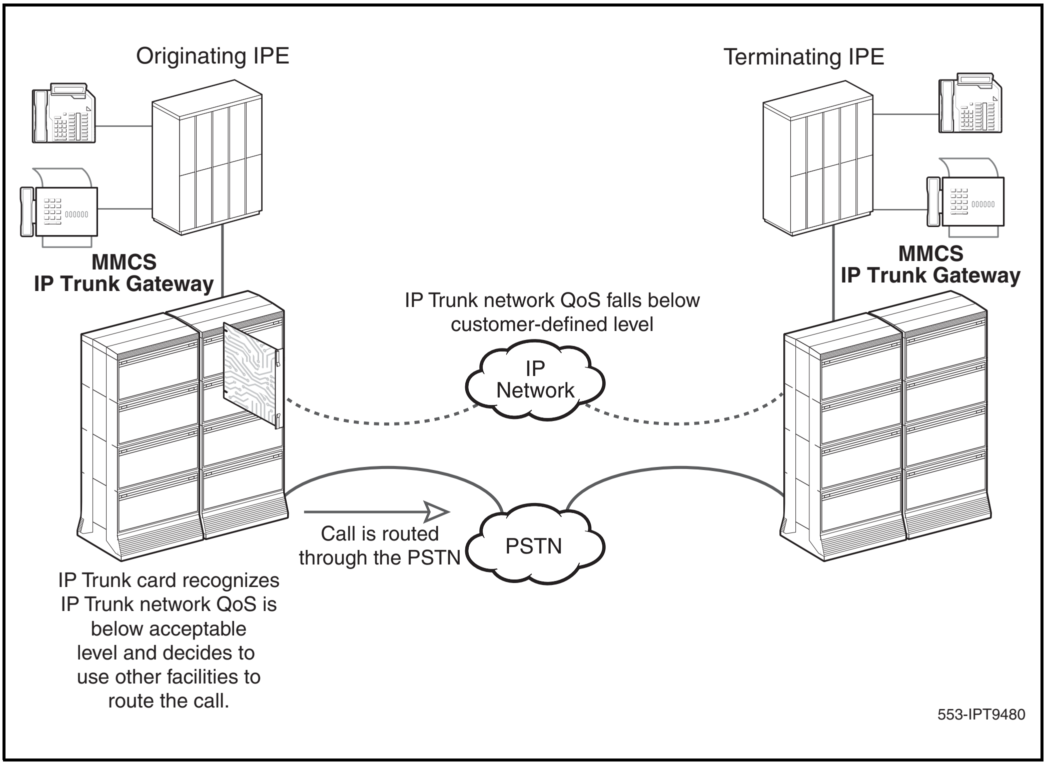
The Meridian 1/CS 1000M provides alternate routing based on BARS or NARS. BARS/NARS translates the dialed LOC, NPA, NXX, or Special Number (SPN) into an entry on the Route List Block (RLB) and searches the trunks in the associated Route Data Block (RDB).

The trigger for fallback to alternate trunk facilities is defined per call, per customer. The local Active Leader makes the decision to use the fallback feature. The selection of routes is based on the customer-configured database. The customer must configure the alternate routing to the PSTN in the Meridian 1/CS 1000M database.

The fallback to alternate facilities uses an ISDN DCH mechanism. The Step Back on Congestion over ISDN feature provides fallback to alternate trunk facilities functionality. When the Meridian 1/CS 1000M presents an outgoing call and receives a release message back that indicates network problems, Stepback on Congestion allows a new route to be found for the call (for instance, the PSTN). The route selected depends on the customer's database. If an alternate route is not configured in the route list, the calls rejected by IP Trunk 3.01 (and later) is routed to some other treatment. Fallback is optional, based on the configuration of the route list.

Figure 22 on page 111 shows the fallback to alternate facilities functionality.

Figure 22
Example of a fallback to alternate facilities situation


Originating IPE
Terminating IPE
MMCS
IP Trunk Gateway
MMCS
IP Trunk Gateway
IP Trunk network QoS falls below customer-defined level
IP Network
PSTN
Call is routed through the PSTN
IP Trunk card recognizes IP Trunk network QoS is below acceptable level and decides to use other facilities to route the call.
553-IPT9480

Fallback in IP Trunk 3.01 (and later)

In QoS monitoring, the local node queries the remote node and gets a response; the remote node queries the local node and gets a response. If the remote node cannot query the local node, QoS monitoring is not available. When an IP Trunk 3.01 (and later) node uses a Gatekeeper to resolve an address, IP Trunk 3.01 (and later) cannot monitor QoS and provide fallback. This function resides with the device resolving the address.

As a result, for all calls going to the Gatekeeper, such as in IP Peer Networking, no fallback can occur. The call either goes through with possibly a lower QoS, or the call clears instead of falling back. All QoS control is in the hands of the Gatekeeper.

However, for calls using the ATPM static address tables, the IP Trunk 3.01 (and later) Leader retains awareness of network status and can cause fallback to the PBX, if needed.

The full QoS fallback function is available for locally provisioned addresses.

IP Peer and Qos

The IP Peer Networking nodes do not support QoS monitoring. The capability must be enabled for both sides in order for it to work, but it cannot be enabled for IP Peer Networking. Therefore, do not enable QoS monitoring for any numbers terminating on an IP Peer Networking node. If this is done, the IP Peer Networking node is unreachable for that IP Trunk 3.01 (and later) node.

IP Trunk 3.01 (and later) nodes can perform QoS monitoring only on remote IP Trunk 3.01 (and later) nodes provisioned locally with SL1, SL1 with ESN5, or CS 1000S node capabilities.

Return to the IP network

Unless the DCH is down and all trunks appear busy to the system, outgoing calls are introduced to the IP Trunk 3.01 (and later) node. Each call is tested against the outgoing address translation and Quality of Service (QoS) for the destination node. After the QoS returns to an acceptable level, all new outgoing calls are again routed through the IP network. The call connections that were established under the fallback to alternate facilities condition are not affected.

Type of Service

The IP packet handler has a byte of data for Type of Service (ToS). This byte allows the user to indicate a packet’s priority so that routers can more efficiently handle data packets. For example, a router can decide to queue low priority data while immediately passing packets marked as high priority.

The OTM User Interface allows two ToS values to be configured: data and control. Data packets transmit the voice or fax call's data, while control packets setup and maintain the call. Both can be configured for any value in the range of 0 – 255 (0 is the default). When an IP Trunk 3.01 (and later) node is configured, ToS bits are initially set to default values. The OTM 2.1 (and later) IP Trunk 3.01 (and later) node administration interface allows the customer to configure these bits for potentially better interworking with different manufacturers' routing equipment. The extent of any improvement from setting these ToS bits depends on the network routing equipment. Improvements can vary depending on the router's prioritization algorithms.

The data ToS is placed in every voice or fax data packet sent from the IP trunk card. To optimize the speech quality, ToS is usually configured for low-latency and high-priority.

The control ToS is placed in every signaling message packet sent from the IP trunk card. Signaling links use Transmission Control Protocol (TCP) which provides a retransmission mechanism. In addition, the latency of the control packets is not as critical as it is for the data packets.

Each entry in the routing table has a configurable ToS. ToS values are configured in the DSP Profile window. For a route entry to be selected for an outgoing packet, both the configured route and the ToS must match. Two cases must be considered: local subnet traffic and remote traffic.

The remote subnet packets is the H.323 call data for an IP Trunk 3.01 (and later) node which is not on the local subnet and must go through a router. There is a default gateway entry (0.0.0.0) that specifies the gateway address for this traffic. The ToS does not matter for this route. If the route and ToS do not match any of the other route entries, the packet is routed here. The entry is configured for the TLAN network interface.

Local subnet packets is the H.323 call data intended for another IP Trunk 3.01 (and later) node connected to the same subnet. This can be the immediate subnet. For traffic to be sent on the local subnet, the routing table entry for the TLAN network interface must be selected. Each table entry (except the default route) has a ToS value configured against it. Since there are two ToS values configured (one for control data and one for voice data), there must be two route entries for the local subnet in the table.

If both table entries are not present, a condition occurs where packets for voice, control, or both can be sent to the default route because the ToS does not match the local subnet entry. These packets go to the router and then back on the subnet, wasting router resources and increasing traffic on the subnet.

The IP trunk card configures two route table entries for the local subnet if a different ToS is configured for the voice and control packets. Otherwise, a single entry is created.

CAUTION — Service Interruption

Only technical personnel with detailed knowledge of router capabilities should make changes to ToS. Improper changes to ToS can degrade network performance.

Fax support

The IP trunk card transfers T.30 protocol (G3 Fax) implementations over the IP network. Near real-time operational mode is supported where two T.30 facsimile terminals are able to engage in a document transmission in which the T.30 protocol is preserved.

The trunk uses the T.38 protocol on the connection between a pair of IP Trunk 3.01 (and later) nodes.

The call acts in the same way as a gateway-to-gateway H.323 call. The call is set up using the normal voice call process (that is, the normal voice call codec negotiation process occurs and the corresponding codec payload size and jitter buffer values are used). When the call setup is complete, the two G3 Fax terminals are linked. The DSP detects the fax call setup tones and switches to handle the fax call. For the remainder of the call, the parameters administered for the fax call are used (for example, payload size).

Some implications of the fax call setup process are as follows:

- a voice codec must be configured, even if only fax calls will be made
- both ends of the call must be able to negotiate to a common voice codec for the calls to be successful

All T.30 session establishment and capabilities negotiation are carried out between the telephones through the IP trunk cards over the IP Trunk 3.01 (and later) network using the T.38 protocol. In terms of the internet fax service roles, the IP trunk card acts as both the fax on-ramp gateway and the fax off-ramp gateway, depending on the call direction.

The on-ramp gateway demodulates the T.30 transmission received from the originating G3 Fax terminal. The T.30 facsimile control and image data is transferred in an octet stream structure, using a Real Time Protocol (RTP) payload, over User Datagram Protocol (UDP) transport mechanism.

Signaling specified by H.323 V.2 protocol is used for IP Trunk 3.01 (and later) to IP Trunk 3.01 (and later) call setup.

Modules supporting facsimile transmission are responsible for the following:

- fax speed detection and adjustment
- protocol conversion from G3 Fax to RTP payload for fax data transfer
- T.30 fax protocol support
- T.38 fax-over-IP protocol
- V.21 channel 2 binary signaling modulation and demodulation
- High-level Data Link Control (HDLC) framing
- V.27 term (2400/4800 bps) high speed data modulation and demodulation
- V.29 (7200/9600 bps) high speed data modulation and demodulation
- V.17 (14390 bps) high speed data modulation
- V.21 channel 2 detection
- Multi-channel operation support

  Note: If two ends support T.30 protocol, they are compatible only if external factors (for instance, delay and signal quality) permit. Only IP Trunk 3.01 (and later) node fax calls are supported.

  Note: IP Trunk 3.01 (and later) supports a maximum fax speed of 14.4 Kbps.

Remote Access

Remote Access is supported on IP Trunk 3.01 (and later). Remote Access allows an OTM user with no IP Trunk 3.01 (and later) data, including Nortel support personnel, to manage the IP trunk card remotely.

Management and support of the IP Trunk 3.01 (and later) network depend on IP networking protocols including SNMP, FTP, and Telnet. The Nortel Netgear RM356 modem router or equivalent should be installed on the ELAN subnet in order to provide remote support access for IP Trunk 3.01 (and later) and other IP-enabled Nortel products.

The Nortel Netgear RM356 modem router integrates the functions of a V.90 modem, a PPP remote access server, an IP router, and a 4-port 10BaseT Ethernet hub, and provides a range of security features that may be configured so as to comply with the customer's data network security policy.

> ***Note:*** Do not install a modem router on the ELAN subnet without the explicit approval of the customer's IP network manager. The RM356 modem router is not secure unless it is configured correctly according to the customer's network security policy and practices.

Alternatively, the PC application, pcANYWHERE$^{©}$, can be installed in host mode on the OTM PC to provide remote access to any PC with a modem. The remote user dials the OTM PC which contains the required IP Trunk 3.01 (and later) data (whether stored locally or on an OTM server). Once connected, the remote user can perform any operation available to that PC.

Per-call statistics support using RADIUS Client

The IP Trunk 3.01 (and later) architecture isolates the TLAN network interface from the system. However, the system does not have direct access to per-call statistics on the voice quality of the call. These statistics are important for the purpose of the following:

- make sure the network is providing the contractual service level
- solve help desk inquiries or refund “bad call” charges
- identify network problems and track network performance

IP Trunk 3.01 (and later) uses a Remote Authentication Dial In User Service (RADIUS) client to transmit these statistics from the IP trunk card to a network device:

- The IP trunk card sends a Start record when a call begins.
- The IP trunk card sends an End record when the call is released.
- The End record contains QoS information and the amount of data sent.
- Both records contain the Called and Calling Party numbers for call identification.
- The OTM Call Accounting application does not correlate RADIUS per call statistics with the Meridian 1/CS 1000M CDR.

A network “listener” receives Start and End messages and stores the data. Applications can retrieve the stored data for processing and presentation to the user.

A RADIUS client on the IP trunk card allows per-call statistics of the IP network call to be sent from the cards to a network listener. The client is based on RFC2139, which defines the accounting portion of the RADIUS protocol. The IP trunk card uses the authentication algorithm based on RFC1321.

Configuration

Use OTM 2.1 (and later) to configure the following RADIUS parameters:

- enable/disable RADIUS record generation
- IP address of the RADIUS listener
- IP port number of the RADIUS listener
- key for authenticating RADIUS records (the key is maintained between the RADIUS client and the RADIUS server)

Data is configured at the IP Trunk 3.01 (and later) node level and is distributed to all the IP trunk cards associated with the IP Trunk 3.01 (and later) node.

Messaging

The RADIUS client sends two records to the network listener: one when the call is answered and one at the end of the call. The messages are sent by the Follower card which processes the voice call (not the DCHIP or Leader if they are not handling the voice data). The RADIUS protocol uses UDP for message exchange. The client sends a message to the listener and waits for an acknowledgment. If no acknowledgment is received, the client re-transmits the record using the standard exponential backoff theme. The data is stored on the IP trunk card until an acknowledgment is received. When an acknowledgment is received, the data is discarded. The client stores a maximum of 100 records. This allows two Start and two End records for each of the 24 or 32 ports (depending on whether it is an ITG-Pentium 24-port trunk card or a Media Card 32-port trunk card).

Start record

The Start record is sent when the call is answered. It contains the following fields:

- Calling party number
- Originating IP address and port
- Called party number
- Destination IP address and port (of the actual card handling the call, not the remote Leader)
- Call start time
- Call duration (time from call initiation to call answer)
- Codec used
- Orig/Term call side indication
- Snapshot of remote Gateway’s QoS at time of call connect

The calling and called numbers (with their corresponding IP addresses) are just that, regardless of which end is doing the originating. So the Follower card on the originating side generates a RADIUS record with its own IP address as the originating IP address. The terminating Follower also generates a RADIUS record with that far end’s IP address as the originating IP address and its own IP address as the destination address.

If the call is not answered or is rejected, only an End record is generated.

End record

The End record is sent when the call is released. It contains the following fields:

- Calling party number
- Originating IP address and port
- Called party number
- Destination IP address and port (of the actual card handling the call, not the remote Leader)
- Call start time
- Call duration (time from call answer to call release)
- Codec used
- Orig/Term call side indication
- Number of bytes transferred (sent octets/packets)
- Number of packets transferred (sent octets/packets)
- Snapshot of latency seen at the end of the call
- Packet loss
- Snapshot of remote Gateway’s QoS at time of call release

The End record is also sent for calls which are not answered or are rejected. These records do not include the packet loss, number of bytes transferred, number of packets transferred and latency.

SNMP MIB

SNMP is the protocol used to communicate OTM IP Trunk 3.01 (and later) alarms or events. Support for the SNMP Management Information Bases (MIB) on the IP trunk card is composed of two parts: the standard MIB-2 and extensions for the IP trunk card.

MIB-2 support

Support of MIB-2 is enabled by the use of the WindRiver SNMP agent, WindNet©. The WindNet© agent supports the following MIB-2 groups:

- system
- interfaces
- AT
- IP
- Internet Control Message Protocol (ICMP)
- TCP
- UDP
- SNMP

The WindNet agent supports both SNMP-V1 and V2c protocols.

IP Trunk 3.01 (and later) SNMP agent

The SNMP agent supports the Operation, Administration, and Maintenance (OA&M) of IP Trunk 3.01 (and later), using OTM 2.1 (and later). It can configure the IP trunk card through file transfer services. The agent supports the SNMP-V1 protocol.

The SNMP agent provides the following capabilities:

- Retrieval of system wide variables, such as:
  - card state
  - number of DSPs on the card
  - number of available voice channels
  - IP addresses
  - software version
  - number of IP Trunk 3.01 (and later) nodes in fallback (that is, PSTN operation)

- Control of D-channel state, such as:
  - enable
  - disable
  - release
  - establish
- Retrieval of DSP information, such as:
  - DSP firmware
  - DSP self-test status
  - card reset
- SNMP configuration (that is, community names and trap subscription)
  - alarm generation through SNMP traps
- File transfer, including configuration files, software upgrade, dialing plan files, bootp files, activity log, and call trace files

Codec profiles

Codec refers to the voice coding and compression algorithm used by the DSPs on the IP trunk card. The G.XXX series of codecs are standards defined by the International Telecommunications Union (ITU). Different codecs have different QoS and compression properties. The specific codecs and the order in which they are to be used for codec negotiation is configured in OTM 2.1 (and later).

When configuring the IP Trunk 3.01 (and later) node in OTM 2.1 (and later), select the image containing the needed codecs, and the preferred codec negotiation order. The final codec used is determined by the codec negotiation process with the far end during call setup. Parameters can be configured for each codec in an image.

IP Trunk 3.01 (and later) supports the following codecs:

- G.711
- G.729AB

- G.729B
- G.723.1

G.711

The G.711 codec delivers “toll quality” audio at 64 kbit/s. This codec is optimal for speech quality, as it has the smallest delay and is resilient to channel errors. However, it uses the largest bandwidth. The G.711 codec is the default codec if the preferred codec of the originating node is not available on the destination IP Trunk 3.01 (and later) node. Voice Activity Detection/Silence Suppression is configurable through OTM 2.1 (and later). An ITG-Pentium 24-port trunk card supports 24 channels per card with G.711. A Media Card 32-port trunk card supports 32 channels per card with G.711.

G.729AB

The G.729AB codec is the default preferred codec when adding a new IP Trunk 3.01 (and later) node in OTM 2.1 (and later). This codec provides near toll-quality voice at a low delay. The G.729AB codec uses compression at 8 kbit/s (8:1 compression rate). Optional B Voice Activity Detection/Silence Suppression is configurable through OTM 2.1 (and later). An ITG-Pentium 24-port trunk card supports 24 channels per card with G.729AB. A Media Card 32-port trunk card supports 32 channels per card with G.729AB.

G.729B

The G.729B codec uses compression at 8 kbit/s (8:1 compression rate). Optional B Voice Activity Detection/Silence Suppression is configurable through OTM 2.1 (and later). An ITG-Pentium 24-port trunk card supports only 16 channels per card with G.729B due to higher DSP resources required for this codec. The Media Card 32-port trunk card does not support G.729B.

G.723.1 (5.3 kbit/s or 6.3 kbit/s)

The G.723.1 codec provides the greatest compression. Voice Activity Detection/Silence Suppression is configurable through OTM 2.1 (and later). An ITG-Pentium 24-port trunk card supports 24 channels per card with

G.723.1. A Media Card 32-port trunk card supports 32 channels per card with G.723.1.

Three downloadable DSP profiles support the codecs shown in Table 10.

Table 10
Codecs supported by IP Trunk 3.01 (and later)

Profile 1 **32 ms. Echo Cancel Tail** **24 ports/card for ITG-P 24-port card** **32 ports/card for SMC 32-port card**	**Profile 2** **32 ms. Echo Cancel Tail** **24 ports/card for ITG-P 24-port card** **32 ports/card for SMC 32-port card**	**Profile 3** **32 ms. Echo Cancel Tail** **16 ports/card for ITG-P 24-port card** **Not supported for SMC 32-port card**
PCM A-law (G.711)	PCM A-law (G.711)	PCM A-law (G.711)
PCM μ-law (G.711)	PCM μ-law (G.711)	PCM μ-law (G.711)
G.729AB	G.723.1 5.3 kbit/s	G.729B
Clear Channel	G.723.1 6.3 kbit/s	Clear Channel
Fax	Clear Channel	Fax
	Fax	

Each codec supports one of three sets of parameters: one for DSP, one for fax, and one for codec.

WARNING

The Media Card 32-port trunk card does not support Profile 3.

Security passwords

When Telneting into the ELAN network interface or using the debug port, a password must be entered when prompted. Two levels of passwords are used to prevent unauthorized data access. Unauthorized data access occurs when an unauthorized individual is able to view or modify confidential data, such as employee lists, password lists, and electronic mail. This information can be used to bypass Direct Inward System Access (DISA) restrictions and avoid charges.

The following are the two levels of passwords for IP Trunk 3.01 (and later):

- Administrator level
- Technical support level

Administrator level

The Administrator level is the most basic level of password. It provides unrestricted access to all IP Trunk administration options and to most of the IP trunk card level administration options. It does not, however, allow any type of low-level diagnostics to be performed.

Technical support level

The Technical support level is for use by Nortel personnel only. It allows low-level message monitoring and factory testing.

ITG engineering guidelines

Contents

This section contains information on the following topics:

Introduction

The Meridian Integrated IP Telephony Gateway (ITG) system performs the following actions:

- compresses PCM voice
- demodulates Group 3 fax
- routes the packetized data over a private internet, or intranet
- provides virtual analog ISDN Signalling Link (ISL) TIE trunks between Meridian 1 ESN nodes
- enables interworking with other Nortel VoIP products such as CS 1000S, CS 1000M, and Business Communication Manager (BCM)

IP Trunk 3.01 (and later) routes voice traffic over existing private IP network facilities with available under-used bandwidth on the private WAN backbone.

IP Trunk 3.01 (and later) is targeted towards the Enterprise customer who has a Meridian 1/CS 1000M system installed for providing corporate voice services and an intranet for corporate data services. A customer is expected to use the IP Trunk 3.01 system to move traffic from a PSTN-based network to the intranet. Voice and fax services which depended on circuit-switched and Time Division Multiplexing (TDM) technology are transported using packet-switched and statistical multiplexing technology.

This chapter provides guidelines for designing a network of IP Trunk 3.01 (and later) nodes over the corporate intranet. It describes how to qualify the corporate intranet to support an IP Trunk 3.01 (and later) network and how to determine changes required to maintain the quality of voice services when moving those services from the PSTN. It addresses requirements for the successful integration with the customer's existing LAN. By following these guidelines, the IP Trunk 3.01 (and later) network can be designed so that the cost and quality tradeoff is at best imperceptible and at worst within a calculated tolerance.

> ***Note:*** Pre-installation analysis of the data network enables IP Trunk 3.0 (and later) to be provisioned correctly. For proper analysis and deployment, obtain a network diagram or a description of the network topology and hierarchy. Nortel recommends using a data network analyzer (for example, Sniffer™) for evaluation and troubleshooting.

Audience

This chapter is intended for telecom and datacom engineers who design and install the IP Trunk 3.01 (and later) node portion of the VoIP network. It is assumed that the telecom engineer is familiar with engineering the Meridian 1/CS 1000 system and obtaining system voice and fax traffic statistics. It is assumed that the datacom engineer is familiar with the intranet architecture, LAN installations, tools for collecting and analyzing data network statistics, and data network management systems.

For information on designing a Meridian 1/ CS 1000 network, refer to the following NTP:

- *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120)

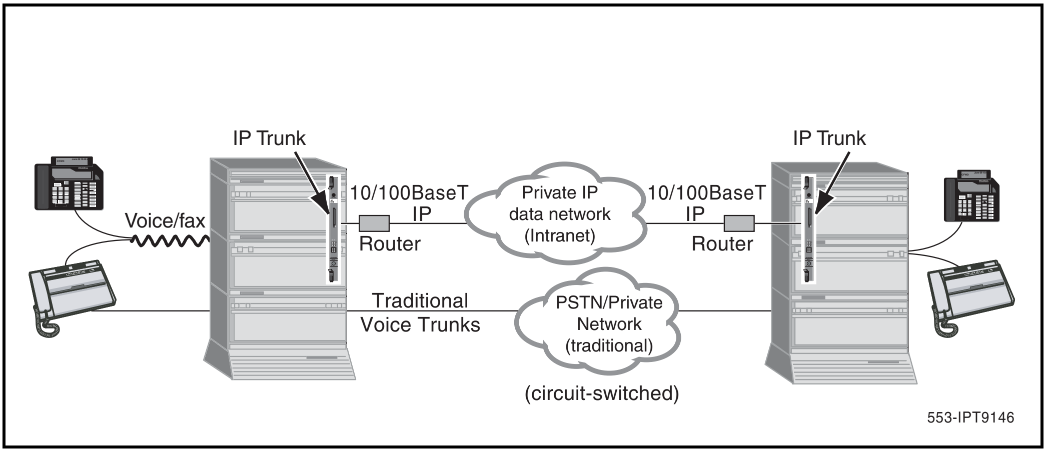
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)
- *Communication Server 1000S: Planning and Engineering* (553-3031-120)
- *Communication Server 1000E: Planning and Engineering* (553-3041-120)

Equipment requirements

The IP Trunk 3.01 (and later) system was designed for operation on a well-provisioned, stable LAN. Delay, delay variation or jitter, and packet loss must be minimized end-to-end across the LAN and WAN. The design and configuration of the LAN and WAN that link the IP Trunk 3.01 (and later) system must be determined. If the intranet becomes overloaded, new calls to the IP Trunk 3.01 (and later) system fall back to normal circuit-switched voice facilities so that the Quality of Service (QoS) does not degrade for new calls.

IP Trunk 3.01 (and later) is for intranet use only. IP Trunk 3.01 (and later) provides virtual analog ISL TIE trunks between two Meridian 1 systems in an ESN network, as shown in Figure 23. IP Trunk 3.01 (and later) does not support modem traffic except for Group 3 fax. The technician must configure the Meridian 1/ CS 1000M routing controls to route modem traffic over circuit-switched trunks instead of over IP Trunk 3.01 (and later).

Figure 23
The IP Trunk 3.01 (and later) intranet



IP Trunk 3.01 (and later) is available for the following systems running CS 1000 Release 4.0 software:

- Meridian 1 PBX 61C CP PII
- Meridian 1 PBX 81C CP PII
- Meridian 1 PBX 11C Chassis
- CS 1000M SG
- CS 1000M MG
- CS 1000M Cabinet
- CS 1000M Chassis

The IPE trunk cards plug into the Meridian 1/CS 1000M IPE shelf.

A maximum of eight ITG-Pentium 24-port trunk cards can fit on one IPE shelf. Each card takes up two slots on the IPE shelf.

A maximum of 16 Media Card 32-port trunk cards can fit on one IPE shelf. Each IP trunk card takes up one slot on the IPE shelf. For Class B compliance to EMC regulations, only 10 Media Card 32-port trunk cards can be placed on an IPE shelf. For Class A compliance, there are no limitations on the

Media Card 32-port trunk card. For more information, see Appendix C: "Environmental and electrical regulatory data" on page 597.

An IPE shelf can contain a mixture of ITG-Pentium 24-port trunk cards and Media Card 32-port trunk cards.

Cabinet systems operating under Class B Electro-Magnetic Compatibility (EMC) standards can only hold a total of two IP Trunk cards, divided between the main and expansion cabinets. This can be extended to two cards in each main or expansion cabinet if all cabinets are separated from each other by at least ten meters distance. For Cabinet systems operating under Class A EMC standards, there are no restrictions.

For Meridian 1 Option 11C Cabinet, Meridian 1 PBX 11C Chassis, CS 1000M Cabinet, and CS 1000M Chassis systems, the SDI/DCH (NTAK02BB) card occupies one slot on the cabinet and is connected to the IP trunk card through the backplane. Only ports 1 and 3 are available for use as DCHI.

The IP trunk card uses a 10BaseT Ethernet network interface located on the card backplane I/O connector to carry IP Trunk 3.01 (and later) system management traffic; it connects to the ELAN subnet.

Scope

These engineering guidelines address the design of the IP Trunk 3.01 (and later) network, which consists of the following:

- IP Trunk 3.01 (and later) nodes
- Telephony LAN (TLAN) subnets to which the IP Trunk 3.01 (and later) nodes are connected
- A corporate intranet which interconnects the various TLAN subnets

These guidelines require that the customer has a corporate intranet in place that spans the sites where the IP Trunk 3.01 (and later) nodes are to be installed.

Network engineering guidelines overview

Previously, Meridian 1 networks depended on voice services such as LEC and IXC private lines. With IP Trunk 3.01 (and later) technology, the Meridian 1 and CS 1000 systems can select a new delivery mechanism, one that uses packet-switching over a data network or corporate intranet. The role of the IP Trunk 3.01 (and later) node is to convert steady-stream digital voice into fixed-length IP packets, provide ISDN signalling, and translate PSTN numbers into IP addresses. The IP packets are transported across the IP data network with a low latency that varies with strict limits.

> ***Note:*** The term “voice services” also includes fax services.

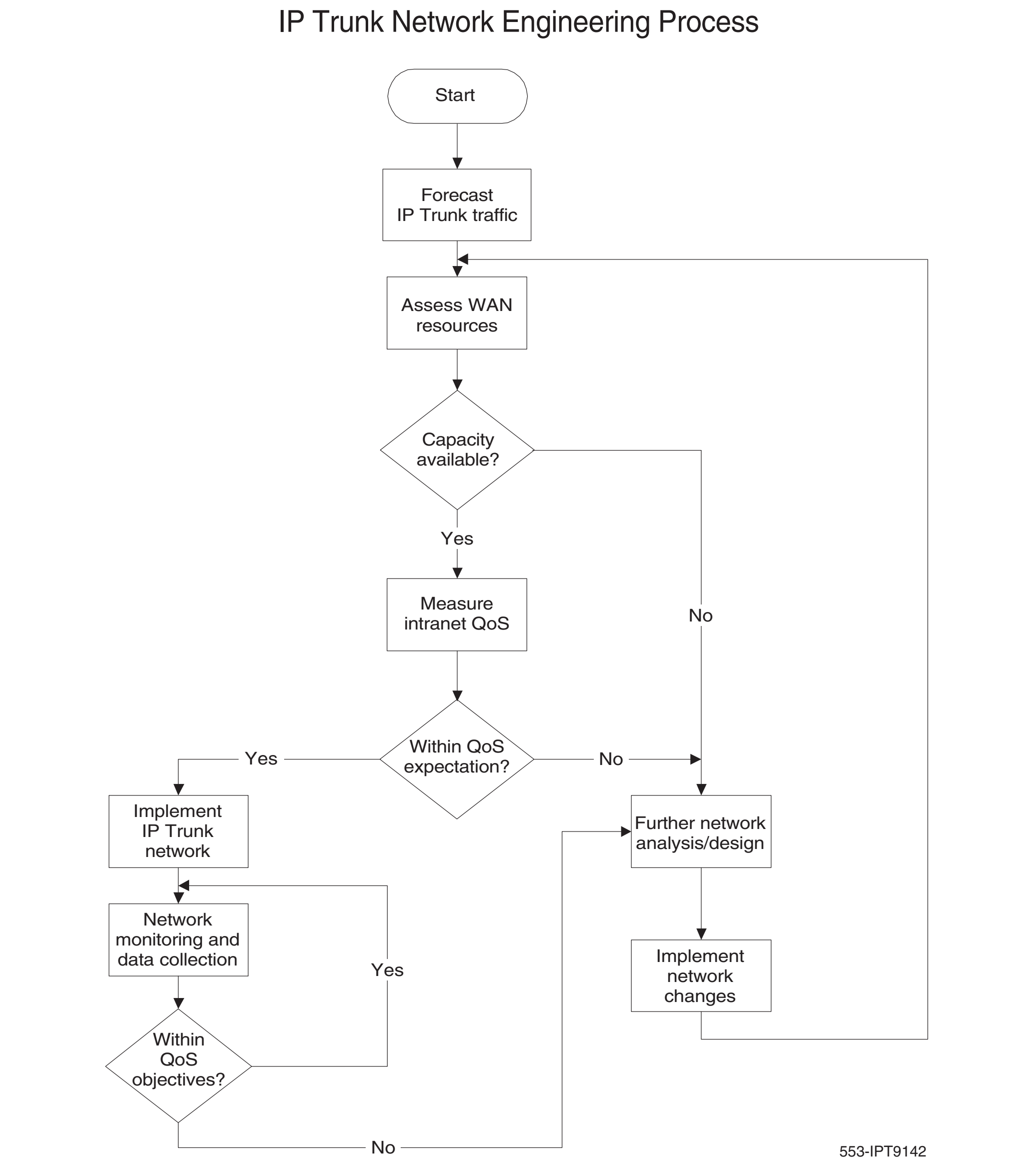
IP evolved from a protocol that allowed multi-vendor hosts to communicate. The protocol adopted packet-switching technology, providing bandwidth efficiency for bursty data traffic that can tolerate high latency and jitter (variation in latency). Since IP supported the TCP transport layer, which provided connection-oriented and reliable transport, IP took on the properties of being connectionless and a best-effort delivery mechanism. The TCP/IP paradigm worked well in supporting data applications at that time.

New considerations come into play now when the same corporate network is expected to deliver voice traffic. The intranet introduces impairments, delay, delay variation, and data packet loss, at levels that are higher than those delivered by voice networks. Delay between talker and listener changes the dynamics and reduces the efficiency of conversations, while delay variation and packet errors causes introduces glitches in conversation.

Connecting the IP Trunk 3.01 (and later) nodes to the corporate intranet without preliminary assessments and QoS mechanisms can result in unacceptable degradation in voice service. Correct design procedures and principles must be considered.

A good design for the IP Trunk 3.01 (and later) network must begin with an understanding of traffic and the underlying network that will transmit the traffic. See Figure 24 on page 133.

Figure 24
IP Trunk 3.01 (and later) network engineering process


IP Trunk Network Engineering Process
Start
Forecast IP Trunk traffic
Assess WAN resources
Capacity available?
Yes
No
Measure intranet QoS
Within QoS expectation?
Yes
No
Implement IP Trunk network
Further network analysis/design
Network monitoring and data collection
Yes
Implement network changes
Within QoS objectives?
No
553-IPT9142

Three preliminary steps must be undertaken.

1 Calculate IP Trunk 3.01 (and later) traffic. Estimate the amount of traffic that the system will route through the IP Trunk 3.01 (and later) network. This total must include the estimated traffic between the IP trunk cards and the Signaling Server. This in turn places a traffic load on the corporate intranet. This is described in “IP Trunk 3.01 (and later) traffic engineering” on page 134.

2 Assess WAN link resources. If resources in the corporate intranet are not sufficient to adequately support voice services, the cause is usually insufficient WAN resources. “Assess WAN link resources” on page 169 outlines how this assessment can be made.

3 Measure the existing intranet's Quality of Service (QoS). Estimate the quality of voice service the corporate intranet can deliver. “Measure intranet QoS” on page 191 describes how to measure prevailing delay and error characteristics of an intranet.

After the assessment phase, the IP Trunk 3.01 (and later) network can be designed and implemented. This design not only involves the IP Trunk 3.01 (and later) elements, but can also require making design changes to the existing customer intranet. “Fine-tune network QoS” on page 182 and “Implement QoS in IP networks” on page 175 provide guidelines for making modifications to the intranet.

IP Trunk 3.01 (and later) traffic engineering

To design a network is to size the network so that it can accept a calculated amount of traffic. The purpose of the IP Trunk 3.01 (and later) network is to deliver voice traffic that meets QoS objectives. Since traffic determines network design, the design process must start with obtaining an offered IP Trunk 3.01 (and later) traffic forecast. The traffic forecast drives drive the following:

- IP Trunk 3.01 (and later) hardware requirements
- WAN requirements
- TLAN subnet requirements

Traffic forecasting is a process that often requires several tries to achieve satisfactory results. For example, a WAN might not have enough bandwidth to support all the IP trunks required; therefore the codec choice or the number of trunks provisioned must be adjusted.

Estimate voice traffic calculations

Follow the steps in Procedure 4 to calculate an estimate of voice traffic.

Procedure 4
Estimating voice traffic

1 Calculate Voice on IP traffic.

CCS/user=# of calls/ * Average Holding Time (in seconds)/100

Total voice CCS (Tv) = CCS/user x No. of VoIP users

The number of VoIP users (telephones) is the potential population in the system that can generate/receive traffic through the IP Trunk 3.01 (and later) node. This number may be estimated for a new Meridian 1 customer.

If the installation is for an existing customer, base the VoIP traffic on measured route traffic from traffic report TFC002, which provides CCS for each route. A customer must determine the amount of expected private network voice traffic.

2 Calculate Fax on IP traffic

CCS/user sending fax = # of pages sent/fax * Average Time to send a page (default 48 seconds)/100

CCS/user receiving fax = # of pages received/fax * Average Time to receive a page (default 48 seconds)/100

Total fax CCS (Tx) = CCS/fax sent*No. of users sending fax + CCS/fax received* No. of users receiving fax

The user sending or receiving a fax can be the same person or different persons. It is the number of faxed documents and the average number of pages per faxed document that are important. The time unit for fax traffic is also the busy hour. The busy hour selected must be the hour that gives the highest combined voice and fax traffic.

3 Total the ITG CCS.

Total IP Trunk 3.01 (and later) traffic (T) = Tv + Tx

4 Refer to Poisson P.01 table to find IP Trunk 3.01 (and later) ports required to provide a blocking Grade of Service of 1% assuming Poisson random distribution of call origination and zero correlation among calls.

Note: A lower Grade of Service, such as P.10, may be preferred if overflow routing is available through the PSTN, circuit-switched VPN, or ITG ISL TIE trunks.

For P.01 blocking Grade of Service, the number of trunks (IP Trunk 3.01 (and later) ports) in Table 11 on page 139 which provides a CCS higher than T is the solution. For P.10 blocking Grade of Service, refer to Table 12 on page 140.

5 Calculate bandwidth output. Refer to Table 18 on page 158 (Silence Suppression disabled). Tv/36 and Tx/36 indicate the average number of simultaneous callers.

Note: This calculation requires perfectly queued and perfectly smooth traffic.

Tv/36*bandwidth output per port = voice bandwidth per node (Bv)

Tx/36*bandwidth output per port = fax bandwidth per node (Bx)

Total bandwidth (Bt) = Bv + Bx

For WAN calculation, consider only the larger of fax traffic sent or received.

6 Adjust requirement for traffic peaking.

Peak hour bandwidth per node = Bt*1.3 (default)

End of Procedure

Procedure 5 on page 137 is used to calculate IP Trunk 3.01 (and later) port and, therefore, IP network bandwidth requirements. In the WAN environment, the traffic parcel is defined for each destination pair (route). The total node traffic should be sub-divided into destination pair traffic. The rest of the calculation procedure continues to apply.

Example 1:
IP Trunk 3.01 (and later) ports and bandwidth engineering (Silence Suppression enabled)

In this configuration example of 120 VoIP users, each user generates four calls using the IP network (originating and terminating) with an average holding time of 150 seconds in the busy hour.

In the same hour, 25 faxes were sent and 20 faxes received. The faxes sent averaged 3 pages, while the faxes received averaged 5 pages. The average time to set up and complete a fax page delivery is 48 seconds.

The codec of choice is G.729AB, voice packet payload is 30 ms.
The fax modem speed is 14.4 kbit/s and payload is 16.6 ms. How many IP Trunk 3.01 (and later) ports are needed to meet P.01 blocking Grade of Service? What is the traffic in kbit/s generated by this node to the TLAN subnet?

Follow the steps in Procedure 5 to calculate IP Trunk 3.01 (and later) port and bandwidth requirements.

Procedure 5
Calculating IP Trunk 3.01 (and later) port and bandwidth requirements

1 Calculate VoIP traffic during busy hour.

CCS/user = 4*150/100 = 6 CCS

Tv = 120*6 = 720 CCS

2 Calculate fax on IP traffic during busy hour.

CCS/fax sent = 3*48/100 = 1.44 CCS

CCS/fax received = 5*48/100 = 2.4 CCS

Total fax CCS (Tx + Rx) = 1.44*25 + 2.4*20 = 36+ 48= 84 CCS

3 Calculate IP Trunk 3.01 (and later) traffic during busy hour.

Total traffic (T) = Tv + Tx = 720 + 84 = 804 CCS

4 Refer to the Poisson P.01 table (Table 11 on page 139) to find the number of IP Trunk 3.01 (and later) ports required for 1% blocking Grade of Service. For P.10 blocking Grade of Service, refer to Table 12 on page 140.

804 CCS can be served by 35 IP Trunk 3.01 (and later) ports with P.01 blocking Grade of Service. Two ITG-Pentium 24-port trunk cards are needed to serve this customer.

5 Calculate average bandwidth use on the TLAN subnet.

For voice:

720/36*30.7 = 614 kbit/s

For fax:

84/36*46.1 =108 kbit/s

Total bandwidth = 614 + 108 = 722 kbit/s

6 Adjust requirement for traffic peaking

Peak hour bandwidth requirement = 722*1.3 = 939 kbit/s

This is the spare bandwidth a TLAN subnet requires to transmit the VoIP and fax traffic. Nortel recommends that the TLAN subnet handle IP Trunk 3.01 (and later) traffic exclusively.

End of Procedure

Note: This example is based on the G.729AB codec with 30 ms payload size and Silence Suppression enabled. For relations of user-selectable parameters such as payload size, codec type, packet size and QoS, refer to “Set QoS expectations” on page 192.

Calculate the number of IP Trunk 3.01 (and later) ports required

IP Trunk 3.01 (and later) TIE trunks are provisioned based on average busy-hour traffic tables, using the calculated amount of voice and fax traffic between IP Trunk 3.01 (and later) nodes. Table 11 shows the number of trunks required based on average busy hour CCS for a 1% blocking Grade of Service. Table 12 on page 140 shows the number of trunks required based on average busy-hour CCS for a 10% blocking Grade of Service.

> ***Note:*** A lower Grade of Service, such as P.10, might be preferred if overflow routing is available through the PSTN, circuit-switched VPN, or IP Trunk 3.01 (and later) TIE trunks.

Table 11
Trunk traffic – Poisson 1% blocking Grade of Service (Part 1 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	0.4	21	426	41	993	61	1595	81	2215
2	5.4	22	453	42	1023	62	1626	82	2247
3	15.7	23	480	43	1052	63	1657	83	2278
4	29.6	24	507	44	1082	64	1687	84	2310
5	46.1	25	535	45	1112	65	1718	85	2341
6	64	26	562	46	1142	66	1749	86	2373
7	84	27	590	47	1171	67	1780	87	2404
8	105	28	618	48	1201	68	1811	88	2436
9	126	29	647	49	1231	69	1842	89	2467
10	149	30	675	50	1261	70	1873	90	2499
11	172	31	703	51	1291	71	1904	91	2530
12	195	32	732	52	1322	72	1935	92	2563
13	220	33	760	53	1352	73	1966	93	2594
14	244	34	789	54	1382	74	1997	94	2625
15	269	35	818	55	1412	75	2028	95	2657
16	294	36	847	56	1443	76	2059	96	2689
17	320	37	876	57	1473	77	2091	97	2721
18	346	38	905	58	1504	78	2122	98	2752
19	373	39	935	59	1534	79	2153	99	2784
Note: For trunk traffic greater than 4427 CCS, allow 29.5 CCS per trunk.									

Table 11
Trunk traffic – Poisson 1% blocking Grade of Service (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
20	399	40	964	60	1565	80	2184	100	2816
101	2847	111	3166	121	3488	131	3810	141	4134
102	2879	112	3198	122	3520	132	3843	142	4167
103	2910	113	3230	123	3552	133	3875	143	4199
104	2942	114	3262	124	3594	134	3907	144	4231
105	2974	115	3294	125	3616	135	3939	145	4264
106	3006	116	3326	126	3648	136	3972	146	4297
107	3038	117	3359	127	3681	137	4004	147	4329
108	3070	118	3391	128	3713	138	4037	148	4362
109	3102	119	3424	129	3746	139	4070	149	4395
110	3135	120	3456	130	3778	140	4102	150	4427
Note: For trunk traffic greater than 4427 CCS, allow 29.5 CCS per trunk.									

Table 12
Trunk traffic – Poisson 10% blocking Grade of Service (Part 1 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	3.8	18	462	35	996	52	1548	69	2109
2	19.1	19	492	36	1028	53	1581	70	2142
3	39.6	20	523	37	1060	54	1614	71	2175
4	63	21	554	38	1092	55	1646	72	2209
5	88	22	585	39	1125	56	1679	73	2242
6	113	23	616	40	1157	57	1712	74	2276
7	140	24	647	41	1190	58	1745	75	2309
8	168	25	678	42	1222	59	1778	76	2342
9	195	26	710	43	1255	60	1811	77	2376
10	224	27	741	44	1287	61	1844	78	2410
11	253	28	773	45	1320	62	1877	79	2443
12	282	29	805	46	1352	63	1910	80	2477
13	311	30	836	47	1385	64	1943	81	2510
14	341	31	868	48	1417	65	1976	82	2543
Note: For trunk traffic greater than 4843 CCS, allow 34 CCS per trunk.									

Table 12
Trunk traffic – Poisson 10% blocking Grade of Service (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
15	370	32	900	49	1450	66	2009	83	2577
16	401	33	932	50	1482	67	2042	84	2610
17	431	34	964	51	1515	68	2076	85	2644
86	2678	99	3116	112	3552	125	3992	138	4434
87	2711	100	3149	113	3585	126	4026	139	4468
88	2745	101	3180	114	3619	127	4060	140	4502
89	2778	102	3214	115	3653	128	4094	141	4536
90	2812	103	3247	116	3687	129	4128	142	4570
91	2846	104	3282	117	3721	130	4162	143	4604
92	2880	105	3315	118	3755	131	4196	144	4638
93	2913	106	3349	119	3789	132	4230	145	4672
94	2947	107	3383	120	3823	133	4264	146	4706
95	2981	108	3417	121	3857	134	4298	147	4741
96	3014	109	3450	122	3891	135	4332	148	4775
97	3048	110	3484	123	3924	136	4366	149	4809
98	3082	111	3518	124	3958	137	4400	150	4843

Note: For trunk traffic greater than 4843 CCS, allow 34 CCS per trunk.

Calculate number of IP trunk cards required

The number of IP trunk cards is not just a function of the total number of ports required. It is important to determine if an IP Trunk 3.01 (and later) node has enough CPU capacity to handle the expected call volume.

As the size of an IP Trunk 3.01 (and later) implementation increases, real-time engineering becomes more important. The IP trunk cards that are acting as the Leader card or DCHIP card have a limited amount of CPU resources. For nodes with more than four cards and/or in large networks, such as those with more than 30 QoS endpoints, the CPU capacity (real-time capacity) must be considered.

> **Recommendation**
>
> Nortel strongly recommends implementing suitable QoS mechanisms on any IP network carrying VoIP.

Leader and DCHIP card standard configuration rules

1 Leader 0 with no DCHIP and all voice ports configured. Leader 1 with DCHIP supporting all Followers. This configuration should be suitable for most sites.

2 Leader 0 with no DCHIP and all voice ports configured. Leader 1 with DCHIP supporting half of the Followers. A Follower card with DCHIP supporting the other half of the Followers. This rule covers D-Channel redundancy with two IP Trunk 3.01 (and later) routes per node.

3 Leader 0 with DCHIP but no voice ports configured supporting Leader 1 and all Followers. This rule covers very large nodes and networks with multiple IP Trunk 3.01 (and later) routes per node.

4 Leader 0 with DCHIP and all voice ports configured supporting Leader 1 and all Followers. This configuration can only be used for smaller nodes and networks that do not have a large call volume.

To set up an incoming voice or fax call, the Follower card must communicate with the Follower card at the far end to set up and tear down the call. However, the Leader card must assist the Follower card in obtaining the IP address of the far end Follower card and provide network performance statistics so that the Follower card can set up the call correctly. The Leader card CPU real-time must be engineered to reserve enough capacity to provide this call processing functionality.

Additionally, the DCHIP card sends and receives all D-channel messages from the system to all Follower cards. In a multi-card node, the DCHIP card CPU real-time must be engineered to reserve enough capacity to successfully transmit and receive D-channel messages.

Card role

IP Trunk cards have various roles. Each role is affected by the amount of traffic in varying degrees. The following card roles are listed in order from the most impacted by call volume to the least affected by call volume:

DCHIP card role

Generally, the number of available voice ports on the IP trunk card having the DCHIP card must be engineered as either the number of cards per node and/or the traffic rate per node increase. Single card nodes are a special case for DCHIP functionality, as the DCHIP traffic both originates and terminates on the same card. This is the opposite of a multi-card node configuration, where the DCHIP traffic originates and terminates across the IP LAN. With IP Trunk 3.01 (and later), there is no additional work for the DCHIP role whether the calls are Gatekeeper-routed or not.

Leader card role

The Leader card plays a role in all call termination as the owner of the Node IP address and the resource (port) availability manager for the node. The Leader card also maintains the functionality for QoS probing generation and termination for the node. For this reason, the number of available voice ports on the Leader card must be engineered inversely to the total number of IP Trunk 3.01 (and later) nodes with QoS enabled in the IP Trunk 3.01 (and later) TLAN subnet. IP Trunk 3.01 (and later) registers and re-registers with a Gatekeeper. Unless the Time To Live (TTL) value is extremely low (under 15 seconds), the TTL has a very minor effect on the Leader card.

Single card role

The role of the IP trunk card in a single card node should not be impacted by real-time limitations. The only consideration that limits the capacity of a single Card node is the number of QoS endpoints being monitored. This has the same effect on single card nodes as it does on Leader cards. As for all cards with voice channels, there is an increase in the amount of work involved with Gatekeeper-routed calls. This increase in most cases, is not significant enough to affect most customer configurations.

Backup Leader/Follower role

The Backup Leader/Follower card roles have no additional real-time impacts over normal call processing, which is primarily governed by the customer traffic profile. If the IP Trunk 3.01 (and later) node is making mostly

Gatekeeper-routed calls, there is an increase in call processing, but the effects on the Follower card are minimal.

The real-time capacity of the Leader Card depends on various factors, including the following:

1 Host module CPU – Intel Pentium-based or Intel StrongARM (SA).

2 The number of ports on the Leader Card configured to transmit voice or fax traffic, the selected codec, and voice sample size.

3 The size of the IP Trunk 3.01 (and later) network (number of nodes in the network).

4 The endpoint types, such as IP Trunk 3.01 (and later), ITG Trunk 2.0, BCM, or CS 1000S and how calls are routed (Gatekeeper-routed or not).

5 Average Hold Time (AHT) of calls and the distribution of incoming calls. Nodes that have a high number of incoming calls, such as call centers, place a large load on the CPU and system. For more information, see "System performance under heavy load" on page 567.

6 Number of probe packets sent to every Leader Card at a remote node.

Factors 1, 2, 4, and 5 significantly impact the real-time capacity of the Leader card. Factors 3 and 6 impact the real-time requirement of the Network Monitoring Module on the Leader Card.

In IP Trunk 3.01 (and later), factors 1, 2, and 5 also impact the real-time capacity of the IP trunk card providing DCHIP functionality.

Factors that effect the real-time capacity

The following factors affect real-time capacity:

- host module type
- the number of ports configured on the Leader card, codec selection, and voice sample size
- size of the IP Trunk 3.01 (and later) network
- endpoint type
- the Average Hold Time (AHT) and distribution of incoming calls

Host module type

The Media Card 32-port trunk card has a significant real-time advantage for already-established calls; therefore, the Media Card 32-port trunk card supports more ports then the ITG-Pentium 24-port trunk card. The ITG-Pentium card has an advantage in the processing of call setup messages.

Additionally, other factors, such as the number of QoS endpoints being monitored, have a greater effect on the Media Card 32-port trunk card. In most applications, these differences have no effect on a customer configuration.

The number of ports configured on the Leader card, codec selection, and voice sample size

The number of voice ports configured on an IP trunk card can reduce the card's ability to fulfil other roles, such as the Leader card or DCHIP card. In large networks or large nodes, it might be necessary to disable some or all of the voice ports on an IP trunk card.

The more bandwidth a voice codec and voice sample size requires, the more packets are sent and received. For example, using the G.711 voice codec with a 10ms payload results in more packets being generated than other codecs generate. The extra packets use some of the IP trunk card's real-time capacity. This would only become a concern if the IP trunk card is a Leader or DCHIP card. Disabling the voice ports on an IP trunk card has a greater benefit in terms of saving real-time capacity than using a lower bandwidth codec.

Size of the IP Trunk 3.01 (and later) network

If QoS is enabled on an IP Trunk 3.01 (and later) network, the size of the network has a direct impact on the real-time capabilities of an IP trunk Leader card and on single card nodes.

In a default QoS configuration, the Leader card must terminate and generate a total of 50 probe packets per QoS-enabled ITG Trunk 2.x/IP Trunk 3.01 (and later) node every 15 seconds. These extra packets generated and received use real-time capabilities that would otherwise be used for call processing. If the number of nodes in a network that is being monitored exceeds the capabilities of the Leader card, implement other VoIP QoS methods.

For more information, see “Implement QoS in IP networks” on page 175.

Endpoint type

The endpoint type has no effect on real-time capacity for calls already established. The real-time capacity of the card is affected during call setup for Outgoing calls that use a Gatekeeper. Each outgoing call that uses a Gatekeeper sends an extra message, the ARQ message, to resolve a dialed number to a destination IP address. On a properly configured IP Trunk 3.01 (and later) node, this does not limit the capabilities of the node, because the outgoing call uses a Follower card which has more then sufficient resources.

The Average Hold Time (AHT) and distribution of incoming calls

The customer's call flow impacts the real-time engineering considerations of IP Trunk 3.01 (and later) in three ways, as follows:

1 **Total active voice call time (CCS calculation):**
If the active voice call time is lower, the call rate might be higher.

2 **The nature of call establishment and termination:**
Multiple simultaneous call setup/teardown events (less then half a second between call setups across multiple ports) have a significant impact on the peak CPU utilization of IP Trunk cards, especially in multi-card nodes where the DCHIP card communication is across the local IP LAN.

3 **Call direction**:
The IP Trunk Leader card real-time is impacted more on the call-terminating side than the call-originating side. However, the relative difference between terminating and originating IP trunk card CPU utilization is also call-profile dependent. This can vary from 20% less overhead on call origination to 0% less overhead.

Recommendation

Nortel recommends that if an IP Trunk 3.01 (and later) node has a mixture of Media Card 32-port trunk cards and ITG-Pentium 24-port trunk cards, ensure that the Leader 0 card is an ITG-Pentium 24-port trunk card. Additionally, in a mixed-card node, the DCHIP card should be an ITG-Pentium 24-port trunk card.

The Media Card 32-port trunk card can be used as a Leader or DCHIP card when the node contains all Media Cards 32-port trunk cards.

In this section, the following assumptions are made to project the Leader Card real-time capacity:

- The number of probe packets per Leader Card is 25.

- If the average hold time is 180 seconds, the number of calls per hour per port is 15.3 calls.
- If the average hold time is 10 seconds, the number of calls per hour per port is 187.5 calls.
- 50% of the calls are incoming and 50% are outgoing.

ITG-Pentium 24-Port trunk card Leader 0 and DCHIP card real-time capacity

The ITG-Pentium 24-port trunk card is based on the Intel Pentium CPU. The real-time capacity analysis of the ITG-Pentium 24-port trunk card Leader 0 is as follows. The following assumptions are made:

1. The minimum number of Follower cards required is a function of the call rate (which is limited by the Leader and DCHIP card) and the Average Hold Time (AHT) (which is a function of the number of channels per card). The number of Follower cards is calculated by the number of voice channels required (using Poisson 1 percent blocking Grade of Service) divided by the number of channels per card. The number of Follower cards required is affected by whether the Leader card has the voice channels enabled or not.
2. Peakedness factor for call processing is equal to 1.3. This implies that 30% fluctuation is allowed in the voice traffic.
3. Calls can terminate or originate on the Leader card. Voice ports are allowed on the Leader card, depending on configuration for anticipated traffic. Enabling the voice ports on a Leader or DCHIP card decreases the number of Follower cards required by one card, but can substantially affect the amount of traffic that can be handled for that node.
4. When VAD has been enabled in OTM 2.1 (and later), the voice fluctuation factor is equal to 1.5. A voice fluctuation factor of 1.5 implies that, during a conversation, voice is on 50% more than the average, in contrast to silence periods of a conversation. With VAD status equal to “off”, the voice fluctuation factor is equal to 1.1.
5. 15% of CPU real-time has been reserved for the Network Monitoring Module.

6 Gatekeeper-routed calls create a higher load on the card.

7 The values in the tables are valid for all Voice codecs and voice sample size including G.711, 10 ms voice sample.

Nortel recommends that traffic on a single card ITG-Pentium 24-port trunk card node never exceed the following:

- 5000 calls/hour – Gatekeeper-routed
- 6000 calls/hour – non-Gatekeeper-routed

In a multi-card node, the various roles necessary in processing calls, such as Leader card, DCHIP card, and Follower card, can be divided over multiple cards. This ensures that no IP trunk card exceeds its real-time capacity.

The maximum number of cards one DCHIP card can support is limited by the restriction of 382 TIE trunks for one D-Channel. Therefore, only 12 Media Cards 32-port or 16 ITG-Pentium 24-port trunk cards can be supported by one DCHIP card.

Recommendation

Nortel recommends a node never exceed the ratio of 12 Media Card 32-port trunk cards or 16 ITG-Pentium 24-port trunk cards to one Leader card.

A node has only one Leader card; however, more then one DCHIP card can be provisioned. If a DCHIP card fails, all IP trunk cards with channels that use that D-channel are out of service; the remaining IP trunk card channels, though, do remain in service. This configuration provides some redundancy and less work for each DCHIP card.

In a multi-card node, do not have the Leader function and DCHIP function on the same IP trunk card, unless all voice channels are disabled on that card. A Leader card needs to have voice channels provisioned on the IP trunk card to receive provisioning for the Gatekeeper, but disabling the voice channels allows the Leader card to handle a significantly higher number of calls/hour. The IP trunk card providing DCHIP functionality can be any card in the node including the Backup Leader (Leader 1) and Follower card. As with the

Leader card, disabling the voice channels on the DCHIP card significantly increases the number of calls/hour that can be processed.

The Leader card can support all Gatekeeper-routed calls, all locally-resolved calls, or a mixture of both. The Leader card can support the same number of Follower cards for all codecs with payload sizes of 10, 20, and 30 milliseconds, and with VAD on or off.

Table 13 and Table 14 on page 151 show the real-time capacity of the ITG-Pentium 24-port trunk card in the role of Leader card and the role of DCHIP card.

Table 13
Real-time capacity of a single card node with all 24 ports enabled

Calls/hr	CCS	AHT	Maximum number of nodes monitoring QoS	Comment
490	882	180s	96	Normal traffic
1500	900	60	46	
3000	900	30	30	
6000	600	10	0	Maximum capacity of card

Table 14
Real-time capacity of an ITG-Pentium 24-port trunk card in the Leader or DCHIP role

Number of QoS nodes in network	Calls/hr supported	Voice ports enabled on Leader card	At 1% blocking with *x* seconds of Average Hold Time (AHT), the minimum number of ITG-Pentium 24-port trunk card Follower cards required at:				
			AHT=10s	AHT=30s	AHT=60s	AHT=120s	AHT=180s
100	4862	24	1	3	5	9	12

Table 14
Real-time capacity of an ITG-Pentium 24-port trunk card in the Leader or DCHIP role

Number of QoS nodes in network	**Calls/hr supported**	**Voice ports enabled on Leader card**	**At 1% blocking with *x* seconds of Average Hold Time (AHT), the minimum number of ITG-Pentium 24-port trunk card Follower cards required at:**				
50	5238	24	2	3	5	9	13
0[1]	6000	24	2	3	6	10	15
100	7876	0	2	4	7	13	18
50	9334	0	5	5	8	15	22
0[1]	10692	0	2	5	9	17	25

[1] – A DCHIP card does not perform QoS probing. Use the “0 QoS nodes” row for a DCHIP card.

To achieve successful VoIP, a minimum amount of bandwidth must be reserved. Bandwidth is not guaranteed unless QoS mechanisms are implemented.

Media Card 32-port trunk card Leader 0 and DCHIP card real-time capacity

The Media Card 32-port trunk card is based on the Intel StrongARM CPU. The real-time capacity analysis of the Media Card 32-port Leader 0 card is as follows. The following assumptions are made:

1 The minimum number of Follower cards required is a function of the call rate (which is limited by the Leader and DCHIP card) and the Average Hold Time (AHT) (which is a function of the number of channels per card). The number of Follower cards is calculated by the number of voice channels required (using Poisson 1 percent blocking Grade of Service) divided by the number of channels per card. The number of Follower cards required is affected by whether the Leader card has the voice channels enabled or not.

2 Peakedness factor for call processing is equal to 1.3. This implies that 30% fluctuation is allowed in voice traffic.

3 Calls can terminate or originate on the Leader card. Voice ports are allowed on the Leader card, depending on configuration for anticipated traffic. Enabling the voice ports on a Leader or DCHIP card decreases the number of Follower cards required by one card, but can substantially affect the amount of traffic that can be handled for that node.

4 When VAD has been enabled in OTM 2.1 (and later), the voice fluctuation factor is equal to 1.5. A voice fluctuation factor of 1.5 implies that, during a conversation, voice is on 50% more than the average, in contrast to silence periods of a conversation. With VAD status equal to "off", the voice fluctuation factor is equal to 1.1.

5 15% of CPU real-time has been reserved for Network Monitoring Module.

6 Gatekeeper-routed calls create a higher load on the card.

7 The values in the tables are valid for all Voice codecs and voice sample size including G.711, 10 ms voice sample.

Recommendation

Nortel recommends that traffic on a single card Media Card 32-port trunk card node never exceed the following:

- 4000 calls/hour – Gatekeeper-routed
- 5500 calls/hour – non-Gatekeeper-routed

In a multi-card node, the various roles necessary in processing calls, such as Leader card, DCHIP card, and Follower card, can be divided over multiple cards. This ensures that no IP trunk card exceeds its real-time capacity.

8 The maximum number of cards one DCHIP card can support is limited by the restriction of 382 TIE trunks for one D-Channel. Therefore, only 12 Media Cards 32-port or 16 ITG-Pentium 24-port trunk cards can be supported by one DCHIP card.

Recommendation

Nortel recommends a node never exceed the ratio of 12 Media Card 32-port trunk cards or 16 ITG-Pentium 24-port trunk cards to one Leader card.

A node has only one Leader card; however, more then one DCHIP card can be provisioned. If a DCHIP card fails, all IP trunk cards with channels that use that D-channel are out of service; the remaining IP trunk card channels, though, do remain in service. This configuration provides some redundancy and less work for each DCHIP card.

In a multi-card node, do not have the Leader function and DCHIP function on the same IP trunk card, unless all voice channels are disabled on that card. A Leader card must have voice channels provisioned on the IP trunk card to receive provisioning for the Gatekeeper, but disabling the voice channels allows the Leader card to handle a significantly higher number of calls/hour. The IP trunk card providing DCHIP functionality can be any card in the node including the Backup Leader (Leader 1) and Follower card. As with the Leader card, disabling the voice channels on the DCHIP card significantly increases the number of calls/hour that can be processed.

The Leader card supports all Gatekeeper-routed calls, all locally-resolved calls, or a mixture of both. The Leader card support the same number of Follower cards for all codecs with payload sizes of 10, 20, and 30 milliseconds, and with VAD on or off.

Table 15, Table 16 on page 155, and Table 17 on page 155 show the capacity of the Media Card 32-port trunk card in the role of Leader card and the role of DCHIP card. This information is equally applicable to single card nodes or multi-card nodes and small or large IP Trunk networks. Refer to this information for all Media Card 32-port trunk card installations.

Table 15
Real-time capacity of a single card node with all 32 ports enabled

Calls/hr	CCS	AHT	Maximum number of nodes monitoring QoS	Comment
490	882	180s	96	Normal traffic
1500	900	60	46	
3000	900	30	30	
6000	600	10	0	Maximum capacity of card

Table 16
Real-time capacity of a Media Card 32-port trunk card in the Leader role

Number of QoS nodes in network	Calls/hr supported	Voice ports enabled on Leader card	At 1% blocking with *x* seconds of Average Hold Time (AHT), the minimum number of Media Card 32-port trunk card Follower cards required at:				
			AHT=10s	AHT=30s	AHT=60s	AHT=120s	AHT=180s
100	2615	32	1	2	2	4	5
50	3574	32	1	2	3	5	7
0	6000	32	1	3	4	8	11
100	3045	0	1	2	3	4	6
50	6376	0	1	3	5	8	12
0	10281	0	2	4	7	13	18

Table 17
Real-time capacity of a Media Card 32-port trunk card in the DCHIP role

Calls/hr supported	**Voice ports enabled on DCHIP card**	**At 1% blocking with *x* seconds of Average Hold Time (AHT), the minimum number of Media Card 32-port trunk card Follower cards required at:**				
		AHT=10s	AHT=30s	AHT=60s	AHT=120s	AHT=180s
6000	0	1	3	4	8	11
5800	32	1	3	4	8	11

In order to achieve successful VoIP, a minimum amount of bandwidth must be reserved. Bandwidth is not guaranteed unless QoS mechanisms are implemented.

Calculate Ethernet and WAN bandwidth usage

Table 18 on page 158 lists the Ethernet and WAN bandwidth use of IP Trunk 3.01 (and later) ports with different codecs with Silence Suppression Disabled. One port is a channel fully loaded to 36 CCS, where one CCS (Centi-Call-Second) is a channel/circuit being occupied 100 seconds. 36 CCS is a circuit occupied for a full hour.

To calculate the bandwidth requirement of a route, divide the total route traffic by 36 CCS and multiply by the bandwidth use. All traffic data must be based on the busy hour of the busy day.

To calculate resource requirements (IP Trunk 3.01 (and later) ports and TLAN subnet/WAN bandwidth), traffic parcels are summarized in different ways:

1 Add all sources of traffic for the IP Trunk 3.01 (and later) network, such as voice, faxes sent, and faxes received, together to calculate IP Trunk 3.01 (and later) port requirements and TLAN subnet bandwidth requirements.

2 For data rate requirement at each route, the calculation is based on each destination pair.

3 For fax traffic on a WAN, only the larger of either the fax-sent or fax-received traffic is to be accounted for.

The engineering procedures for the TLAN subnet and WAN are different. The following calculation procedure is for the TLAN subnet. The modification required for WAN engineering is included in these procedures.

IMPORTANT!

Voice packets must have priority over data packets.

When the WAN route prioritizes voice traffic over data traffic, the route bandwidth can be engineered to 90% loading level; otherwise, a WAN route with bandwidth of 1.536 Mbit/s or more can only be loaded up to 80%. A smaller WAN pipe (64 kbit/s) is recommended to a loading of 50%.

In Table 18 on page 158, the first WAN bandwidth is without Frame Relay or ATM overhead.

The Frame Relay overhead is 8 bytes (over IP packet).

The LLC SNAP (Link Layer Control SubNetwork Attachment Point) and AAL5 overhead for ATM is 16 bytes (over IP packet).

IP packet size over 53 bytes requires two ATM cells, over 106 bytes requires three ATM cells, and so on. Within the same number of cells, the bandwidth requirements are the same for packets with different sizes.

Note: OTM 2.1 (and later) input for fax is in bytes, ranging from 20 to 48;
30 bytes is the default.This differs from voice applications where payload size is the input.

Table 18
Silence Suppression disabled TLAN Ethernet and WAN IP bandwidth usage per IP Trunk 3.01 (and later) port (Part 1 of 2)

Codec type	Codec Multi - frame duration (ms) See Note 8.	Voice/fax payload size (bytes)	IP header size (bytes)	Ethernet header size (bytes)	Full-duplex Ethernet Bandwidth (bps)	PPP WAN Bandwidth (bps) See Note 9.	Frame Relay WAN bandwidth (bps)	ATM WAN bandwidth (bps)
G.711 (64 kbit/s) voice	10 20 30	80 160 240	40 40 40	26 26 26	116,800 90,400 81,600	101,600 82,800 76,533	102,400 83,200 76,800	127,200 106,000 84,800
DSP profileAB/ G.729A (8kbit/s) voice	10 20 30	10 20 30	40 40 40	26 26 26	60,800 34,400 25,600	45,600 26,800 20,533	46,400 27,200 20,800	84,800 42,400 28,267
G.723.1 (5.3 kbit/s) voice	30	20	40	26	22,933	17,867	18,133	26,571
G723.1 (6.3 kbit/s)	30	24	40	26	24,000	18,933	19,200	28,267
T.30/T.38 G3 Fax	16.6 25	30 30	40 40	26 26	46,265 30,720	37,108 24,960	37,590 24,960	50,600 33,900

Table 18
Silence Suppression disabled TLAN Ethernet and WAN IP bandwidth usage per IP Trunk 3.01 (and later) port (Part 2 of 2)

Codec type	Codec Multi - frame duration (ms) See Note 8.	Voice/fax payload size (bytes)	IP header size (bytes)	Ethernet header size (bytes)	Full-duplex Ethernet Bandwidth (bps)	PPP WAN Bandwidth (bps) See Note 9.	Frame Relay WAN bandwidth (bps)	ATM WAN bandwidth (bps)

Note 1: Based on voice multiframe encapsulation for Realtime Transport Protocol per H.323 V2.

Note 2: The bolded rows contain the default payload/packet size for each codec in OTM 2.1 (and later).

Note 3: TLAN subnet data rate is the effective Ethernet bandwidth consumption.

Note 4: TLAN subnet kbit/s for voice traffic = 2*Ethernet frame bits*8/frame duration in ms

Note 5: WAN kbit/s for voice traffic = IP packet bytes*8/frame duration in ms

Note 6: Overhead (RTP/UDP header + IP header) of packets over the voice payload multiframe is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.

Note 7: An Interframe gap is not included in the above bandwidth calculation, because of the low probability of occurring in this type of application.

Note 8: Length of speech captured at each end. By definition, payload is one way.

Note 9: These values do not include overhead from the network header (IEEE 802.3) that is automatically added at the TLAN subnet link. To determine the approximate bandwidth used on the TLAN subnet when including the network header, divide the values in the column "Bandwidth use on TLAN subnet in kbit/s (two way)" by 2.

Silence Suppression engineering considerations

Silence Suppression/Voice Activity Detection (VAD) results in average bandwidth savings over time, not in instantaneous bandwidth savings. For normal conversations, Silence Suppression creates a 40% savings in average bandwidth used. For example, a single G.729AB voice packet will still consume 30 Kbps of bandwidth but the average bandwidth used for the entire call would be approximately 23 Kbps.

To calculate the average bandwidth, perform the following calculation:

Codec bandwidth from Table 18 on page 158 x (0.6)

When voice services with multi-channel requirements are extensively used in an IP Trunk 3.01 (and later) network, such as Conference, Music-on-hold, and Message Broadcasting, additional voice traffic peaks to the IP network are generated due to the simultaneous voice-traffic bursts on multiple channels on the same links.

In those cases, even when Silence Suppression is enabled on the IP trunk card, Nortel recommends using the more conservative bandwidth calculations of Table 18 on page 158 with Silence Suppression disabled to calculate the portion of the bandwidth requirement caused by simultaneous voice traffic.

Fax engineering considerations

The fax calculation is based on a 30-byte packet size and a data rate of 64 kbit/s (with no compression) The frame duration (payload) is calculated by using the equation:

30*8/14400=16.6 ms

where 14,400 bit/s is the modem data rate.

Bandwidth output is calculated by the equation:

108*8*1000/16.6=52.0 kbit/s

Bandwidth output to WAN is:
70*8*1000/16.6=33.7 kbit/s.

Payload and bandwidth output for other packet sizes or modem data rates must be calculated in a similar manner.

Fax traffic is always one-way. Fax pages sent and fax pages received generate data traffic to the TLAN subnet. For WAN calculation, only the larger traffic parcel of the two must be considered.

Trunk Anti-Tromboning (TAT) and Trunk Route Optimization (TRO) considerations

Trunk Anti-Tromboning (TAT) was designed to remove tromboning trunks after a call was answered by a third party. Anti-Tromboning can occur in the following scenarios.

- If a call is re-directed due to call forward or hunt, trunks are torn down after the third party answers.
- Tromboning trunks are removed due to call modification, such as transfer or conference, after the third party answers the call and the call modification is completed.
- For calls entering the private network on CO trunks, the private network trunks being tromboned due to call modification or call redirection are removed.

The removal of trunks in the previous scenarios frees resources that would be otherwise tied up due to tromboning. Therefore, a customer can reduce the call blocking caused by excessive trunk tromboning. This feature works in a PRI, ISL, and VNS network.

TAT enhancement

IP Trunk 3.01(and later) introduces an improved TAT validation check that greatly reduces the number of valid anti-tromboning cases for which TAT is blocked. The check works by comparing the H.323 Gateway Endpoint ID (EPID) that allows TAT to optimize trunk connections in all valid anti-tromboning cases. The EPID is the MAC address of an H.323 Gateway host, such as an IP Trunk card or Signaling Server.

As a fallback TAT validation mechanism, IP Trunk 3.01 (and later) uses the IP Trunk 3.01 validation check of comparing called and calling numbers. IP Peer in CS 1000 Release 2.0, IP Trunk 3.01, BCM 3.0.1, and BCM 3.5 do not support the new TAT validation check comparing EPIDs. Therefore, when interoperating with these systems, IP Trunk 3.01 (and later) falls back to the IP Trunk 3.01 (and later) TAT validation mechanism of comparing called and calling numbers. This results in the blocking of the TAT operation in several valid anti-tromboning cases, as previously discussed.

When tromboning of IP Trunks occurs due to limited TAT operation with CS 1000 Release 2.0 and BCM 3.5, BCM and IP Peer use H.245 signaling to the IP Trunk 3.01 (and later) node to establish a direct media path between the two tromboned IP Trunks. There are three cases of direct media path connection between two tromboned IP Trunks (trunk channels) when interoperating with BCM and IP Peer:

- Both IP Trunks are on the same Media Card 32-port trunk card running IP Trunk 3.01 (and later).

  The circuit-switched path between the tromboned trunks is connected by the time switch on the Media Card 32-port trunk card. There is no voice quality degradation due to delay or multiple transcoding since the speech path does not pass through the IP Trunk codecs and packetization/depacketization. The tromboned trunks are busy for the duration of the call.

- Both IP Trunks are on the same ITG-Pentium 24-port trunk card running IP Trunk 3.01 (and later).

  The media path between the tromboned trunks is connected by the IP loopback route on the ITG-Pentium 24-port trunk card. Voice quality degradation may occur due to delay and multiple transcoding since the speech path passes through both codecs and packetization/depacketization. The tromboned trunks are busy for the duration of the call.

- The two IP Trunks are on different IP Trunk cards.

  The media path between the tromboned trunks is connected by the TLAN network interface route between the two IP Trunk cards. Voice quality degradation may occur due to delay and multiple transcoding since the speech path passes through both codecs and packetization/depacketization. The tromboned trunks are busy for the duration of the call.

TAT as a method of Improving Voice Quality in a VoIP network

In a purely TDM network, TAT provides a method of eliminating the unnecessary use of trunking resources.

In a VoIP network, there are three primary benefits of TAT.

1. As in a TDM network, TAT eliminates tromboning of trunks and frees up valuable trunking resources.
2. TAT provides a method of reducing bandwidth requirements, which can be crucial over a slow WAN link. If TAT is not used, a tromboned call using a G.729 codec can theoretically use 60-70Kbps on a WAN link. By using TAT, bandwidth can be reduced to zero for a tromboned call.
3. TAT improves voice quality. If a call is tromboned using a G.729 codec, multiple transcodings can diminish voice quality. Since each transcoding introduces errors for a G.729 codec, the goal is to eliminate as many hops as possible. TAT provides the means to accomplish this.

TAT call Scenario

The following call scenario helps to understand TAT.

1. Site 1 and Site 2 both have an IP Trunk 3.01 (or later) node installed. IP Trunk 3.01 (and later) is used for trunking between the two sites.
2. Telephone A at Site 1 calls Telephone B at Site 2. Telephone B answers the call and decides to transfer the call to Phone C which is located at Site A.
3. Telephone C answers the call transferred from Telephone B at Site 2.
4. After the call has been answered by Telephone C, Site B sends a TAT Invoke message to Site A. Site B only sends a TAT Invoke message if the Tromboned Trunks belong to the same D-Channel and Customer. If a customer has multiple DCHIP cards in their node, The first leg of the call could be associated with one D-Channel and the second leg of the call associated with another D-Channel. In this case, TAT will not be invoked.

To prevent problems, the following recommendations are made:

- The use of multiple DCHIPs in a node or the use of multiple IP Trunk 3.01 (and later) nodes in a system must be implemented with caution. It can lead to poor voice quality in certain call scenarios.

- Tromboned Trunks must belong to the same customer.
- TAT must be configured in the RCAP prompt for D-Channel Configuration. IP Trunk 3.01 (and later) Nodes at both sites must have TAT in the RCAP of their respective D-channels.

Therefore, TAT can fail if the originating side has multiple DCHIPs configured or multiple nodes configured in a system. TAT failure can also occur if the recipient of the TAT Invoke message has multiple DCHIPs or IP Trunk 3.01 (and later) nodes.

If Site A in the previously described scenario had multiple DCHIPs or multiple IP Trunk 3.01 (and later) nodes, TAT would fail. The reason is as follows: if the call between Telephone A and Telephone B was set up using one D-Channel and the call between Telephone B and Telephone C was set up using another D-Channel, then the D-Channel for the first leg of the call is not able to validate the Call Reference Value* for the second leg of the call. This prevents TAT from being used.

*The Facility message invoking TAT is sent using the Call Reference Value of the first call, which was from Telephone A to Telephone B. The TAT Invoke includes the Call Reference Value of the second call, which was Telephone B transferring the call to Telephone C.

TAT versus TRO

Nortel recommends that both Trunk Route Optimization (TRO) and TAT be implemented with IP Trunk 3.01 (and later) nodes.

TRO functions in a different manner than TAT. TRO is invoked before the call has been answered. TAT is invoked once the call has been answered. To reduce the number of trunks being used due to call redirection by CFNA, Hunt, or Forward all Calls, configure TRO in the RDB. TRO must be enabled at all sites.

If Telephone A at Site 1 calls Telephone B at Site 2, and Telephone B forwards a call using CFNA to Telephone C at Site 3, then TRO must be enabled at Sites 1 and 2. If TRO is enabled at both sites, Site 2 will drop out, freeing up the trunk, and only trunks on Site 1 and 3 are used. This reduces the number of trunks in use, conserves bandwidth, and improves voice quality.

The TRMB prompt in RDB does not have to be set to Yes for TAT or TRO to work. The function of the TRMB prompt is to allow or disallow tromboning caused by NARS/BARS mis-configuration. For example, Site A has DSC of 4000 pointing to Site B. Site B has DSC of 4000 pointing back to Site A. If a caller at Site A dials 4000, this can lead to the call orbiting between the two sites. This is commonly referred to as the “Ping-Pong” effect. Therefore, Nortel recommends setting TRMB to NO.

WAN route bandwidth engineering

After the TLAN subnet traffic is calculated, determine the bandwidth requirement for the WAN. In this environment, bandwidth calculation is based on network topology and destination pairs.

Before network engineering can begin, obtain the following network data:

- A network topology and routing diagram.
- A list of the sites where the IP Trunk 3.01 (and later) nodes are to be installed.
- List the sites with IP Trunk 3.01 (and later) traffic, and the codec and frame duration (payload) to be used.
- Obtain the offered traffic in CCS for each site pair; if available, separate voice traffic from fax traffic (fax traffic sent and received).
- In a network with multiple time zones, use the same real-time busy hour varying clock hours) at each site that yields the highest overall network traffic. Traffic to a route is the sum of voice traffic plus the larger of one way fax traffic (either sent or received.

Table 19 summarizes traffic flow of a 4-node IP Trunk 3.01 (and later) network.

Table 19
Example: Traffic flow in a 4-node IP Trunk 3.01 (and later) network

Destination Pair	Traffic in CCS
Santa Clara/Richardson	60
Santa Clara/Ottawa	45
Santa Clara/Tokyo	15
Richardson/Ottawa	35
Richardson/Tokyo	20
Ottawa/Tokyo	18

The codec selection is on a per-IP trunk card basis. During call setup negotiation, only the type of codec available at both destinations is selected. When no agreeable codec is available at both ends, the default codec G.711 is used.

> ***Note:*** Nortel recommends that all cards in an IP Trunk 3.01 (and later) system have the same image. If multiple codec images are used in an IP Trunk 3.01 (and later) network, the calls default to the G.711 group when the originating and destination codecs are different.

The IP Trunk 3.01 (and later) port requirement for each node is calculated by counting the traffic on a per-node basis, based on Table 11 on page 139. The port requirements for the example in Table 19 are given in Table 20 on page 167.

Table 20
Example: Determine IP trunk card requirements

ITG Site	Traffic in CCS	ITG Ports	IP trunk cards
Santa Clara	120	9	1
Richardson	115	9	1
Ottawa	98	8	1
Tokyo	53	6	1

Assume that the preferred codec to handle VoIP calls in this network is G.729AB.

Table 21 summarizes the WAN traffic in kbit/s for each route. The recommended incremental bandwidth requirement is included in the column adjusted for 30% traffic peaking in busy hour. This assumes no correlation and no synchronization of voice bursts in different simultaneous calls. This assumes some statistical model of granularity and distribution of voice message bursts due to Silence Suppression.

Table 21
Example: Incremental WAN bandwidth requirement

Destination Pair	CCS on WAN	WAN traffic in kbit/s	Peaked WAN traffic (x1.3) in kbit/s
Santa Clara/Richardson	60	18.7	24.3
Santa Clara/Ottawa	45	14.0	18.2
Santa Clara/Tokyo	15	4.7	6.1
Richardson/Ottawa	35	10.9	14.2
Richardson/Tokyo	20	6.2	8.1
Ottawa/Tokyo	18	5.6	7.3

The following example illustrates the calculation procedure for Santa Clara and Richardson. The total traffic on this route is 60 CCS. To use the preferred codec of G.729AB with a 30 ms payload, the bandwidth on the WAN is 11.2 kbit/s. WAN traffic is calculated using the following formula:

(60/36)*11.2 = 18.7 kbit/s

Augmenting this number by 30% gives a peak traffic rate of 24.3 kbit/s. This is the incremental bandwidth required between Santa Clara and Richardson to carry the 60 CCS voice traffic during the busy hour.

Assume that 20 CCS of the 60 CCS between Santa Clara and Richardson is fax traffic. Of the 20 CCS, 14 CCS is from Santa Clara to Richardson, and 6 CCS is from Richardson to Santa Clara. What is the WAN data rate required between those two locations?

Traffic between the two sites can be broken down to 54 CCS from Santa Clara to Richardson, and 46 CCS from Richardson to Santa Clara, with the voice traffic 40 CCS (60 – 20) being the two-way traffic.

The bandwidth requirement calculation would be:

(40/36)*11.2 + (14/36)*33.6 = 25.51 kbit/s

where 14 CCS is the larger of two fax traffic parcels (14 CCS as compared to 6 CCS).

After adjusting for peaking, the incremental data rate on WAN for this route is 33.2 kbit/s. Compare this number with 24.3 kbit/s when all 60 CCS is voice traffic, it appears that the reduction in CCS due to one-way fax traffic (20 CCS as compared to 14 CCS) will not compensate for higher bandwidth requirement of a fax as compared to a voice call (33.7 kbit/s as compared to 11.2 kbit/s) in this example.

This section deals with nodal traffic calculation in both the TLAN subnet and WAN. It indicates the incremental bandwidth requirement to handle voice on data networks.

Assess WAN link resources

For most installations, IP Trunk 3.01 (and later) traffic will probably be routed over WAN links within the intranet. WAN links are the highest repeating expenses in the network and they often cause capacity problems in the network. Unlike LAN bandwidth, which is virtually free and easily implemented, WAN links, especially inter-LATA and international links, take time to finance, provision, and upgrade. For these reasons, it is important to determine the state of WAN links in the intranet before installing the IP Trunk 3.01 (and later) network.

Each voice conversation, (G.729AB codec, 30 ms payload) consumes 11.2 kbit/s of bandwidth or 18.6 kbit/s with Silence Suppression disabled for *each* link that it traverses in the intranet. A DS0 64 kbit/s WAN link would support 5 simultaneous telephone conversations with Silence Suppression enabled, or 2 simultaneous telephone conversations with Silence Suppression disabled.

Link utilization

To start this assessment, obtain a current topology map and link utilization report of the intranet. A visual inspection of the topology map should reveal which WAN links are likely to be used to deliver IP Trunk 3.01 (and later) traffic. Alternately, use the Traceroute tool. See "Measure intranet QoS" on page 191.

Next, determine the current utilization of those links. Note the reporting window that appears in the link utilization report. For example, the link utilization can be averaged over a week, a day, or one hour. To be consistent with the dimensioning considerations, obtain the busy period (peak hour) utilization of the trunk. See "IP Trunk 3.01 (and later) traffic engineering" on page 134. Because WAN links are full-duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.

The third step is to assess how much spare capacity is available. Enterprise intranets are subject to capacity planning policies that ensure capacity use remains below some determined utilization level. For example, a planning policy might state that the utilization of a 56 kbit/s link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, for instance, 80%. The carrying capacity of the 56 kbit/s link would be 28 kbit/s and for the T1, 1.2288 Mbit/s. In some organizations the thresholds can be lower than those used in this example; in the event of link failures, there must be spare capacity to re-route traffic.

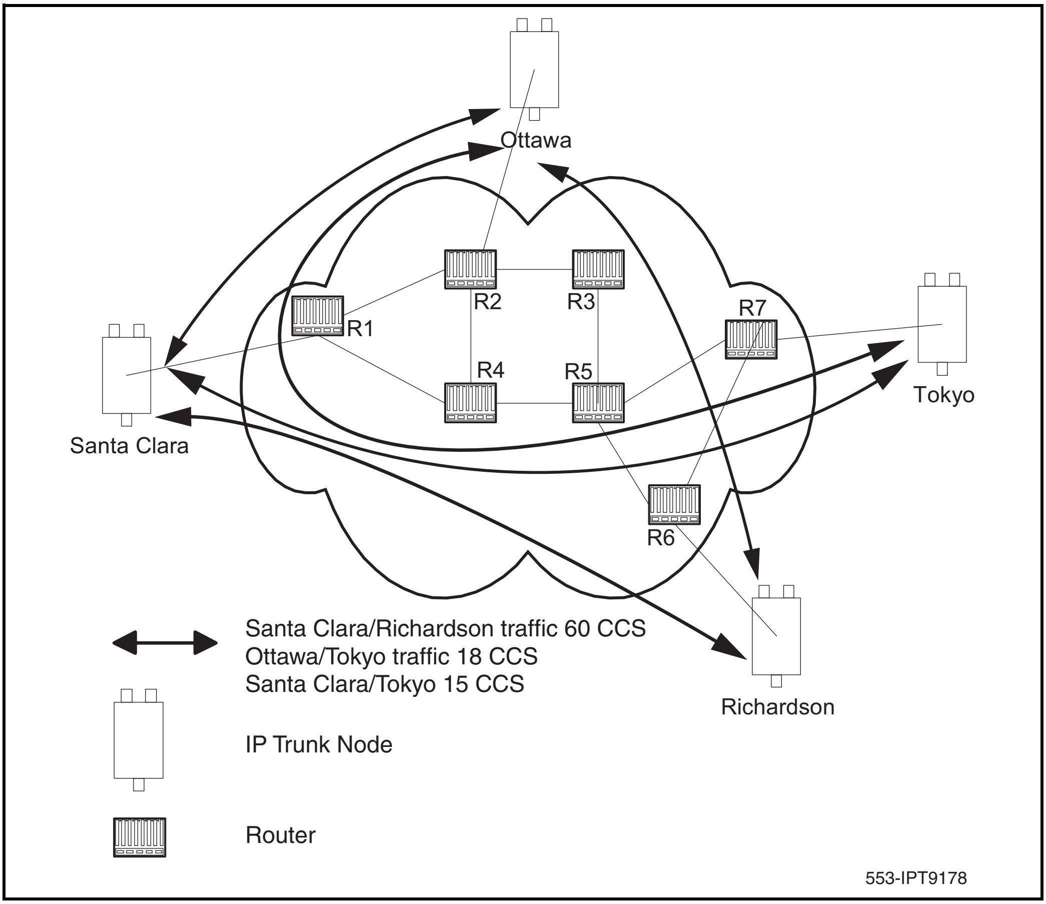
Some WAN links can be provisioned on top of Layer 2 services such as Frame Relay and ATM; the router-to-router link is actually a virtual circuit, which is subject not only to a physical capacity, but also to a “logical capacity” limit. Obtain, in addition to the physical link capacity, the QoS parameters, especially the Committed Information Rate (CIR) for Frame Relay and Maximum Cell Rate (MCR) for ATM.

The difference between the current capacity and its allowable limit is the available capacity. For example, a T1 link utilized at 48% during the peak hour, with a planning limit of 80%, had an available capacity of approximately 492 kbit/s.

Estimate network loading caused by IP Trunk 3.01 (and later) traffic

At this point, enough information has been obtained to “load” the IP Trunk 3.01 (and later) traffic on the intranet. Figure 25 on page 171 illustrates how this is done on an individual link.

Figure 25
Calculate network load with IP Trunk 3.01 (and later) traffic



Suppose the intranet has a topology as shown in Figure 25 and a prediction on the amount of traffic on a specific link, R4-R5, is required. From the "IP Trunk 3.01 (and later) traffic engineering" section and Traceroute measurements, the R4-R5 link is expected to support the Santa Clara/Richardson, Santa Clara/Tokyo, and the Ottawa/Tokyo traffic flows; the other IP Trunk 3.01 (and later) traffic flows do not route over R4-R5. The summation of the three flows yields 93 CCS or 24 kbit/s as the incremental traffic that R4-R5 will need to support.

To complete this exercise, total the traffic flow for every site pair to calculate the load at each IP Trunk 3.01 (and later) endpoint.

Route Link Traffic Estimation

Routing information for all source-destination pairs must be recorded as part of the network assessment. This is done using the Traceroute tool. An example of the output is shown below.

```
Richardson3% traceroute santa_clara_itg4

traceroute to santa_clara_itg4 (10.3.2.7), 30 hops
max, 32 byte packets

      r6 (10.8.0.1) 1 ms  1 ms  1 ms

      r5 (10.18.0.2) 42 ms  44 ms  38 ms

      r4 (10.28.0.3) 78 ms  70 ms  81 ms

      r1 (10.3.0.1) 92 ms  90 ms  101 ms

      santa_clara_itg4 (10.3.2.7) 94 ms  97 ms  95 ms
```

The Traceroute program can be used to check if routing in the intranet is symmetric for each source-destination pair. Use the –g loose source routing option as shown in the following command syntax:

```
Richardson3% traceroute -g santa_clara_itg4 richardson3
```

The Traceroute program identifies the intranet links that transmit IP Trunk 3.01 (and later) traffic. For example, if Traceroute of four site pairs yield the results shown in Table 22, then the load of IP Trunk 3.01 (and later) traffic per link can be computed as shown in Table 23.

Table 22
Traceroute identification of intranet links

Site pair	Intranet route
Santa Clara/Richardson	R1-R4-R5-R6
Santa Clara/Ottawa	R1-R2
Santa Clara/Tokyo	R1-R4-R5-R7
Richardson/Ottawa	R2-R3-R5-R6

Table 23
Route link traffic estimation

Links	Traffic from:
R1-R4	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R4-R5	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R5-R6	Santa Clara/Richardson +Richardson/Ottawa
R1-R2	Santa Clara/Ottawa + Tokyo/Ottawa
R5-R7	Santa Clara/Tokyo + Ottawa/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Enough capacity

For each link, Table 24 compares the available link capacity to the additional IP Trunk 3.01 (and later) load. For example, on link R4-R5, there is plenty of available capacity (492 kbit/s) to accommodate the additional 24 kbit/s of IP Trunk 3.01 (and later) traffic.

Table 24
Computation of link capacity as compared to ITG load

Link		Utilization (%)		Available capacity (kbit/s)	Incremental IP Trunk 3.01 (and later) load		Sufficient capacity?
End-points	Capacity (kbit/s)	Threshold	Used		Site pair	Traffic (kbit/s)	
R1-R2	1536	80	75	76.8	Santa Clara/Ottawa + Ottawa/Tokyo	21.2	Yes
R1-R4	1536	80	50	460.8	Santa Clara/Tokyo + Santa Clara/ Richardson + Ottawa / Tokyo	31.4	Yes
R4-R5	1536	80	48	492	Santa Clara/Richardson + Ottawa/ Tokyo + Santa Clara/Tokyo	31.4	Yes

Some network management systems have network planning modules that compute network flows in the manner just described. These modules provide more detailed and accurate analysis, as they can take into account actual node, link, and routing information. They also help assess network resilience by conducting link and node failure analysis. By simulating failures and re-loading network and re-computed routes, the modules indicate where the network might be out of capacity during failures.

Insufficient link capacity

If there is not enough link capacity, implement one or more of the following options:

- Use the G.723 codec series.
  Compared to the default G.729AB codec with 30 ms payload, the G.723 codecs use 9% to 14% less bandwidth.
- Upgrade the link's bandwidth.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources are less frequent. For a more complete assessment, consider the impact of incremental IP Trunk 3.01 (and later) traffic on routers and LAN resources in the intranet. Perhaps the IP Trunk 3.01 (and later) traffic is traversing LAN segments that are saturated, or traversing routers whose CPU utilization is high.

Implement QoS in IP networks

Today’s corporate intranets developed because of the need to support data services, services which found a “best effort” IP delivery mechanism sufficient. Standard intranets are designed to support a set of QoS objectives dictated by these data services.

When an intranet takes on a real-time service, such as VoIP, the users of that service impose additional QoS objectives on the intranet. Some of these targets are less stringent compared with those imposed by current services, while other targets are more stringent. If a data intranet not exposed to real-time services in the past now has to deliver IP Trunk 3.01 (and later) traffic, the QoS objectives for delay impose an additional design constraint on the intranet.

One approach is to simply subject all intranet traffic to additional QoS constraints and design the network to the strictest QoS objectives. This would improve the quality of data services, even though most applications might not perceive a reduction of, for example, 50ms in delay. Improving the network results in one that would be adequately engineered for voice, but over-engineered for data services.

The best approach to consider is the use of QoS mechanisms in the intranet when the intranet is carrying mixed traffic types.

QoS mechanisms are extremely important to ensure satisfactory voice quality. If QoS mechanisms are not used, there is no guarantee that the bandwidth needed for voice traffic will be available. For example, a data file being downloaded from the intranet could use most of the WAN bandwidth. Unless voice traffic has been configured to have higher priority, the data file download could use most of the available bandwidth. This would cause voice packet loss and therefore poor voice quality.

Recommendation

Nortel strongly recommends implementing suitable QoS mechanisms on any IP network carrying VoIP.

This section outlines what QoS mechanisms can work in conjunction with the IP Trunk 3.01 (and later) node and the intranet-wide consequences if the mechanisms are implemented.

Traffic mix

Before implementing QoS mechanisms in the network, assess the traffic mix of the network. QoS mechanisms depend on the process and ability to distinguish traffic by class to provide differentiated services.

If an intranet is designed to deliver only IP Trunk 3.01 (and later) traffic, and all traffic flows are of equal priority, then there is no need to consider QoS mechanisms. This network would only have one class of traffic.

In most corporate environments, the intranet primarily supports data services. When planning to offer voice services over the intranet, assess the following:

- Are there existing QoS mechanisms? What kind? IP Trunk 3.01 (and later) traffic should take advantage of established mechanisms if possible.
- What is the traffic mix? If the volume of IP Trunk 3.01 (and later) traffic is small compared to data traffic on the intranet, then IP QoS mechanisms will be sufficient. If IP Trunk 3.01 (and later) traffic is significant, data services might be impacted when those mechanisms are biased toward IP Trunk 3.01 (and later) traffic.

TCP traffic behavior

The majority of corporate intranet traffic is TCP-based. Unlike UDP, which has no flow control, TCP uses a sliding window flow control mechanism. Under this scheme TCP increases its window size, increasing throughput until congestion occurs. Congestion is detected by packet losses, and when that happens the throughput is quickly throttled down, and the whole cycle repeats. When multiple TCP sessions flow over few bottleneck links in the intranet, the flow control algorithm can cause TCP sessions in the network to throttle at the same time, resulting in a periodic and synchronized surge and ebb in traffic flows. WAN links appear to be congested at one period of time time and then are followed by a period of under-utilization. There are two consequences, as follows:

- WAN link inefficiency
- IP Trunk 3.01 (and later) traffic streams are unfairly affected

IP Trunk 3.01 (and later) DiffServ support for IP QoS

If the intranet provides differentiated services based on the DiffServ/TOS field, then the IP Trunk 3.01 (and later) traffic and other traffic marked with this DiffServ/TOS value can be delivered with the goal of meeting this class of traffic's QoS objectives.

Configure the DiffServ/TOS value for signaling and voice packets to obtain better QoS over the IP data network (LAN/WAN).

The Differentiated Service (DiffServ) Code Point (DSCP) determines the priority of the control and voice packets in the network router queues.

IMPORTANT!

The values entered in these two fields must be coordinated across the entire IP data network. Do not change them arbitrarily.

DiffServ values must first be converted to a decimal value of the DiffServ byte in the IP packet header. Table 25 shows the recommended DiffServ traffic classes for various applications.

Table 25
Recommended DiffServ classes

Traffic type	DiffServ class	DSCP (binary)	DSCP (decimal)
Voice media	Expedited Forwarding	101110	46
Voice signaling	Class Selector 5	101000	40
Data traffic	default	000000	0

Note: The DSCP comprises 6 bits within the 8-bit TOS field.

Queue management

Queueing delay

From “Queuing delay” on page 184, it can be seen that queueing delay is a major contributor to delay, especially on highly-utilized and low-bandwidth WAN links. Routers that are TOS-aware and support class-based queuing can help reduce queueing delay of voice packets when these packets are treated with preference over other packets.

Class-based Queueing

To this end, Class-Based Queueing (CBQ) can be considered for implementation on these routers, with the IP Trunk 3.01 traffic prioritized against other traffic. CBQ, however, can be CPU-intensive and might not scale well when applied on high-bandwidth link. Therefore, if implementing CBQ on the intranet for the first time, do so selectively. Usually CBQ is implemented at edge routers or at entry routers into the core.

Buffer management and WRED

The global synchronization situation described in "TCP traffic behavior" on page 177 can be countered using a buffer management scheme which discards packets randomly as the queue starts to exceed some threshold.

Weighted Random Early Detection (WRED), an implementation of this strategy, additionally inspects the TOS bits in the IP header when considering which packets to drop during buffer build up. In an intranet environment where TCP traffic dominates real-time traffic, WRED can be used to maximize the dropping of packets from long-lived TCP sessions and minimize the dropping of voice packets.

As in CBQ, check the configuration guidelines with the router vendor for performance ramifications when enabling WRED. If global synchronization is to be countered effectively, implement WRED at core and edge routers.

Use of Frame Relay and ATM services

IP can be transported over Frame Relay and ATM services, both of which provide QoS-based delivery mechanisms. If the router can discern IP Trunk 3.01 (and later) traffic by inspecting the TOS field or observing the UDP port numbers, it can forward the traffic to the appropriate Permanent Virtual Circuit (PVC) or Switched Virtual Circuit (SVC). At the data link layer, the differentiated virtual circuits must be provisioned. In Frame Relay, the differentiation is created by having both "zero-Committed Information Rate (CIR)" and CIR-based PVCs; in ATM, differentiation is created by having VCs with different QoS classes.

Internet Protocols and ports used by IP Trunk 3.01 (and later)

The following IP applications and protocols are used by IP Trunk 3.01 (and later) and must be transmitted across the customer's intranet by all IP routers and other network equipment. This information should be validated and included in the IP Trunk 3.01 (and later) network engineering guidelines.

Customers using firewalls must be aware of all UDP and TCP ports being used by IP Trunk 3.01 (and later) and provision their equipment accordingly.

IP Trunk 3.01 (and later) management protocols

IP Trunk 3.01 (and later) uses the UDP and TCP port numbers for SNMP, Telnet, and FTP (the default port numbers for these common IP applications).

IP Trunk 3.01 (and later) management LAN ports

In addition to the TCP and UDP ports used for standard IP applications, there are IP trunk-specific ports used. Messages sent between the DCHIP Leader card and other cards use TCP port 6001. When the Backup Leader card and the Follower cards boot up, they obtain their IP address from the Leader card over UDP ports 67 – 68.

IP Trunk 3.01 (and later) H.323 Voice Gateway Protocols

H.225 Call Setup Signaling uses TCP port 1720 for the destination port. H.323 Register and Admission Signaling (RAS) uses UDP port 1719. RAS is used when registering with a Signaling Server Gatekeeper.

Realtime Transport Protocol (RTP) uses UDP port 2300-2363 by default. In OTM 2.1 (and later), RTP can also be provisioned to use UDP port 17301 – 17362.

The option is also available to manually enter the starting value for the RTP port range in OTM 2.1 (and later). This should only be done at the request of a field engineer.

IP Trunk 3.01 (and later) Voice Gateway Protocols

On the TLAN subnet, IP trunk cards within a node use UDP ports 2001 – 2002 for inter-card communication.

When using the dialing plan tables to resolve an address for non-call associated signaling, Nortel MCDN messages use UDP port 15000 on the TLAN subnet to communicate with cards on the far end of the network.

IP Trunk 3.01 QoS Network Probing Proprietary Protocol

QoS probing uses UDP port 5000.

Port numbers used by IP Trunk 3.01 (and later)

Table 26 and Table 27 on page 181 list the pre-defined ports used by IP Trunk 3.01 (and later).

Table 26
Pre-defined TCP ports

Network interface	Port use	Port number
ELAN	DCHIP inter-card messaging	6001
TLAN	H.225 TCP port	1720 (destination port only)

Table 27
Pre-defined UDP ports

Interface	Port use	Port number
ELAN	BOOTP Server	67 (on Leader card)
ELAN	SNMP	161
TLAN	RTP Ports	2300 – 2362 (TCID*2 + 2300) **or** 17300 – 17362 (TCID*2 + 17300)
TLAN	RTCP Ports	2301 – 2363 (TCID*2 + 2300 + 1) **or** 17301 – 17363 (TCID*2 + 17300 + 1)

QoS fallback thresholds and IP Trunk 3.01 (and later)

In IP Trunk 3.01 (and later), QoS remains in effect when communicating between non-Gatekeeper-routed endpoints (IP Trunk 3.01 (and later) endpoints). For more information, see "Fallback threshold" on page 225 and "Setting the QoS threshold for fallback routing" on page 226.

However, QoS fallback for Gatekeeper-routed calls (calls to Gatekeeper-routed endpoints) is not possible. This is because the calls routed by the Gatekeeper can be directed to a variety of endpoints, some of which might not have direct PSTN connectivity such as a Nortel IP Phone 2004 on a CS 1000S system.

A well engineered network greatly reduces the need for QoS fallback to PSTN. A well engineered network includes the following features:

- implementing network QoS features such as DiffServ and 802.1Q/p to give priority to real-time voice traffic
- limiting the maximum frame size and fragmenting large frames on low-speed WAN links
- limiting the quantity of voice traffic that is transmitted over low-speed WAN links

For further information, refer to
Communication Server 1000S: Planning and Engineering (553-3031-120).

Fine-tune network QoS

Topics presented in this section deal with issues that impact the QoS of IP Trunk 3.01 traffic. They help to understand how to fine-tune a network to improve its QoS, but are not directly involved as a part of network engineering procedure. These are advanced topics to help a technician fine-tune the network to improve QoS, but they are not a part of the required procedure for initial IP Trunk 3.01 (and later) network engineering.

Further network analysis

This section describes actions that can be taken to investigate the sources of delay and error in the intranet. This and the next section discuss several strategies for reducing one-way delay and packet loss. The key strategies are: as follows:

- reduce link delay
- reduce hop count
- adjust jitter buffer size
- implement IP QoS mechanisms

Components of delay

End-to-end delay is caused by many components. The major components of delay are as follows:

- propagation delay
- serialization delay
- queuing delay
- routing and hop count
- IP Trunk 3.01 (and later) system delay

Propagation delay

Propagation delay is affected by the mileage and medium of links traversed. Within an average-size country, the one-way propagation delay over terrestrial lines is under 18 ms; within the U.S. the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and trans-oceanic circuits, use the rule-of-thumb of 1 ms per 100 terrestrial miles.

If a circuit goes through a satellite system, estimate each hop between earth stations to contribute 260 ms to the propagation delay.

Serialization delay

Serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is calculated using the following formula:

Serialization delay in ms = 8 * (IP packet size in bytes)/(link bandwidth in kbit/s)

Table 28 shows what the serialization delay for voice packets on a 64 kbit/s and 128 kbit/s link. The serialization delay on higher speed links are considered negligible.

Table 28
Serialization delay

Codec	Frame duration	Serialization delay over 64 kbit/s link (ms)	Serialization delay over 128 kbit/s link (ms)
G.711A/ G.711U	10 ms	14.00	0.88
	20 ms	24.00	1.50
	30 ms	34.00	2.13
G.729A/ G.729AB	10 ms	5.25	0.33
	20 ms	6.50	0.41
	30 ms	7.75	0.48
G.723.1 5.3 kbit/s	30 ms	6.50	0.41
G.723.1 6.3 kbit/s	30 ms	7.00	0.44

Queuing delay

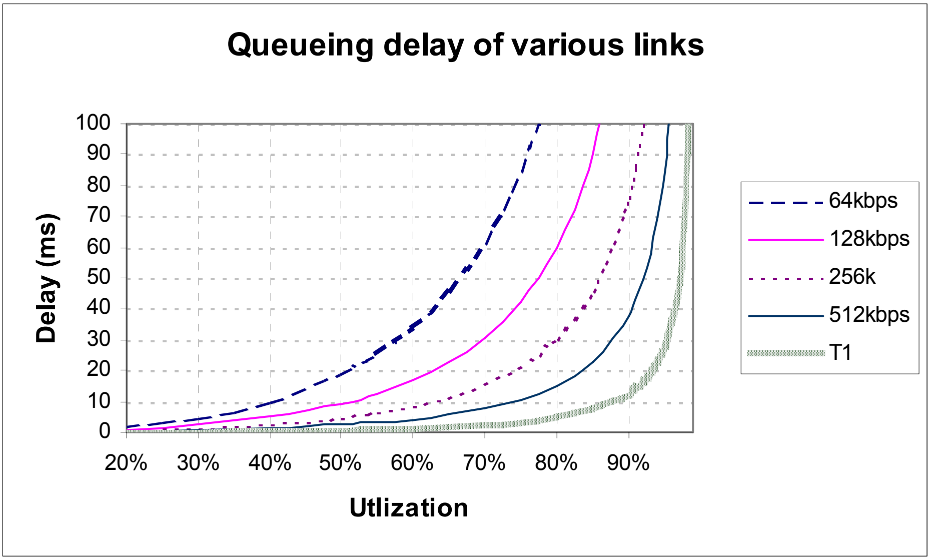
Queueing delay is the time it takes for a packet to wait in transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queueing time in ms is estimated by the following formula:

p*p*(average intranet packet in bytes)/(1-p)/(link speed in kbit/s)

where p is the link utilization level.

The average size of intranet packets carried over WAN links generally is between 250 and 500 bytes. Figure 26 displays the average queueing delay of the network based on a 300-byte average packet size.

Figure 26
Queuing delay of various links



553-9183

As can be seen in Figure 26, queueing delays can be significant for links with bandwidth under 512 kbit/s. Higher speed links can tolerate much higher utilization levels.

Routing and hop count

Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design at many levels, such as the architecture, topology, routing configuration, link and speed.

IP Trunk 3.01 (and later) system delay

Together, the transmitting and receiving IP Trunk 3.01 (and later) nodes contribute a processing delay of about 33 ms to the end-to-end delay. This is the amount of time required for the encoder to analyze and packetize speech, and is required by the decoder to reconstruct and de-packetize the voice packets.

There is a second component of delay which occurs on the receiving IP Trunk 3.01 (and later) node. For every call terminating on the receiver, there is a jitter buffer which serves as a holding queue for voice packets arriving at the destination ITG. The purpose of the jitter buffer is to smooth out the effects of delay variation, so that a steady stream of voice packets can be reproduced at the destination. The default jitter buffer delay for voice is 60 ms.

Other delay components

Other delay components, generally considered minor, are as follows.

- **Router processing delay**
  The time it takes to forward a packet from one link to another on the router is the transit or router processing delay. In a healthy network, router processing delay is a few milliseconds.

- **LAN segment delay**
  The transmission and processing delay of packets through a healthy LAN subnet is just one or two milliseconds.

Reduce link delay

In this and the next few sections, different methods of reducing one-way delay and packet loss in the IP Trunk 3.01 (and later) network are examined.

Link delay is defined as the time it takes for a voice packet to be queued on the transmission buffer of a link until it is received at the next hop router. Link delay can be reduced by the following:

- Upgrading link capacity.
  This reduces the serialization delay of the packet, and more significantly, it reduces the utilization of the link and the queueing delay. To estimate how much delay can be reduced, refer to the tables and formulas given in "Serialization delay" on page 183 and "Queuing delay" on page 184. Before upgrading a link, check both routers connected to the link intended for the upgrade and comply with router configuration guidelines.
- Changing the link from satellite to terrestrial.
  This should reduce the link delay by on the order of 100 to 300 ms.
- Implementing a priority queueing discipline.
  See "Queue management" on page 178.

To determine which links should be considered for upgrading, first list all the intranet links used to support the IP Trunk 3.01 (and later) traffic, which can be derived from the Traceroute output for each site pair. Then using the intranet link utilization report, note the highest utilized and/or the slowest links. Estimate the link delay of suspect links using the Traceroute results .

Assume that a 256kbit/s link from Router1 toRouter2 has a high utilization; the following is a Traceroute output that traverses this link:

```
Richardson3% traceroute santa_clara_itg4

traceroute to santa_clara_itg4 (10.3.2.7), 30 hops
max, 32 byte packets

      router1 (10.8.0.1) 1 ms  1 ms  1 ms

      router2 (10.18.0.2) 42 ms  44 ms  38 ms

      router3 (10.28.0.3) 78 ms  70 ms  81 ms

      router4 (10.3.0.1) 92 ms  90 ms  101 ms
```

```
santa_clara_itg4 (10.3.2.7) 94 ms  97 ms  95 ms
```

The average rtt time on that link is about 40 ms; the one-way link delay is about 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of this link's delay is caused by queueing. Looking at Figure 26 on page 185, if this link is upgraded to T1, approximately 19 ms is shaved off the delay budget.

Reduce hop count

End-to-end delay can be reduced significantly by reducing hop count, especially on hops that traverse WAN links. Some the ways to reduce hop count include the following:

- Attach the TLAN subnet directly to the WAN router.
- Improve meshing. Add links to help improve meshing; adding a link from router1 to router4 in the previous Traceroute example might cause the routing protocol to use that new link, thereby reducing the hop count by two.
- Node reduction. Co-located nodes can be connected into one larger and more powerful router.

These guidelines affect the whole intranet, as they affect network architecture, design and policies and involves considering cost, political and IP design issues. These topics are beyond the scope of this document.

Adjust jitter buffer size

The jitter buffer parameters directly affect end-to-end delay. Lowering the voice playout settings decreases one-way delay, but the decrease comes at a cost of allowing less waiting time for voice packets that arrive late. Refer to “IP Trunk 3.01 (and later) DSP profile settings” on page 222 for guidelines on re-sizing the jitter buffer.

Reduce packet loss

Packet loss in intranets is generally related to congestion somewhere in the network. Bottlenecks in links are where the packet loss is high because packets get dropped, as the packets are arriving faster than the link can transmit them. The task of upgrading highly utilized links can remove the source of packet loss on a particular flow. An effort to reduce hop count gives fewer opportunities for routers and links to drop packets.

Other causes of packet loss not related to queueing delay are as follows:

- Poor link quality.
  The underlying circuit could have such problems as transmission problems, high line error rates, and be subject to frequent outages. The circuit might possibly be provisioned on top of other services, such as X.25, Frame Relay, or ATM. Check with the service provider for information.
- Overloaded CPU.
  This is another commonly-monitored statistic collected by network management systems. If a router is overloaded, it means that the router is constantly performing processing-intensive tasks, which impedes the router from forwarding packets. Determine what the threshold CPU utilization level is and check if any suspect router conforms to the threshold. The router might have to be re-configured or upgraded.
- Saturation.
  Routers can be overworked when there are too many high capacity and high traffic links configured on it. Ensure that routers are dimensioned according to vendor guidelines.
- LAN saturation.
  Packets might also be dropped on under-engineered or faulty LAN segments.
- Jitter buffer too small.
  Packets that arrive at the destination, but too late to be placed in the jitter buffer, are essentially lost packets as well. Refer to “Adjust jitter buffer size” on page 188.
- Frame slips.
  Ensure that clocks are synchronized correctly.

Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation might overlook a substantially better route. A high delay variation can be caused by routing instability, misconfigured routing, inappropriate load splitting, or frequent changes to the intranet. Severe asymmetrical routing results in one site perceiving a poorer QoS than the other site.

The Traceroute program can be used to uncover these routing anomalies. Then routing implementation and policies can be audited and corrected.

Network modeling

Network analysis can be difficult or time-consuming if the intranet and the expected IP Trunk 3.01 (and later) installation is large. Commercial network modeling tools exist to analyze what-if scenarios predicting the effect of topology, routing, and bandwidth changes to the network. The modelling tools work with an existing network management system to load current configuration, traffic and policies into the modelling tool. Network modeling tools can help to analyze and try out any of the recommendations given in this document to predict how delay and error characteristics would change the network.

Time-of-Day voice routing

Other important objectives associated with IP Trunk 3.01 (and later) network translations and route list blocks are as follows:

1. Make IP Trunk 3.01 (and later) the first-choice, least-cost entry in the Route List Block.
2. Use Time-of-Day (ToD) scheduling to block voice traffic to the IP Trunk 3.01 (and later) route during peak traffic periods on the IP data network when degraded QoS causes all destination IP Trunk 3.01 (and later) nodes to be in fallback mode.

The proper time to implement either setting is described as follows:

1. Make the IP Trunk 3.01 (and later) the first-choice, least-cost entry in the route list block.

   An IP Trunk 3.01 (and later) route should be configured with a higher priority (lower entry number) than the fallback route in the LD 86 Route List Blocks (RLB) of the ESN configuration. All calls to the target destination with VoIP capability will try the IP route first before falling back to traditional circuit-switched network.

2 Turn off the IP Trunk 3.01 (and later) route during peak traffic periods on the IP data network.

Based on site data, if fallback routing occurs frequently and consistently for a data network during specific busy hours; for example, every Monday 10-11 a.m., and Tuesday 2-3 p.m. These hours should be excluded from the RLB to maintain a high QoS for voice services. By not offering voice traffic to a data network during known peak traffic hours, the incidence of conversation with marginal QoS can be minimized. This technique reduces some of the cost savings associated with using IP Trunk 3.01 (and later) and should only be utilized if other methods of improving the IP network QoS are not possible.

The time schedule is a 24-hour clock which is divided up the same way for all 7 days. Basic steps to program ToD for IP Trunk 3.01 (and later) routes are as follows:

a Go to LD 86 ESN data block to configure the Time-of-Day Schedule (TODS) for the required ITG control periods.

b Go to LD 86 RLB and apply the TODS on/off toggle for that route list entry associated with an IP Trunk 3.01 (and later) route.

3 Use the traditional PSTN for modem traffic.

IP Trunk 3.01 (and later) does not support modem traffic except Group 3 fax. Routing controls must be configured to route modem traffic over circuit-switched trunks instead of over IP Trunk 3.01 (and later).

Use the ESN TGAR, NCOS, and facility restriction levels to keep general modem traffic off the IP Trunk 3.01 (and later) route.

Measure intranet QoS

End-to-end delay and error characteristics of the current state of the intranet can be measured. These measurements help set acceptable QoS standards when using the corporate intranet to transmit voice services.

QoS evaluation process overview

There are two main objectives when dealing with the QoS issue in an IP Trunk 3.01 (and later) network:

1 to predict the expected QoS

2 to evaluate the QoS after integrating IP Trunk 3.01 (and later) traffic into the intranet

The process for either case is similar; one is without IP Trunk 3.01 (and later) traffic and one is with. The differences are discussed in this section.

In the process, it is assumed that the PING program is available on a PC, or some network management tool is available to collect delay and loss data and access the TLAN subnet that connects to the router to the intranet.

1 Use PING or an equivalent tool to collect round-trip delay (in ms) and loss (in%) data.

2 Divide the delay by 2 to approximate one-way delay. Add 93 ms to adjust for ITG processing and buffering time.

3 Use a QoS chart, or Table 34 on page 206, to predict the QoS categories: excellent, good, fair or poor.

4 If a customer wants to manage the QoS in a more detailed fashion, re-balance the values of delay compared to loss by adjusting IP Trunk 3.01 (and later) system parameters, such as preferred codec, payload size, and routing algorithm, to move resulting QoS among different categories.

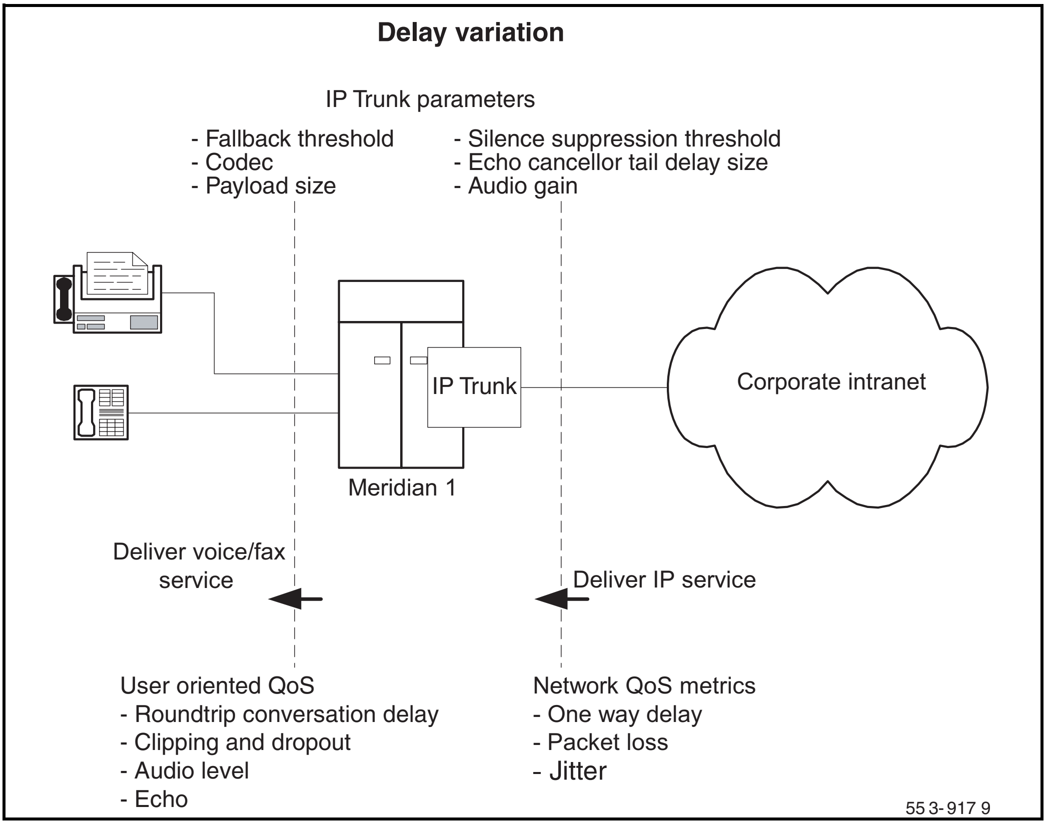
5 If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

Set QoS expectations

The users of corporate voice and data services expect these services to meet some perceived QoS, which in turn influences network design. The goal is to design and allocate enough resources in the network to meet users’ needs. QoS metrics or parameters are what quantifies the needs of the “user” of the “service”.

In the context of a Meridian 1/CS 1000M system with IP Trunk 3.01 (and later), Figure 27 shows the relationship between users and services.

Figure 27
Relationship between users and services



From the diagram, it can be seen that there are two interfaces to consider:

- The Meridian 1/CS 1000M system, including the IP Trunk 3.01 (and later) nodes, interfaces with the end users; voice services offered by the system must meet user-oriented QoS objectives.
- The IP Trunk 3.01 (and later) nodes interface with the intranet; the service provided by the intranet is “best-effort delivery of IP packets”, not “guarantee QoS for real-time voice transport.” IP Trunk 3.01 (and later) translates the QoS objectives set by the end-users into IP-oriented QoS objectives. The guidelines call these objectives *intranet QoS objectives*.

The IP Trunk 3.01 (and later) node can be enabled to monitor the intranet's QoS. In this mode, two parameters, the *receive fallback threshold* and the *transmit fallback threshold,* on the IP Trunk 3.01 (and later) node dictate the minimum *QoS level* of the IP Trunk 3.01 (and later) network. The fallback thresholds are configured on a per-site pair basis.

The QoS level is a user-oriented QoS metric which takes on one of these four settings: excellent, good, fair, and poor, indicating the quality of voice service. IP Trunk 3.01 (and later) periodically calculates the prevailing QoS level per site pair, based on its measurement of the following:

- one-way delay
- packet loss
- Codec

When the QoS level is below the fallback threshold, any new calls to that destination are routed over circuit-switched voice facilities.

The computation is derived from ITU-T G.107 Transmission Rating Model. When the QoS level falls below the fallback threshold levels for that particular destination, that call is not accepted by the originating IP Trunk 3.01 (and later) node; instead the call is re-routed by ESN features over traditional circuit-switched voice facilities.

Figure 28, Figure 29 on page 196, and Figure 30 on page 197 show the operating regions in terms of *one-way delay* and *packet loss* for each codec and required QoS level as determined by IP Trunk 3.01 (and later). Note that among the codecs, G.711(A-law)/G.711(u-law) delivers the best quality for a given intranet QoS, followed by G.729AB and then G.723.1 (6.4 kbp/s) and lastly G.723.1 (5.3 kbp/s). These figures determine the delay and error budget for the underlying intranet in order for it to deliver a required quality of voice service.

Fax is more susceptible to packet loss than the human ear is; quality starts to degrade when packet loss exceeds 4%. Nortel recommends that fax services be supported with IP Trunk 3.01 (and later) operating in either the Excellent or Good QoS level. Avoid offering fax services between two sites that can guarantee no better than a Fair or Poor QoS level.

Figure 28
QoS levels with G.729A/AB codec

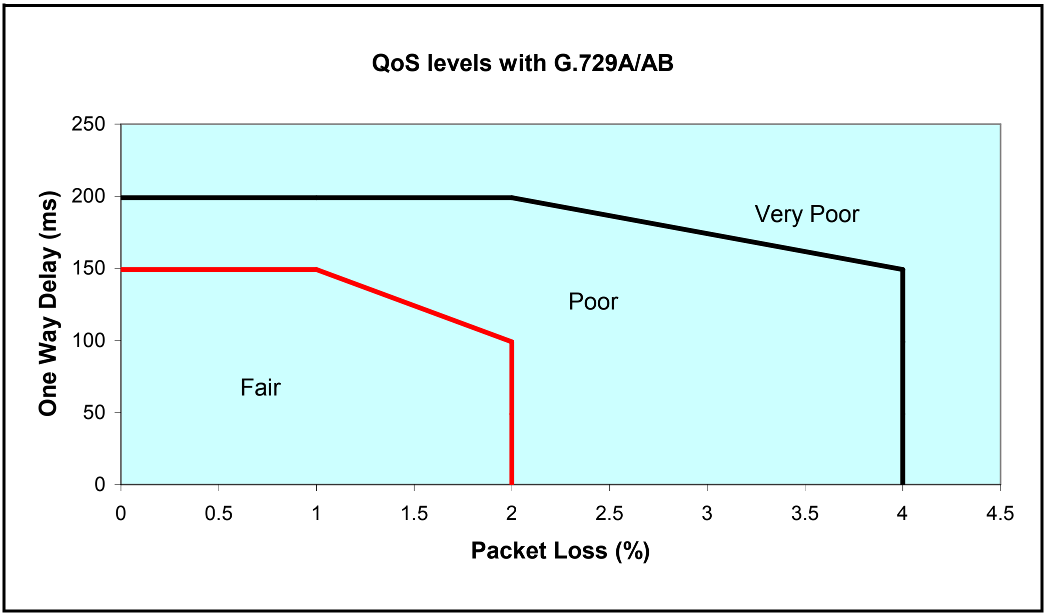


Figure 29
QoS level with G.711 codec

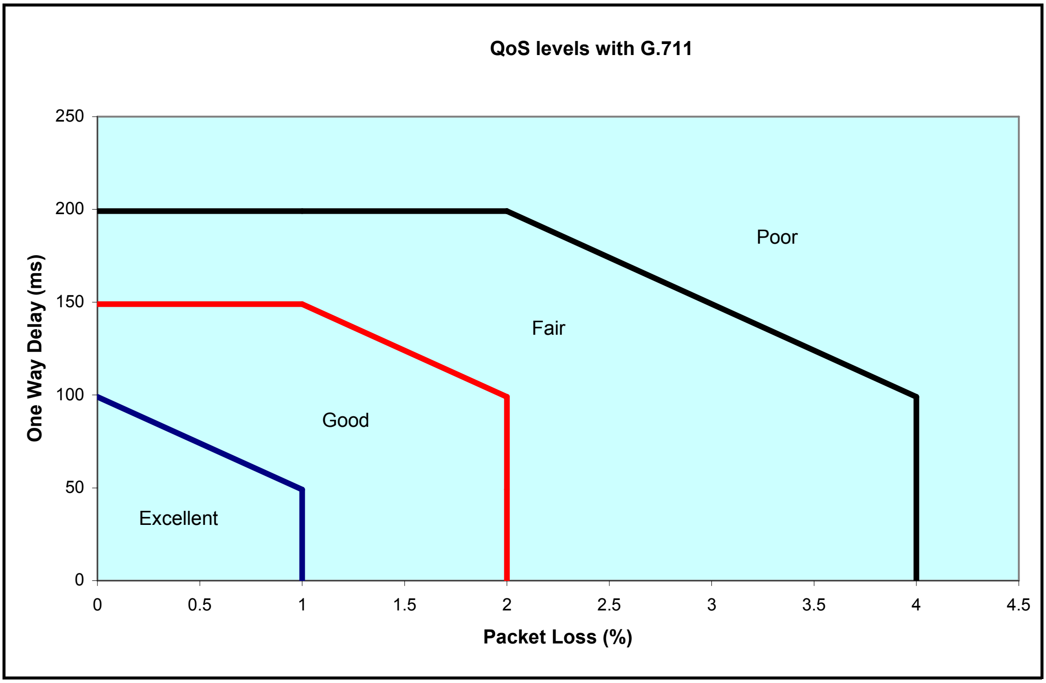
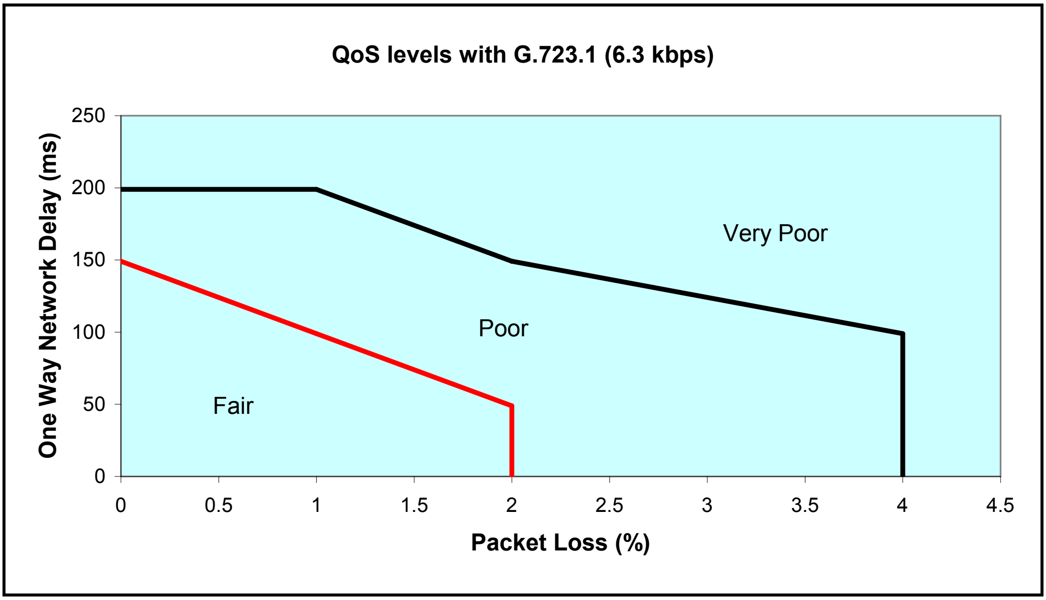


Figure 30
QoS level with G.723 codec



Obtain QoS measurement tools

PING and Traceroute are standard IP tools that are usually included with a network host's TCP/IP stack. A survey of QoS measurement tools and packages, including commercial ones, can be found in the home page of the Cooperative Association for Internet Data Analysis (CAIDA) at www.caida.org These include delay monitoring tools that include features like timestamping, plotting, and computation of standard deviation.

Measure end-to-end network delay

The basic tool used in IP networks to measure end-to-end network delay is the `PING` program. `PING` takes a delay sample by sending an ICMP packet from the host of the `PING` program to a destination server. `PING` then waits for the packet to make a round trip. A sample of PING is as follows:

```
Richardson3% PING -s santa_clara_itg4 60
```

```
PING santa_clara4 (10.3.2.7): 60 data bytes

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=97ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=100ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=102ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=97ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=95ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=94ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=112ms

68 bytes from (10.3.2.7): icmp_seq=0 ttl=225
time=97ms

^?

--- Richardson3 PING Statistics ---

8 packets transmitted, 8 packets received, 0% packet
loss

round-trip (ms) min/avg/max = 94/96/112
```

The time field displays the round trip time (*rtt*).

So that the delay sample results match what the IP Trunk 3.01 (and later) node can experience, the PING host must be on a working LAN segment attached to the router supporting the IP Trunk 3.01 (and later) node. The selection of destination host is just as important, following these same guidelines for the source host.

Set the size of the PING probe packets to 60 bytes, to approximate the size of probe packets sent by IP Trunk 3.01 (and later) used in determining when new calls need to fall back.

Some implementations of PING support the -v option for setting the TOS. IP Trunk 3.01 (and later) allows the 8-bit DiffServ/TOS field to be set to any value specified by the IP network administrator for QoS management purposes. For example, if a decimal value of 36 is entered in OTM 2.1 (and later), this is interpreted as TOS Precedence = Priority and Reliability = High. If PING measurements are made on an intranet that uses prioritization based on the TOS field, the *rtt* measured will be higher than the actual delay of voice packets when the -v option is not used. See “Queue management” on page 178.

Make note of the variation of *rtt* from the PING output. It is from repeated sampling of *rtt* that a delay characteristic of the intranet can be obtained. In order to obtain a delay distribution, the PING tool can be embedded in a script which controls the frequency of the PING probes, timestamps them, and stores the samples in a raw data file. The file can then be to be analyzed later using spreadsheet and other statistics packages. Determine if the intranet's network management software has any delay measurement modules which can obtain a delay distribution for specific site pairs.

Delay characteristics vary depending on the site pair and the time-of-day. The assessment of the intranet should include taking delay measurements for each IP Trunk 3.01 (and later) site pair. If there are significant fluctuations of traffic in the intranet, it is best to include PING samples during the intranet's peak hour. For a more complete assessment of the intranet's delay characteristics, obtain PING measurements over a period of at least a week.

Measure end-to-end packet loss

The PING program also reports if the ICMP packet made its round trip correctly or not. Use the same PING host setup to measure end-to-end error. Use the same packet size parameter.

Sampling error rate, however, requires taking multiple PING samples, at least 30 to be statistically significant. Therefore, obtaining an error distribution requires running PING over a greater period of time. The error rate statistic collected by multiple PING samples is called Packet Loss Rate (PLR).

Adjust PING measurements

Make adjustments to the PING statistics as required in the following situations.

One-way as compared to roundtrip

The PING statistics are based on round trip measurements, where the QoS metrics in the Transmission Rating model are one-way. In order to make the comparison compatible, the delay and packet error PING statistics are to be halved.

Adjustment caused by IP Trunk 3.01 (and later) processing

The PING measurements are taken from PING host to PING host. The Transmission Rating QoS metrics are from end-user to end-user and include components outside the intranet. The PING statistic for delay must be further modified by adding 93 ms to account for the processing and jitter buffer delay of the IP Trunk 3.01 (and later) nodes. No adjustment has to be made for error rates.

If the intranet measurement barely meets the round trip QoS objectives, there is a possibility that the one-way QoS is not met in one of the direction of flow. This can be true even if the flow is on a symmetric route, due to the asymmetric behavior of data processing services.

Late packets

Packets that arrived outside of the window allowed by the jitter buffer are discarded by IP Trunk 3.01 (and later). To determine which PING samples to ignore, first calculate the average one-way delay based on all the samples. Add 500 ms to the average. This is the maximum delay. All samples whose one-way delay exceeds this maximum are considered late packets and removed from the sample. Calculate the percentage of late packets and add that to the packet loss statistic.

Network delay and packet loss evaluation example

From PING data, calculate the average one-way delay (halved from PING output and adding 93 ms IP Trunk 3.01 (and later) processing delay) and standard deviation for latency. Do a similar calculation for packet loss without adjustment.

Adding a standard deviation to the mean of both delay and loss is for planning purposes. A customer might want to know whether traffic fluctuation in their intranet reduces the user's QoS.

Table 29 provides a sample measurement of network delay and packet loss for the G.729A codec between various nodes.

Table 29
Sample measurement results for G.729A codec

	Measured one-way delay (ms)		Measured Packet loss (%)		Expected QoS level (See page 206)	
Destination pair	**Mean**	**Mean+σ**	**Mean**	**Mean+σ**	**Mean**	**Mean+σ**
Santa Clara/ Richardson	171	179	1.5	2.1	Excellent	Good
Santa Clara/ Ottawa	120	132	1.3	1.6	Excellent	Excellent
Santa Clara/ Tokyo	190	210	2.1	2.3	Good	Good
Richardson/ Ottawa	220	235	2.4	2.7	Good	Good

As an example, the delay and loss pair of traffic from Santa Clara to Richardson (171 ms and 1.5%) will meet "excellent" criterion, but their counter part with standard deviation (179 ms and 2.1%) can achieve only "good" QoS.

Since the algorithm implemented in IP Trunk 3.01 (and later) calculates only mean and not standard deviation, it confirms the “excellent” rating (if the objective is set for excellent, it will not fallback to alternate facilities), but the customer has up to a 50% chance of experiencing a service level inferior to an “excellent” level.

In contrast, the site pair Santa Clara/Ottawa has both QoS levels of mean and mean+standard deviation falling in the excellent region. The customer has more confidence that during peak traffic period, the “excellent” service level is likely to be upheld (better than 84% chance under the assumption of Normal distribution).

Other measurement considerations

The PING statistics described above measure the intranet prior to IP Trunk 3.01 (and later) installation, which means that the measurement does not take into consideration the expected load created by the IP Trunk 3.01 (and later) users.

If the intranet capacity is tight and the IP Trunk 3.01 (and later) traffic significant, consider making intranet measurements under load. Load can be applied using traffic generator tools. The amount of load should match the IP Trunk 3.01 (and later)-offered traffic estimated in “IP Trunk 3.01 (and later) traffic engineering” on page 134.

Estimate voice quality

The perceived quality of a telephone call is dependent on many factors, such as codec characteristics, end-to-end delay, packet loss, and the perception of the individual listener.

The E-Model Transmission Planning Tool is a model used to produce a quantifiable measure of voice quality based on relevant factors. Refer to two ITU-T recommendations (ITU-T E.107 and E.108) for more information on the E-Model and its application.

A simplified version of the E-Model is applied to IP Trunk 3.01 (and later) to provide an estimate of the voice quality that the user can expect, based on various configuration choices and network performance metrics.

The simplified E-Model is as follows:

R = 94 – lc – ld – lp

where:
lc = codec impairment (see Table 30 on page 203)

ld = delay impairment (see Table 31 on page 204)

lp = packet loss impairment (see Table 32 on page 204)

Note: This model already takes into account some characteristics of the IP Phone, and therefore the impairment factors are not identical to those shown in the ITU-T standards.

Refer to Table 33 on page 205 for the translation of R values into user satisfaction levels.

Table 30
Impairment factors of codecs

Codec	Codec Impairment (lc) (msec frames)
G.711	0
G.729A/AB	11 - 20 or 30
G.729A/AB	16 - 40 or 50
G.723.1 (5.3 Kbps)	19
G.723.1 (6.3 Kbps)	15

Table 31
Impairment factors due to network delay

Network delay* (msec)	Delay Impairment (Id)
0 - 49	0
50 - 99	5
100 -149	10
150 - 199	15
200 - 249	20
250 - 299	25
* Network delay is the average one-way network delay plus packetization and jitter buffer delay.	

Table 32
Impairment factors due to packet loss

Packet loss (%)	Packet Lose Impairment (Ip)
0	0
1	4
2	8
4	15
8	25

Table 33
R value translation

R Value (lower limit)	MOS	User Satisfaction
90	4.5	Very satisfied
80	4.0	Satisfied
70	3.5	Some users dissatisfied
60	3.0	Many users dissatisfied
50	2.5	Nearly all users dissatisfied
0	1	Not recommended

Use Table 34 to estimate the IP Trunk 3.01 (and later) QoS level based on QoS measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10 ms respectively. The techniques used to determine and apply the information in this table are Nortel proprietary.

Table 34
IP Trunk 3.01 (and later) QoS levels (Part 1 of 3)

		QoS level		
Network delay (ms)	**Packet loss (%)**	**G.711 20**	**G.729A/AB 30**	**G.723.1 (6.3 Kbps) 30**
0 – 49	0	excellent	good	fair
49		excellent	fair	fair
49	2	good	fair	fair
49	4	fair	poor	poor
49	8	poor	not recommended	not recommended
50 – 99	0	excellent	fair	fair
99	1	good	fair	fair
99	2	good	fair	poor
99	4	fair	poor	poor
99	8	poor	not recommended	not recommended
100 – 149	0	good	fair	fair
149	1	good	fair	poor

Note: The QoS levels are equivalent to the following MOS values: See page 108 for more details.

- excellent 4.5
- good 4
- fair 3
- poor 2
- not recommended less than 2

Table 34
IP Trunk 3.01 (and later) QoS levels (Part 2 of 3)

		QoS level		
Network delay (ms)	**Packet loss (%)**	**G.711 20**	**G.729A/AB 30**	**G.723.1 (6.3 Kbps) 30**
149	2	fair	poor	poor
149	4	fair	poor	not recommended
149	8	poor	not recommended	not recommended
150 – 199	0	fair	poor	poor
199	1	fair	poor	good
199	2	fair	poor	fair
199	4	poor	not recommended	not recommended
199	8	not recommended	not recommended	not recommended
200 – 249	0	poor	not recommended	not recommended
249	1	poor	not recommended	not recommended
249	2	poor	not recommended	not recommended
249	4	not recommended	not recommended	not recommended
249	8	not recommended	not recommended	not recommended
250 – 299	0	poor	not recommended	not recommended

Note: The QoS levels are equivalent to the following MOS values: See page 108 for more details.

excellent	4.5
good	4
fair	3
poor	2
not recommended	less than 2

Table 34
IP Trunk 3.01 (and later) QoS levels (Part 3 of 3)

		QoS level		
Network delay (ms)	**Packet loss (%)**	**G.711 20**	**G.729A/AB 30**	**G.723.1 (6.3 Kbps) 30**
299	1	poor	not recommended	not recommended
299	2	poor	not recommended	not recommended
299	4	not recommended	not recommended	not recommended
299	8	not recommended	not recommended	not recommended

Note: The QoS levels are equivalent to the following MOS values: See page 108 for more details.

- excellent 4.5
- good 4
- fair 3
- poor 2
- not recommended less than 2

Sample scenarios

Scenario 1

A local LAN has the following characteristics:

- G.711 codec
- 20 msec network delay
- 0.5% packet loss

To calculate R = 94 - lc - ld - lp, use Table 30, Table 31, and Table 32:

- G.711 codec: lc = 0

- 20 msec network delay: ld = 0
- 0.5% packet loss: lp = 2

Then:

R = 94 - 0 - 0 - 2

R = 92

Using Table 34 on page 206, a value of 92 means the users are very satisfied.

Scenario 2

A campus network has the following characteristics:

- G.711 codec
- 50 msecs delay
- 1.0% packet loss

To calculate R = 94 - lc - ld - lp, use Table 30 on page 203, Table 31 on page 204, and Table 32 on page 204:

- G.711 codec: lc = 0
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 4

Then:

R = 94 - 0 - 5 - 4

R = 85

Using Table 34 on page 206, a value of 85 means that the users are satisfied.

Scenario 3

A WAN has the following characteristics:

- G.729 codec

- 30 msec network delay
- 2% packet loss

To calculate R = 94 - lc - ld - lp, use Table 30, Table 31, and Table 32:

- G.711 codec: lc = 11
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 8

Then:

R = 94 - 11 - 5 - 8

R = 70

Using Table 34 on page 206, a value of 70 means some users are dissatisfied.

Does the intranet meet expected IP Trunk 3.01 (and later) QoS?

At the end of this measurement and analysis, there should be a good indication if the corporate intranet in its present state can deliver adequate voice and fax services. Looking at the “Expected QoS level” column in Table 29 on page 201, the QoS level for each site pair can be gauged.

In order to offer voice and fax services over the intranet, keep the network within a “Good” or “Excellent” QoS level at the Mean+s operating region. Fax services should not be offered on routes that have only “Fair” or “Poor” QoS levels.

If the expected QoS levels of some or all routes fall short of “Good”, evaluate the options and costs for upgrading the intranet. Estimate the amount of one-way delay that must be reduced to raise the QoS level. The section “Fine-tune network QoS” on page 182 provides guidelines for reducing one-way delay. Often this involves a link upgrade, a topology change, or implementation of QoS in the network.

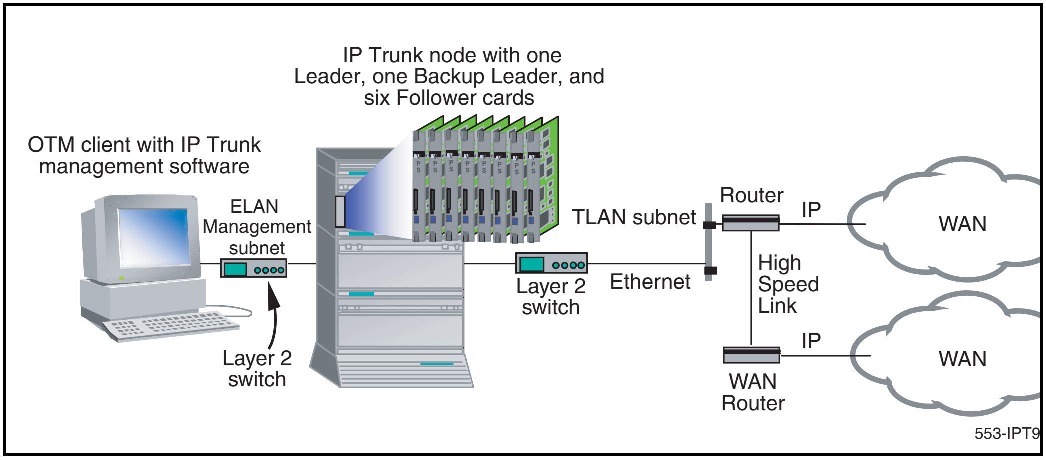
A decision can be made to keep costs down and accept a temporary “Fair” QoS level for a selected route. In that case, having made a calculated trade-off in quality, carefully monitor the QoS level, reset expectations with the end users and be receptive to user feedback.

IP Trunk 3.01 (and later) LAN installation and configuration

Basic setup of the IP Trunk 3.01 (and later) system

Figure 31 on page 211 shows an example of a basic recommended IP Trunk 3.01 (and later) system setup, with separate TLAN (voice) and ELAN (management) subnets. This is an example only; it is not necessarily the setup that must be used.

Figure 31
Basic setup of the IP Trunk 3.01 (and later) system



IP trunk card connections

10/100BaseT Ethernet ports

The Media Card 32-port and ITG-Pentium 24-port trunk cards each have two Ethernet ports.

The 10/100BaseT Ethernet port on the DSP daughterboard, with connectors located on the faceplate or on the I/O panel breakout cable, transmits Voice over IP (VoIP) traffic and connects to the Telephony LAN (TLAN) subnet.

The 10BaseT network interface on the motherboard with a connector on the I/O panel breakout cable transmits IP Trunk 3.01 (and later) system management traffic and D-channel and connects to the ELAN subnet.

RS-232 serial ports

The Media Card 32-port trunk card and ITG-Pentium 24-port trunk card have a DIN-8 serial maintenance port connection on the faceplate and an alternative connection to the same serial port on the I/O panel breakout cable.

Do not connect two maintenance terminals to both the faceplate and I/O panel breakout cable serial maintenance port connections at the same time.

Configure a system with separate subnets for voice and management

Recommendation

Nortel recommends using separate dedicated VLANs and ELAN and TLAN subnets, separated by a router/Layer 3 switch. Refer to "Configure a system with separate subnets for voice and management" on page 212. If it is necessary to use a single ELAN and TLAN subnet, refer to "Single subnet option for voice and management" on page 215.

The Media Card 32-port and ITG-Pentium 24-port trunk cards have two Ethernet ports per card, so the IP Trunk 3.01 (and later) system can support two different TLAN and ELAN subnet connections. The advantages of this setup are as follows:

- to optimize VoIP performance on the TLAN subnet by segregating it from ELAN subnet traffic and connecting the TLAN subnet as close as possible to the WAN router
- to make the amount of traffic on the TLAN subnet more predictable for QoS engineering

- to optimize ELAN subnet performance (for example, for Symposium Call Center Server (SCCS) and CallPilot functional signaling) by segregating the ELAN subnet from TLAN subnet voice traffic
- to enhance network access security by allowing the modem router to be placed on the ELAN subnet, which can be isolated from the customer's network or have access to/from the TLAN subnet only through a firewall router

  Note: When using separate subnets as recommended, the Network Activity LEDs provide valuable maintenance information for the Ethernet voice interface. When using an ITG-Pentium 24-port trunk card in a single subnet configuration, all traffic uses the ELAN subnet. This eliminates the use of the TLAN (voice) network interface.

Subnet configurations

The following restrictions apply:

- The Leader 0 and Leader 1 cards must co-reside on a single TLAN subnet with the Node IP Address.
- Follower cards can reside on separate TLAN subnets.
- All IP trunk cards belonging to the same node must co-reside on the same ELAN subnet.

For dual subnet configuration, make sure the TLAN and ELAN subnets do not overlap.

Example 1
Invalid configuration

The following configuration is not valid, as the TLAN and ELAN subnets overlap.

ELAN IP	10.0.0.136
ELAN GW	10.0.0.129
ELAN Subnet Mask	255.255.255.224
TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57

TLAN GW	10.0.0.1
TLAN Subnet Mask	255.255.255.0.

The ELAN subnet range of addresses – 10.0.0.129 to 10.0.0.160 – overlaps the TLAN subnet range of addresses – 10.0.0.1 to 10.0.0.255. This contravenes the IP addressing practices, as it is equally valid to route the IP packets over either interface. The resulting behavior from such a setup is undetermined.

The overlapping IP address scheme must be corrected when adding a Media Card 32-port trunk card to an existing ITG Trunk 2.x node that consists of ITG 24-port trunk cards and ITG 8-port trunk cards.

Example 2
Valid configuration

The following configuration is valid, as the ELAN and TLAN subnets do not overlap.

The IP addresses can be split as follows.

ELAN IP	10.0.0.136
ELAN GW	10.0.0.129
ELAN Subnet Mask	255.255.255.224

TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57
TLAN GW	10.0.0.1
TLAN Subnet Mask	255.255.255.128.

The TLAN subnet has a range of addresses from 10.0.0.1 to 10.0.0.127. The ELAN subnet is in a separate subnet, with a range of addresses from 10.0.0.129 to 10.0.0.160. This configuration results in smaller TLAN subnet addresses, but it fulfills the requirement that subnets do not overlap.

Selecting public or private IP addresses

Consider a number of factors to determine if the TLAN and ELAN subnets will use private (internal IP addresses) or public IP addresses.

Private IP addresses

Private IP addresses are internal IP addresses that are not routed over the internet. They can be routed directly between separate intranets, provided that there are no duplicated subnets in the private IP addresses. Private IP addresses can be used to configure the TLAN and ELAN subnets, so that scarce public IP addresses are used efficiently.

Three blocks of IP addresses have been reserved for private intranets:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Some routers and firewalls provide a Network Address Translation (NAT) function that allows the customer to map a registered globally unique public IP address to a private IP address without re-numbering an existing private IP address autonomous domain. NAT allows private IP addresses to be accessed selectively over the internet.

Public IP addresses

Public IP addresses can be used for the TLAN and ELAN subnets, but consume limited resources.

This has the same result as the private IP address solution, but the ELAN subnet is accessible from the internet without NAT.

Single subnet option for voice and management

Although not recommended, the “single subnet” option for voice and management could be used in the following situations:

- The combined voice and management traffic on the ELAN subnet is so low that there is no impact on packetized voice QoS performance.
- The customer is willing to tolerate occasional voice quality impairments caused by excessive management traffic.

- There is no modem router on the IP Trunk 3.01 (and later) ELAN subnet because remote support access is provided by Remote Access Server (RAS) on the TLAN subnet.
- Remote support access is not required, and there is no firewall router between the ELAN subnet and the TLAN subnet.

Multiple IP Trunk 3.01 (and later) nodes on the same ELAN and TLAN segments

There are several configurations where it is acceptable to put multiple IP Trunk 3.01 nodes on the same dedicated ELAN and TLAN segments (separate subnets), or on a dedicated ELAN/TLAN segment (single subnet):

1 Several IP Trunk 3.01 (and later) nodes belonging to the same customer in the same system can be configured to route calls with different codecs depending on the digits dialed or the NCOS of the originating telephone, or to limit the maximum number of IP Trunk 3.01 (and later) calls to a particular destination node. The traffic engineering considerations on the TLAN subnet should determine how many different IP Trunk 3.01 nodes can be configured on the same LAN segment.

2 Layer 2 (10 BaseT or 100 Base TX) switching equipment or ATM infrastructure can support a Virtual LAN (VLAN) segment that is distributed across a campus or larger corporate network. In this case, some or all of the ITG destination nodes can be on the same subnet.

3 In test labs, training centers, and trade shows, it is common for destination nodes to be located on the same LAN segment and subnet.

General LAN considerations

Although the TLAN subnet traffic capacity does not limit IP Trunk 3.01 (and later) network engineering, the IP Trunk 3.01 (and later) network design must take into consideration the limitations of the existing LAN and WAN equipment.

Passive Ethernet hubs are not supported. Use Layer Two Ethernet switches for both the ELAN and TLAN subnets. Ideally, managed switches should be used.

WARNING

The ELAN and TLAN subnets must be connected to Layer 2 switches. Shared-media hubs are not supported, as they cause unreliable system operation and unpredictable voice quality.

ELAN and TLAN network interface half- or full-duplex operation

The ELAN network interface on the Media Card 32-port trunk card and the ITG-Pentium 24-port trunk card operates at half-duplex only and is limited to 10BaseT operation. This is due to filtering on the back planes.

The TLAN network interface on the Media Card 32-port trunk card and the ITG-Pentium 24-port trunk card operates on half-duplex or full-duplex and can run at 10BaseT or 100BaseT.

TLAN subnet design

The IP Trunk 3.01 (and later) nodes must connect to the intranet to minimize the number of router hops between the systems if there is adequate bandwidth on the WAN links for the shorter route. This reduces the fixed and variable IP packet delay, and improves the voice QoS.

If a mixed-codec IP Trunk 3.01 (and later) network, or a non-default payload size or fax settings is used, then use the LAN bandwidth consumption in

Table 18 on page 158 to estimate the amount of LAN bandwidth used by each card.

The TLAN network interface must connect to a 10/100BaseT switch. The uplink from the TLAN network interface to the router should be at least 100 Mbps. If the uplink is 100 Mbps, then the maximum number of IP trunk cards allowed on the switch is subject to the limits described in “Calculate Ethernet and WAN bandwidth usage” on page 156.

Consider implementing LAN resiliency. This can involve installing redundant up-links, backup routers and an Uninterruptible Power Source (UPS).

IMPORTANT!

Shared media hubs are not supported. Use Layer 2 switches.

Place the IP Trunk 3.01 (and later) node and the TLAN subnet router as close to the WAN backbone as possible. This enables the following:

- minimizes the number of router hops
- segregates constant bit-rate voice traffic from bursty LAN traffic
- simplifies the end-to-end QoS engineering for packet delay, jitter, and packet loss

If an access router separates the IP Trunk 3.01 (and later) node from the WAN router, there should be a high-speed link, such as Fast Ethernet, FDDI, SONET, OC-3c, ATM STS-3c, between the access router and the WAN backbone router.

Configure the TLAN subnet IP router

The IP Trunk 3.01 (and later) node must be placed on its own TLAN subnet. The router should have a separate 10/100BaseT interface for the TLAN subnet and should not contain any other traffic. Other IP devices should not be placed on the TLAN subnet.

Priority routing for voice packets

Routers having the capability to turn on priority for voice packets should have this feature enabled to improve QoS performance. If the Type of Service (TOS) field or Differentiated Services (DiffServ) is supported on the IP network, the decimal value of the DiffServ/TOS byte can be configured. For example, a decimal value of 46 is interpreted in TOS as “Precedence = Priority” and “Reliability = High”.

CAUTION — Service Interruption

Do not change the DiffServ/ToS byte from the default value unless directed by the network administrator.

Setting up the ELAN subnet

The ELAN subnet is a 10BaseT Ethernet subnet. Very little traffic is generated by the IP Trunk 3.01 (and later) node on this network. Cards generate this traffic when the cards are looking for the Active Leader after a reset and when SNMP traps are emitted due to IP trunk card events and errors.

The ELAN subnet can also carry functional signaling traffic for Symposium Call Center Server (SCCS), Small Symposium Call Center (SSCC), or CallPilot Multimedia Message Server. The ELAN subnet can be configured on a Layer 2 switch to maximize data throughput.

How to avoid system interruption

Duplex mismatch

Duplex mismatches can occur in the LAN environment when one side is set to auto-negotiate and the other is hard-configured. The auto-negotiate side adapts to the fixed-side settings, including speed. For duplex operations, the Auto-negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

To hard-configure all devices for speed/duplex, ensure every device and port is correctly configured in order to avoid duplex mismatch problems.

WARNING
Configure the ports on Layer 2 or Layer 3 switching equipment as **auto-negotiate**.

If one side is manually configured, and the other side is configured as auto-negotiate, the following situation occurs.

The auto-negotiate side sets itself to the manually configured side’s speed, but always sets itself to half-duplex transmission. If the manually-configured side is full-duplex transmission, then a mismatch occurs and voice quality is unsatisfactory.

Recommendation

Nortel recommends that any network equipment connected to the ELAN or TLAN subnet be configured as auto-negotiate for correct operation.

I/O filter connector

The other major TLAN subnet operation problem arises from the standard I/O filter connector in IPE modules on Large Systems.

Use the following guidelines to avoid system interruption stemming from the standard I/O filter connector in IPE modules:

- Ensure that the standard IPE module I/O filter is replaced with the provided Media Card/ITG-specific filter connector that removes filtering from pairs 23 and 24.
- Do not install the Media Card/ITG-specific filter connector on top of the standard IPE module I/O filter connector.
- Replace the IPE module backplane I/O ribbon cable assemblies with those that have interchangeable I/O filter connectors.

- The TLAN UTP cabling must meet the UTP CAT5 termination and impedance uniformity standards.
- The TLAN UTP cabling must not exceed 50 meters for the ITG-Pentium 24-port trunk card.

The TLAN network interface can auto-negotiate to 100BaseT full-duplex. To ensure the TLAN subnet can be used for voice, do the following:

- Install the Media Card/ITG-specific filter connector correctly by replacing the standard IPE Module I/O filter connector.
- Order new IPE Module Backplane I/O ribbon cable assemblies that have interchangeable I/O filter connectors if it becomes necessary to use one of the IPE Modules with molded-on I/O filter connectors.
- Ensure that the TLAN UTP cabling is CAT5 compliant.
- Always keep the TLAN UTP cabling to less than 50 meters for the ITG-Pentium 24-port trunk card.
- As an interim measure, connect to each ITG-Pentium 24-port trunk card and log in to the ITG> shell. In the shell, use the commands **tlanDuplexSet** and **tlanSpeedSet** to configure the TLAN interface to operate at half-duplex 10BaseT.

  Note: If the TLAN subnet is to operate at 10BaseT full-duplex, the TLAN network interface must also be configured to operate at full-duplex. If this is not done, a duplex mismatch is created. Packets are lost if the TLAN network interface is unchanged from auto-negotiate or mistakenly configured for half-duplex.

Because of its high capacity, 100BaseT Ethernet generally does not experience bottlenecks unless servicing a very large network.

WAN links are normally based on PSTN standards such as DS0, DS1, DS3, SONET STS-3c, or Frame Relay. These standards are full-duplex communication channels.

With standard PCM encoding (G.711 codec), a two-way conversation channel has a rate of 128 kbit/s (64 kbit/s in each direction). The same conversation on WAN, such as T1, only requires a 64 kbit/s channel, because a WAN channel is a full-duplex channel.

When simplex/duplex Ethernet links terminate on the ports of an Ethernet switch such as a Baystack 450, the fully duplex Ethernet up-link to the router/WAN can be loaded to 60% on each direction of the link.

IP Trunk 3.01 (and later) DSP profile settings

Codec types

The following codecs can be configured with IP Trunk 3.01 (and later):

- G.711 (A-and Mu-law)
- G.729AB
- G.723.1
- G.729B

Voice Activity Detection (VAD) can be enabled or disabled for all of these codecs using the OTM IP Trunk 3.01 (and later) interface.

Select from three DSP profiles on the IP trunk card. Profile 1 is the default setting.

- Profile 1: G.711, G.729AB, Fax
- Profile 2: G.711, G.723.1, Fax
- Profile 3: G.711, G.729B, Fax

> ***Note 1:*** The Media Card 32-port trunk card does not support Profile 3.
>
> ***Note 2:*** All IP trunk cards must have G.711 in their DSP profiles at all times in order to interwork with CS 1000S systems.

The DSP coding algorithm parameter sets the preferred codec of each IP trunk card. The recommendation is to use Profile 1, and to set the preferred codec to G.729AB with VAD/Silence Suppression with a payload setting of 30 ms. With this codec-payload combination, IP Trunk 3.01 (and later) can deliver good QoS but loads less than 10 kbit/s per port on the intranet.

Nortel recommends that all the nodes in the IP Trunk 3.01 (and later) network have a common preferred codec. From a network planning perspective, this provides a predictable load on the intranet since all calls will negotiated on one codec. If multiple preferred codecs are configured in the network, some calls will negotiate a G.723 5.3K call successfully, while other calls will default to the G.711A/G.711U codec when the originating and destination codecs do not match, since this codec is available in all three images.

Consider the effect if the IP Trunk 3.01 (and later) network results in tandem encoding for some of the users. Too much consecutive coding and encoding by G.729AB, G.723.1, or G.729B codecs can lower the end-to-end QoS.

To maintain an acceptable QoS on speech, Silence Suppression can be disabled under some conditions, such as in tandem networking conditions when some trunk facilities have excessively low audio levels.

Payload size

The IP Trunk 3.01 (and later) default payload sizes are as follows:

- 30 ms for G.729AB, G.729B, and G.723.1 codecs, and 10ms for the G.711A-law and G.711 mu-law codecs
- 30 bytes for fax

The payload size is adjustable to 10 ms and 20 ms for the G.711A-law/G.711 mu-law and G.729AB codec series. In a site pair that experiences packet losses, selecting a smaller payload size improves voice and fax quality, though at the cost of a higher bandwidth use. See Table 18 on page 158.

Jitter buffer parameters (voice playout delay)

There are three parameters that control the size of the jitter buffer in the destination IP Trunk 3.01 (and later) node.

1 Voice playout nominal delay. This can range from twice the payload size to 10 times, subject to a maximum of 320 ms.

2 Voice playout maximum delay.

3 Fax playout nominal delay. This can range from 0 to 300 ms, with 100 ms as the default size.

As discussed in “Adjust jitter buffer size” on page 188, lowering the jitter buffer size decreases the one-way delay of voice packets; however, setting the jitter buffer size too small causes unnecessary packet discard.

If it is necessary to discard to downsize the jitter buffer, first check the delay variation statistics. Obtain the one-way delay distributions originating from all source IP Trunk 3.01 (and later) sites, using the measurements outlined in “Measure intranet QoS” on page 191 or “Post-installation network measurements” on page 226. Compute the standard deviation of one-way delay for every flow. Some traffic sources with few hop counts yield small delay variations, but it is the flows that produce great delay variations that should be used to determine if it is acceptable to resize the jitter buffer. Compute the standard deviation (σ) of one-way delay for that flow. It is recommended that the jitter buffer size should not be set smaller than 2σ.

Silence Suppression parameters (Voice Activity Detection)

Silence Suppression, also known as Voice Activity Detection (VAD), is enabled by default on a new IP Trunk 3.01 (and later) node. Enable/disable VAD using the Enable voice activity detection checkbox on the OTM ITG Node Properties -- DSP Profile codec Options tab. See Figure 55 on page 329. To change the current DSP VAD state to match the current VAD configuration, re-transmit card properties from OTM.

When silence is detected, the IP Trunk 3.01 (and later) node sends a flag to the destination IP Trunk 3.01 (and later) node that denotes start of silence. No voice packets are sent until the silence period is broken. There are two parameters that control Silence Suppression, as follows:

1. Idle noise level. This is set at a default level of –65 dBm0.
2. Voice activity detection threshold. This is set at a default of 0dB. Voice packets are formed when the audio level exceeds the idle noise level by this threshold value.

These default parameters are suitable for most office environments. Increasing either of these two parameters lowers the amount of IP traffic generated, but increases clipping and dropped packets.

Disable Silence Suppression at tandem nodes

Silence Suppression introduces a different concept of half-duplex or full-duplex at the voice message layer that results in a kind of statistical multiplexing of voice messages over the WAN.

When a system equipped with an IP Trunk 3.01 (and later) node serves as a tandem switch in a network where some circuit-switched trunk facilities have an excessively low audio level, Silence Suppression, if enabled, degrades the quality of service by causing choppiness of speech.

Under tandem switching conditions where loss level cannot compensate, disable Silence Suppression using the OTM ITG ISDN Trunk Node Properties DSP profile tab codec options sub-tab. See Step 8 on page 330.

Disabling Silence Suppression *approximately doubles* LAN/WAN bandwidth use. Disabling Silence Suppression consumes more real-time on the IP trunk card.

Table 18 on page 158 shows the bandwidth requirement when Silence Suppression is disabled. This does not impact the data rate for fax, since fax does not have Silence Suppression enabled.

Fallback threshold

There are two parameters, the *receive fallback threshold* and the *transmit fallback threshold,* which can be configured on a per-site pair basis.

“Set QoS expectations” on page 192 and “Measure intranet QoS” on page 191 sections describe the process of determining the appropriate QoS level for operating the IP Trunk 3.01 (and later) network. Site pairs can have very different QoS measurements if some traffic flows are local, while other traffic flows are inter-continental. Consider setting a higher QoS level for the local sites compared to the international sites, thus keeping costs of international WAN links down.

Normally, the fallback threshold in both directions is set to the same QoS level. In site pairs where one direction of flow is more important, set up asymmetric QoS levels.

Setting the QoS threshold for fallback routing

The QoS thresholds for fallback routing are configured in OTM 2.1 (and later). A threshold is configured for the “Receive fallback threshold” as well as the “Transmit fallback threshold.” The available thresholds are Excellent, Good, Fair, and Poor.

Post-installation network measurements

The design process is continual, even after implementation of the IP Trunk 3.01 (and later) network and commissioning of voice services over the network. Network changes in the following – IP Trunk 3.01 (and later) traffic, general intranet traffic patterns, network policies, network topology, user expectations and networking technology – can render a design obsolete or non-compliant with QoS objectives. Review the design periodically against prevailing and trended network conditions and traffic patterns, at least once every two to three weeks initially, then eventually on a quarterly basis.

It is assumed that the customer’s organization already has processes in place to monitor, analyze, and re-design both the system network and the corporate intranet, so that both networks continue to conform to internal QoS standards. When operating VoIP services, the customer’s organization needs to incorporate additional monitoring and planing processes, as follows:

- Collect, analyze, and trend IP Trunk 3.01 (and later) traffic patterns.
- Monitor and trend one-way delay and packet loss.
- Perform changes in IP Trunk 3.01 (and later) and intranet when planning thresholds are reached.

By instituting these new processes, the IP Trunk 3.01 (and later) network can be managed to ensure that desired QoS objectives are always met.

Set ITG QoS objectives

State the design objective of the IP Trunk 3.01 (and later) network. This sets the standard for evaluating compliance to meeting users' needs. When the IP Trunk 3.01 (and later) network is first installed, the design objective expectations have been set, based on the work done in “Measure intranet QoS” on page 191. Initially, set the QoS objective so that for each destination pair, the mean+s of one-way delay and packet loss is below some threshold value to maintain calls between those two sites at a required QoS level. The graphs of Figure 29 on page 196 and Figure 30 on page 197, with the QoS measurements, help determine what threshold levels are appropriate.

Table 35 describes examples of IP Trunk 3.01 (and later) QoS objectives.

Table 35
ITG QoS objectives

Site Pair	IP Trunk 3.01 (and later) QoS objective	Fallback threshold setting
Santa Clara/ Richardson	Mean (one-way delay) + σ(one-way delay) < 120 ms Mean (packet loss) + σ(packet loss) < 0.3%	Excellent
Santa Clara/ Ottawa	Mean (one-way delay) + σ(one-way delay) < 120 ms Mean (packet loss) + σ(packet loss) < 1.1%	Excellent

In subsequent design cycles, review and refine the QoS objective, based on data collected from intranet QoS monitoring.

Having decided on a set of QoS objectives, then determine the planning threshold. The planning thresholds are based on the QoS objectives. These thresholds are used to trigger network implementation decisions when the prevailing QoS is within range of the targeted values. This gives time for implementation processes to follow through. The planning thresholds can be set 5% to 15% below the QoS objectives, depending on the implementation lag time.

Intranet QoS monitoring

To monitor one-way delay and packet loss statistics, install a delay and route monitoring tool, such as PING and Traceroute on the TLAN subnet of each IP Trunk 3.01 (and later) site. Each delay monitoring tool runs continuously, injecting probe packets to each ITG site about every minute. The amount of load generated by this is not considered significant. At the end of the month, the hours with the highest one-way delay are noted; within those hours, the packet loss and standard deviation statistics can be computed.

See “Measure intranet QoS” on page 191 for information about implementation of the PING hosts and the use of scripting.

See “Obtain QoS measurement tools” on page 197 for information about where to obtain other more specialized delay and route monitoring tools.

At the end of the month, analyze each site’s QoS information. Table 36 provides a sample.

Table 36
QoS monitoring

	One-way delay Mean+σ (ms)		Packet loss Mean+σ (%)		QoS		
Site pair	**Last period**	**Current period**	**Last period**	**Current period**	**Last period**	**Current period**	**Objective**
Santa Clara/ Richardson	135	166	1	2	Excellent	Good	Excellent
Santa Clara/ Ottawa	210	155	3	1	Good	Excellent	Excellent

Declines in QoS can be observed through the comparison of QoS between the last period and current period. If a route does not meet the QoS objective, take immediate action to improve the route’s performance.

SNMP network management

Simple Network Management Protocol (SNMP)-based Network Management Systems (NMS) provide a useful way of monitoring a real-time network from end to end. This is important for networks using VoIP. User complaints of slow downloads are no longer enough to diagnose problems. An NMS can ensure that problems on a network running real-time traffic are solved quickly to maintain high-quality service.

SNMP NMS software can be configured to perform the following actions:

- map the network

- monitor network operation through polling of network devices
- centralized alarm management through SNMP traps
- notify network administrators of problems

IP Trunk 3.01 (and later) can be integrated into an NMS to provide an complete view of the converged voice and data network. Problems can be isolated much more quickly when looking at the entire network. An IP trunk card can send alarms through SNMP traps to the NMS. Basic card information can be queried from an IP trunk card. The format of the IP Trunk 3.01 (and later) SNMP traps and structure of management information is provided within the IP Trunk 3.01 (and later) Management Information Base (MIB). To obtain the IP Trunk 3.01 (and later) MIB, contact the Nortel representative.

SNMP Agent support is provided in OTM 2.1 (and later). This integrates OTM with existing NMS software, which allows alarms collected from an IP Trunk 3.01 (and later) node and the system to be forwarded to the NMS from a single point of contact with the PBX.

Nortel also provides a complete line of Enterprise Network management software with Optivity Enterprise Network Management Solutions product line.

IP Trunk 3.01 (and later) network inventory and configuration

Record the current IP Trunk 3.01 (and later) design and log all adds, moves and changes to the IP Trunk 3.01 (and later) network that occur. The following data must be kept:

- ITG site information
  - — location
  - — dialing plan
  - — IP addressing
- Provisioning of IP Trunk 3.01 (and later) nodes
  - — number of cards and ports, IP Trunk 3.01 (and later) node and card parameters

- — fallback threshold level
- — Codec image
- — voice and fax payload
- — voice and fax playout delay
- — audio gain, echo cancellor tail delay size, Silence Suppression threshold
- — software version

User feedback

Qualitative feedback from users helps confirm if the theoretical QoS settings match what end users perceive. The feedback can come from a Helpdesk facility and must include information such as time of day, origination and destination points, and a description of service degradation.

The fallback threshold algorithm requires a fixed IP Trunk 3.01 (and later) system delay of 93 ms, which is based on default IP Trunk 3.01 (and later) settings and its delay monitoring probe packets. The fallback mechanism does not adjust when IP Trunk 3.01 (and later) parameters are modified from their default values. Users can perceive a lower quality of service than the QoS levels at the fallback thresholds in the following situations:

- Delay variation in the intranet is significant. If the standard deviation of one-way delay is comparable with the voice playout maximum delay, it means that there is a population of packets that arrive too late to be used by the IP Trunk 3.01 (and later) node in the playout process.
- The jitter buffer is increased. In this case, the actual one-way delay is greater than that estimated by the delay probe.
- The codec is G.711A or G.711U. The voice packets formed by these codecs are larger (120 to 280 bytes) than the delay probe packets (60 bytes). This means there is greater delay experienced per hop. If there are low bandwidth links in the path, then the one-way delay is noticeably higher both in terms of average and variation.

OTM 2.1 (and later) management and configuration of IP Trunk 3.01 (and later)

Contents

This section contains information on the following topics:

Introduction

The OTM 2.1 (and later) PC application is designed to support both ITG 2.x (ITG Trunk 2.0 and ITG Trunk 2.1) and IP Trunk 3.01 (and later). The OTM 2.1 (and later) application name is **ITG ISDN IP Trunks**.

OTM 2.1 (and later) ITG Engineering rules

OTM 2.1 (and later) can manage multiple nodes with multiple IP trunk cards. The maximum number of IP trunk cards that can be configured by OTM 2.1 (and later) is dependant on the following:

1. All OTM 2.1 (and later) ITG data is stored in a single database file. The entire database is read into PC memory when the program is launched. If a large IP Trunk 3.01 (and later) network is to be managed from a single OTM 2.1 (and later) server, then each OTM 2.1 (and later) PC client should have more than the minimum RAM requirement of 64 Mb. The recommended RAM is 128 Mb or more. If the data is stored on an OTM 2.1 (and later) server, the application launch time increases as the size of the IP Trunk 3.01 (and later) network grows (this also depends on the network speed). For the OTM 2.1 (and later) server, the minimum RAM required is 128 Mb; 256 or more Mb is recommended.
2. In theory, a single OTM 2.1 (and later) installation can support up to 500 system's. However, OTM 2.1 (and later) applications requiring real-time, such as Traffic Analysis retrieval of traffic data, are limited to a much smaller number of systems.
3. OTM 2.1 (and later) Alarm Notification can receive a maximum of 20 SNMP traps per second (based on the recommended PC configuration). In large networks, Nortel recommends that multiple OTM 2.1 (and later) PCs be used to collect traps from the IP trunk cards, each PC supporting one or more IP Trunk 3.01 (and later) nodes. Alarm notification scripts can be used to forward critical alarms to a central OTM 2.1 (and later) PC or Network Management application.

OTM 2.1 (and later) network setup guidelines

Install OTM 2.1 (and later) in a standalone mode or in a network environment. For IP Trunk 3.01 (and later) nodes, install OTM 2.1 (and later) in a network environment to manage multiple IP Trunk 3.01 (and later) nodes, provide multi-user access, and maintain IP Trunk 3.01 (and later) configuration data consistency.

In the network environment, OTM 2.1 (and later) stores databases on a file server. Do not use the server to access OTM 2.1 (and later) as a client PC.

OTM 2.1 (and later) with Windows 98, Windows NT 4.0, and Windows 2000 clients are supported on the following platforms:

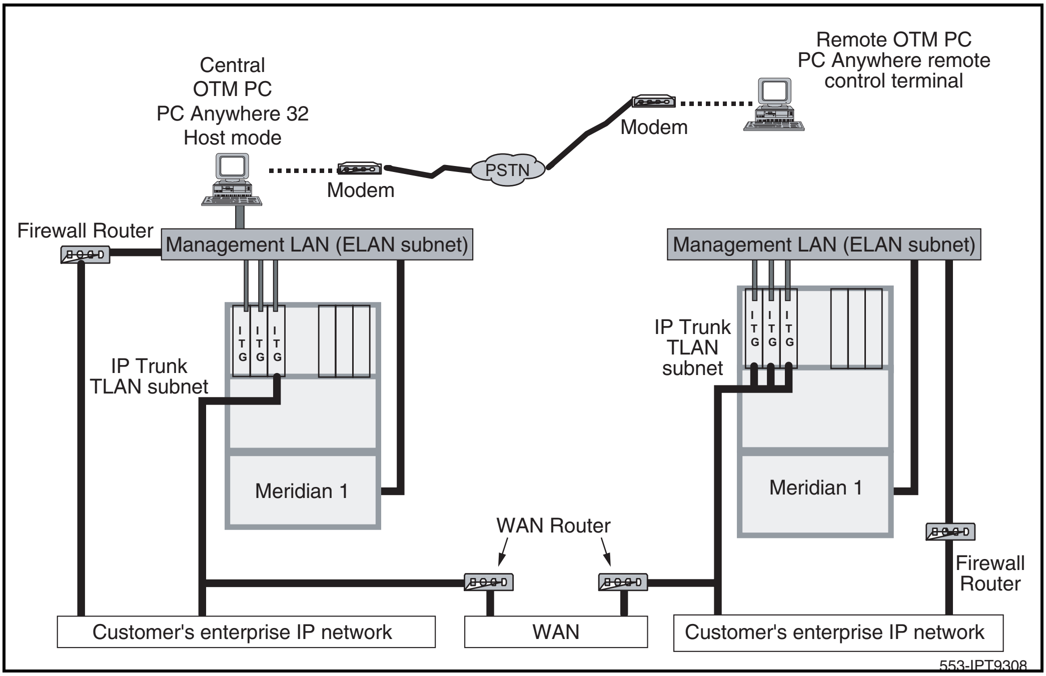
- Windows 2000
- Windows NT 4.0
- OTM 2.1 (and later) 1.0 client requires an OTM 2.1 (and later) server

OTM 2.1 (and later) remote access configuration

Support for remote access can be covered in two scenarios that vary according to the support organizations access to the customer's data network LAN or WAN.

In the first scenario, the support organization has full access to the customer LAN/WAN. See Figure 32.

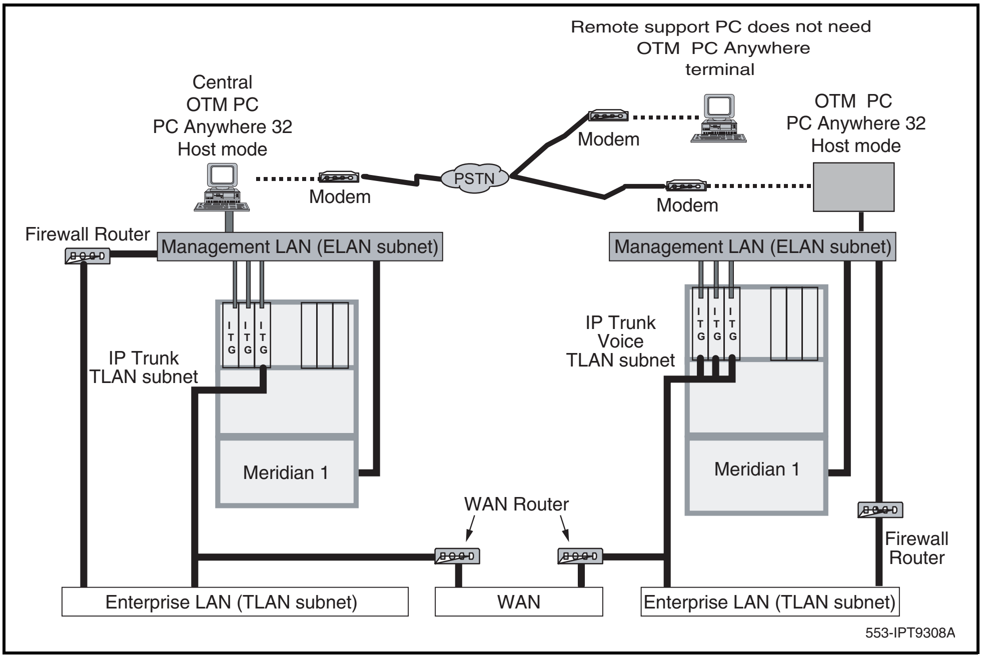
Figure 32
Remote access with full access to the customer's LAN/WAN


Central OTM PC PC Anywhere 32 Host mode
Modem
PSTN
Modem
Remote OTM PC PC Anywhere remote control terminal
Firewall Router
Management LAN (ELAN subnet)
Management LAN (ELAN subnet)
I T G
I T G
I T G
IP Trunk TLAN subnet
IP Trunk TLAN subnet
I T G
I T G
I T G
Meridian 1
Meridian 1
WAN Router
Firewall Router
Customer's enterprise IP network
WAN
Customer's enterprise IP network
553-IPT9308

A single remote support and administration OTM 2.1 (and later) PC can administer a local node through the ITG Management LAN or can administer a remote node through the WAN. The remote access capabilities are provided through a modem router that has access to any of the ITG Management LANs. The Remote OTM 2.1 (and later) PC connects to the ITG Management over a PPP link and then communicates to the IP trunk cards in the same manner as a local OTM 2.1 (and later) PC on the IP Trunk 3.01 (and later) Management LAN. The IP address provided by the modem router (for example, Nortel Netgear RM356 Modem Router) to the remote OTM 2.1 (and later) PC is configured in the modem router and in the SNMP Manager's list of the IP trunk cards. All management communications including alarms are sent over this channel.

In the second scenario, the support organization is denied access to the customer LAN/WAN network for security reasons. See Figure 33.

Figure 33
Remote access with no access to the customer's LAN/WAN



In this case, a local OTM 2.1 (and later) PC on an IP Trunk 3.01 (and later) ELAN subnet has access to only the IP trunk cards on the local node. A private IP address can be used for the OTM 2.1 (and later) PC since management and alarm traffic would only travel over the private IP Trunk 3.01 (and later) ELAN subnet. A modem can be used to connect the remote OTM 2.1 (and later) PC to the local OTM 2.1 (and later) PC with remote access software such as *PC Anywhere*™ running in client-server mode between the local and remote PCs. The local OTM 2.1 (and later) PC communicates with the IP trunk cards for management and alarm information and conveys all information back to the remote OTM 2.1 (and later) PC. There are alternative solutions for remote alarm management available to the customer through third party products. Refer to product bulletins for availability.

OTM 2.1 (and later) PC description

The OTM 2.1 (and later) PC can be attached to a LAN to provide multi-user, multi-site access. The OTM 2.1 (and later) applications and database must reside on a LAN Server with each client accessing the files from the server.

> ***Note:*** The server used for OTM 2.1 (and later) is used as a file server only and must not be used to access OTM 2.1 (and later) as a client PC.

A single network drive location is chosen during the OTM 2.1 (and later) client PC installation process. For multi-system configurations where large data store requirements exceed the capacity of a single drive, or where data integrity is highly valued, a Redundant Array of Inexpensive Disks (RAID) storage solution is recommended. Tape or other backup methods are highly recommended.

When installing OTM 2.1 (and later) client applications, it is important for the network drive to be mapped the same from each PC if an OTM 2.1 (and later) user is expected to be able to login to the network with their network login ID at any OTM 2.1 (and later) client PC.

A PC security device is required for every PC running OTM 2.1 (and later). A security device is not required for the PC server as it is only used to store OTM 2.1 (and later) data and does not actually run any OTM 2.1 (and later) applications.

Each of the OTM 2.1 (and later) client PCs on the customer LAN is allowed connectivity to the IP addresses of the Meridian 1s. Nortel recommends the following:

1. OTM 2.1 (and later) client PC in switchroom has access to the File Server on the customer network.
2. Block broadcast messages from the customer LAN to the system private LAN.
3. Block access to the system private LAN from non-OTM 2.1 (and later) client PCs for security reasons.

OTM 2.1 (and later) PC hardware and software requirements

The following list provides the recommended minimum PC hardware and software recommended to run OTM 2.1 (and later). Other applications launched while using OTM 2.1 (and later) can require increased RAM. The minimum requirements are as follows:

- an Intel Pentium II Processor 400 MHz CPU minimum; Intel Pentium III Processor 600 MHz CPU recommended
- 2 GB or larger hard disk drive with 1000 MB or more free space. Refer to the system datastore column in the hard drive requirements in Table 37 on page 237.
- 256 MB of RAM (minimum); 512 MB recommended
- SVGA color monitor and interface card (800x600 resolution for graphics)
- CD-ROM drive and 3.5 in 1.44 MB floppy disk drive
- two Ethernet Network Interface Cards
- Hayes-compatible modem is optional to connect to remote systems, required for polling configurations (56 Kbps recommended)
- PC COM port with 16550 UART
- printer port (required for the dongle)

- dongle (for server or stand-alone only)
- Windows-compatible mouse (PS/2 mouse preferred to free up a PC serial port)

> **CAUTION — Service Interruption**
>
> Do not install OTM 2.1 (and later) on a Windows NT or Windows 2000 system that is configured as a Primary Domain Controller (PDC).

For detailed information on the software requirements and the supported platforms for OTM 2.1 (and later), refer to *Optivity Telephony Manager: Installation and Configuration* (553-3001-230).

Hard drive requirements

For a single OTM 2.1 (and later) PC configuration, refer to Table 37 to determine the hard drive space required on the OTM 2.1 (and later) PC. Consider both program and data store requirements.

For OTM 2.1 (and later) client configurations (two or more OTM 2.1 (and later) PCs sharing the same database), the common data is stored on a server PC that does not run OTM 2.1 (and later). Estimate the size of the required disk space on this server using the Data Store column in Table 37.

Table 37
Hard drive capacity for OTM 2.1 (and later) applications (Part 1 of 2)

OTM 2.1 (and later) application	**Program store**	**Data store**
Common Services (required)	38 MB	Negligible
ITG	1.5 MB	1.0 MB plus 0.5 MB per 1k IP trunk cards

Table 37
Hard drive capacity for OTM 2.1 (and later) applications (Part 2 of 2)

OTM 2.1 (and later) application	Program store	Data store
Traffic Analysis	5 MB	System dependent: Typically 2.5 to 9 MB per month for each systems traffic data.
ESN	1 MB	System dependent: Allow 1 MB per customer.
Maintenance Windows	1 MB	Negligible
Alarm Management with Alarm Notification	1.5 MB	Negligible

Install and configure IP Trunk 3.01 (and later) node

Contents

This section contains information on the following topics:

Introduction

This chapter describes how to add a new IP Trunk 3.01 (and later) trunk node in OTM, how to install the IP trunk cards and cables, and how to configure and transmit the node properties.

Before you begin

Follow the steps in Procedure 6 to ensure that installation requirements are met.

Procedure 6
Meeting installation requirements

1 Install OTM 2.1 (and later). Make sure the ITG ISDN IP Trunk and Alarm Management applications are installed.

2 Upgrade the system software to CS 1000 Release 4.0.

IP Trunk 3.01 (and later) requires package 145 (ISDN) and package 147 (ISL). Install additional software packages, such as package 148 NTWK, as required, for advanced ISDN features.

3 Verify that required LAN and WAN networking equipment and cables are installed. For networking equipment requirements, refer to “ITG engineering guidelines” on page 125. The IP trunk card requires shielded cables.

4 Ensure the Media Card 32-port trunk card or ITG-Pentium 24-port trunk card, DCHIP PC Card (NTWE07), and cable assemblies required for the site are available.

5 For Large Systems, have the ITG ISL (NT6D80). For Small Systems, IP Trunk 3.01 (and later) requires at least one available port on an SDI/DCH card (minimum vintage NTAK02BB). Ensure D-channel cards have required cables.

6 Verify that the customer site has a Nortel Netgear RM356 Modem Router (or equivalent) on the ELAN subnet. The modem router provides remote support access to IP Trunk 3.01 (and later) and other IP-enabled Nortel products on the system site. See Appendix F on page 605 for more information on routers.

End of Procedure

Installation procedure summary

Table 38 lists the procedures required to install and configure an IP Trunk 3.01 (and later) node. Complete all installation and configuration tasks before transmitting the configuration data to the IP trunk cards.

Table 38
Installation procedures (Part 1 of 3)

Step	Procedure	See page
1	**Create the IP Trunk 3.01 (and later) Installation Summary Sheet.**	246
2	**Install and cable IP Trunk 3.01 (and later) cards.** Card installation procedure	257 257
3	**Configure IP Trunk 3.01 (and later) data.** Configure the ISL D-channel on the system for the DCHIP card for IP Trunk 3.01 (and later). Configure ISDN feature in Customer Data Block. Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units for IP Trunk Route. Configure dialing plans within the corporate network. Disable the Media Card 32-port and ITG-Pentium 24-port trunk cards.	290 290 296 302 307 315

Table 38
Installation procedures (Part 2 of 3)

Step	Procedure	See page
4	**Configure IP Trunk 3.01 (and later) data in OTM 2.1 (and later).** Add an IP Trunk 3.01 (and later) node in OTM 2.1 (and later) manually. Add an IP Trunk 3.01 (and later) node and configure general node properties. Single vs. separate TLAN and ELAN subnets. Configure card properties. Configure DSP profiles for the IP Trunk 3.01 (and later) node. Configure SNMP Traps/Routing and IP addresses tab. Configure Accounting server. Control node access with SNMP community name strings. Exit node property configuration session. Create the IP Trunk 3.01 (and later) node dialing plan using OTM. Retrieve the IP Trunk 3.01 (and later) node dialing plan using OTM.	316 316 317 320 322 326 331 335 337 339 339 344
5	**Transmit IP trunk card configuration data from OTM 2.1 (and later) to the IP trunk cards.** Configure the Leader 0 IP address. Transmit the node properties, card properties and dialing plan to Leader 0. Verify installation and configuration. Transmit card properties and dialing plan to Leader 1 and Follower cards.	347 348 353 354 356
6	**Configure date and time for the IP Trunk 3.01 (and later) node.**	358
7	**Change the default ITG shell password to maintain access security.**	358

Table 38
Installation procedures (Part 3 of 3)

Step	Procedure	See page
8	**Check and download IP trunk card software in OTM 2.1 (and later).** Transmit new software to the IP trunk cards. Upgrade the DCHIP PC Card.	361 363 366
9	**Configure OTM Alarm Management to receive SNMP traps from the IP trunk cards.**	367
10	**Make test calls to the remote nodes (ITG Trunk or IP Trunk).**	371

ESN installation summary

The following is a summary of the actions required to implement ESN:

- In LD 86, provision the ESN block.
  - — Enter the maximum numbers of each type of ESN entity.
  - — Indicate whether CDP is enabled or disabled.
  - — Enter the ESN access codes.
- In LD 86, provision any DGT (Digit manipulation tables) required.
- In LD 86, provision the RLB (Route List Block) RLI (Route List Index) blocks.
  - — Add the RLI entries. Do not skip entries, as ESN searches the table from entry zero until the full initial set of entries are scanned to find an available route.
  - — Enter the RDB for the entry.
  - — Enter the DMI (Digit Manipulation Index), if required.
  - — After the last entry is entered, enter the number of entries in the Initial Set (ISET).
- In LD 87, provision the NCTL (Network Control) block.

- In LD 87, provision the CDP (Coordinated Dialing Plan) entries, as required – LSC, DSC, and TSC. Enter the RLI intended for this code.
- In LD 90, provision the NPA, NXX, LOC, SPN, or other entries as required. Enter the RLI intended for this code.

Create the IP Trunk 3.01 (and later) Installation Summary Sheet

Compile all necessary data before beginning the configuration process. For example, prepare the following information ahead of time:

- The TN, ELAN network interface MAC address, and card density should be recorded during the Media Card 32-port trunk card and ITG-Pentium 24-port installation.
- D-Channel number and CHID should be recorded during the system configuration.
- All ELAN and TLAN network interface IP addresses must be obtained from the system administrator before beginning OTM configuration.

Create an Installation Summary Sheet. This form contains important information about each card, including the fields listed in Table 39 on page 247.

Table 39
IP Trunk 3.01 (and later) Installation Summary Sheet

Site__________________ System__________________ Customer_________ Node Number_________
TLAN Node IP address____
TLAN gateway (router)________________TLAN subnet mask__________________
ELAN gateway (router)________________ELAN subnet mask__________________

TN	ELAN network interface MAC address	ELAN network interface IP address	TLAN network interface IP address	Card role	DCHIP on card	D-Channel	First CHID	Card density
				Leader 0				
				Leader 1				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				
				Follower				

Site__________________ System__________________ Customer_________ Node Number_________
TLAN Node IP address____
TLAN gateway (router)________________TLAN subnet mask__________________
ELAN gateway (router)________________ELAN subnet mask__________________

TN	ELAN network interface MAC address	ELAN network interface IP address	TLAN network interface IP address	Card role	DCHIP on card	D-Channel	First CHID	Card density

Channel Identifier planning

The Channel ID must be in sequential order on a card (no gaps in the numbering like 1, 2, 4, 7) and they must increase in number. If this is not done, the card channels are unusable.

Gaps in numbering can deliberately be left between IP trunk cards to allow for later expansion; for example, to allow for later expansion of a ITG-Pentium 24-Port trunk card to a Media Card 32-port trunk card.

Preferred ISL channel numbering

This section gives several examples of ISL Channel ID numbering.

Single card, sequential numbering, no gaps – ITG-Pentium 24-port trunk card

This is an example using an ITG-Pentium 24-port trunk card. The first channel number can be any value, as long as the maximum is less than or equal to the maximum value of the ISL channel number, which is 382.

Table 40 maps the unit number to the ISL channel number for a single ITG-Pentium 24-port trunk card.

Table 40
Mapping of unit number to ISL Channel number – one card in system (Part 1 of 2)

Unit number (from TN)	ISL Channel number
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
10	11
11	12
12	13
13	14
14	15
15	16
16	17
17	18
18	19
19	20

Table 40
Mapping of unit number to ISL Channel number – one card in system (Part 2 of 2)

Unit number (from TN)	ISL Channel number
20	21
21	22
22	23
23	24

Single card, sequential numbering, no gaps – Media Card 32-port trunk card

This is an example using a Media Card 32-port trunk card. The first channel number can be any value, as long as the maximum is less than or equal to the maximum value of the ISL channel – 382. Table 41 maps the unit number to the ISL channel number for a single Media Card 32-port trunk card.

Table 41
Mapping of unit number to ISL Channel number – one card in system (Part 1 of 3)

Unit number (from TN)	ISL Channel number
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9

Table 41
Mapping of unit number to ISL Channel number – one card in system (Part 2 of 3)

Unit number (from TN)	ISL Channel number
9	10
10	11
11	12
12	13
13	14
14	15
15	16
16	17
17	18
18	19
19	20
20	21
21	22
22	23
23	24
24	25
25	26
26	27
27	28
28	29
29	30

Table 41
Mapping of unit number to ISL Channel number – one card in system (Part 3 of 3)

Unit number (from TN)	ISL Channel number
30	31
31	32

Two cards, sequential numbering, gap left for expansion

This example is for two ITG-Pentium 24-port trunk cards. To allow room for replacement by a Media Card 32-port trunk card at a later date, a gap of eight channels has been left between the cards.

Table 42 maps the unit number to the ISL channel number for a two ITG-Pentium 24-port trunk cards with an eight channel gap between cards. Nortel recommends this configuration as it makes it easy to replace an ITG-Pentium 24-port trunk card with a Media Card 32-port trunk card, without affecting the other card.

If no gap is left in the numbering sequence between the cards, conversion to a Media Card 32-port trunk becomes difficult. The ISL channel numbers on the first card have no room to expand, making it necessary to fully re-provision the second IP trunk card.

Table 42
Mapping of unit number to ISL Channel number – two cards in system and expansion gap (Part 1 of 4)

Unit number (from TN)	ISL Channel number
Card 1	
0	1
1	2
2	3
3	4
4	5

Table 42
Mapping of unit number to ISL Channel number – two cards in system and expansion gap (Part 2 of 4)

Unit number (from TN)	ISL Channel number
5	6
6	7
7	8
8	9
9	10
10	11
11	12
12	13
13	14
14	15
15	16
16	17
17	18
18	19
19	20
20	21
21	22
22	23
23	24
Card 2	
Card 2 ISL channel numbering starts at 33 (24 numbers from Card 1 + 8 numbers for expansion + first number for Card 2 = 24 + 8+ 1 = 33).	

Table 42
Mapping of unit number to ISL Channel number – two cards in system and expansion gap (Part 3 of 4)

Unit number (from TN)	ISL Channel number
0	33
1	34
2	35
3	36
4	37
5	38
6	39
7	40
8	41
9	42
10	43
11	44
12	45
13	46
14	47
15	48
16	49
17	50
18	51
19	52
20	53
21	54

Table 42
Mapping of unit number to ISL Channel number – two cards in system and expansion gap (Part 4 of 4)

Unit number (from TN)	ISL Channel number
22	55
23	56

Incorrect ISL channel numbering plans

This section describes numbering plan errors.

Gaps in ISL channel numbering sequence

Table 43 shows gaps in the ISL numbering plan sequence. A gap between channel numbers causes the IP trunk card to be unable to associate the ISL channel number with the B channel number. Therefore, only units 0 to 4 (loop shelf card 0 to loop shelf card 4) can be used.

Table 43
Channel numbering error – gap on one card

Unit number (from TN)	ISL Channel number
0	1
1	2
2	3
3	4
4	5
5	11
6	12

Decreasing channel numbering sequence

Table 44 on page 256 shows an example of a decreasing ISL channel numbering plan. Using decreasing ISL channel identifiers causes the IP trunk card to be unable to associate the ISL channel number with the B channel number. In this example, only unit 0 (loop shelf card 0) can be used.

Table 44
Channel numbering error – decreasing channel number sequence

Unit number (from TN)	ISL Channel number
0	24
1	23
2	22
3	21
4	20
5	19
6	18
7	17

Overlapping channel numbers

Do not provision the ISL channel numbers on both cards with the same channel numbers. For example, do not configure Channel 10 on both cards. The Meridian 1/CS 1000M rejects this numbering plan but the IP trunk card does not. Therefore, it is possible to implement the incorrect card numbering, making all channels above the first overlapping number unusable.

Install and cable IP Trunk 3.01 (and later) cards

Card installation procedure

> **CAUTION WITH ESDS DEVICES**
>
> Use ESD precautions when unpacking the hardware and unpacking the cards.

Place each IP trunk card in the Meridian 1 or CS 1000 system and record the TN, ELAN MAC address, and card density on the IP Trunk 3.01 (and later) Installation Summary Sheet. The ELAN MAC address is labeled on the IP trunk card faceplate as the motherboard Ethernet address.

Each ITG-Pentium 24-port trunk card requires two slots in a IPE shelf. Only the left slot of the card requires connection to the system IPE backplane and I/O panel. Each Media Card 32-port trunk card requires only one slot in the system IPE shelf.

At least one DCHIP card must be installed in an IP Trunk 3.01 (and later) node. The D-Channel (DCH) PC Card and the associated NTCW84EA DCHIP PC Card Pigtail cable must be installed on to the DCHIP card.

Install a maximum of eight IP trunk cards in an IPE shelf. The ITG-Pentium 24-port trunk card can occupy any two adjacent slots in an IPE shelf, with the left slot of the card plugging into slots 0 to 6 and 8 to 15. The left slot of an IP trunk card cannot be plugged in slot 7, because the XPEC card is situated in-between slots 7 and 8.

To allow a module to hold the maximum number of IP trunk cards, install each ITG-Pentium 24-port trunk card with the left slot of the card inserted in an even-numbered slot.

If the maximum card density for each module is not required, the left slot of the IP trunk card can be inserted in an odd-numbered slot.

The required software version on the ITG-P card is version 5.7.

Note 1: The ITG-Pentium 24-port trunk card requires 24-pair tip and ring I/O cabling. NT8D37AA IPE modules have 24-pair tip and ring I/O cabling for card slots 0, 4, 8, and 12 only. Insert the left slot of the IP trunk card in NT8D37AA slots 0, 4, 8 or 12 only. NT8D37BA or later IPE modules have no such restriction.

Note 2: When multiple IP trunk cards are installed, distribute them between available IPE shelves. This prevents total loss of IP trunking, in the case of localized shelf failure.

CAUTION WITH ESDS DEVICES

Wear an electrostatic discharge strap when handling IP trunk cards. As an additional safety measure, handle all cards only by the edges and, when possible, with the loosened packaging material still around the component.

CAUTION — Equipment Damage

Never install an IP trunk card in an IPE shelf that has been wired for a Central Office Trunk (COT) card. Before inserting the card into the slot, disconnect the cable connecting this card to the Main Distribution Frame (MDF). COT cards can receive ringing voltage, which, when applied to an IP trunk card, can damage the card.

CAUTION — Equipment Damage

Do not overtighten screws. They can break.

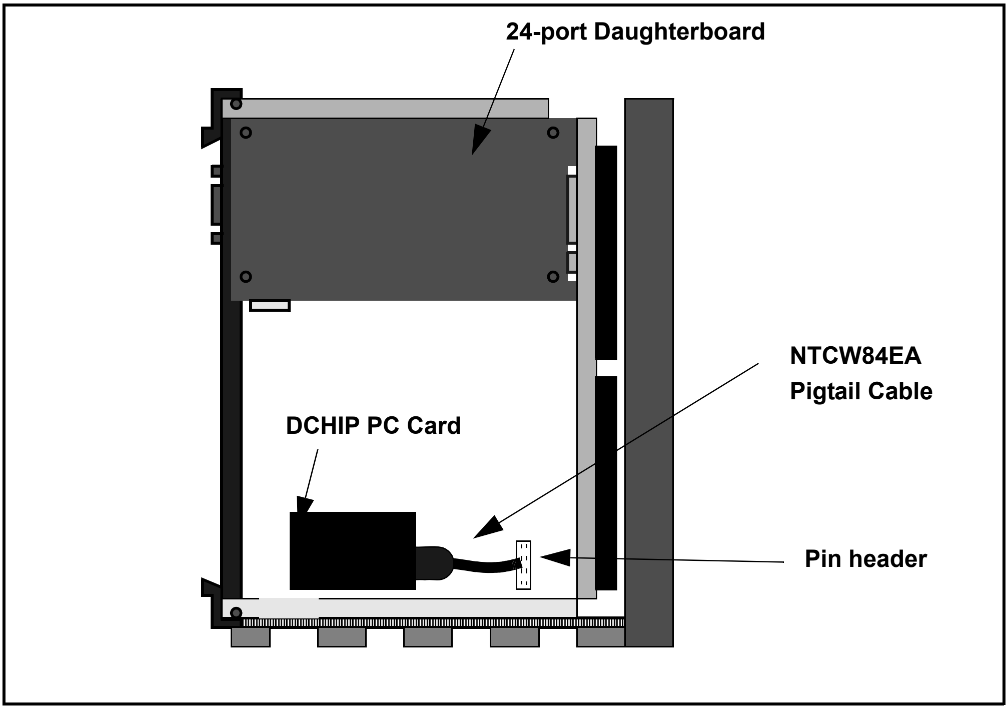
Follow the steps in Procedure 7 on page 259 to install and cable the ITG-Pentium 24-port trunk card.

Procedure 7
Installing and cabling the ITG-Pentium 24-port trunk card

1. Identify the IPE card slots selected for the IP trunk card(s). Use the recorded information from the IP Trunk 3.01 (and later) Installation Summary Sheet (Table 39 on page 247).
2. Remove any existing I/O panel cables associated with any card previously installed in the selected card slot.
3. Install the NTWE07AA DCHIP PC Card into the internal PC Card slot on the IP trunk card that has been selected to provide the DCHIP function. (See Figure 34 on page 260.)
4. Connect the NTCW84EA pigtail cable from port 0 of the DCHIP PC Card to the J14 pin header on the motherboard of the DCHIP card. See Figure 34 on page 260.

   The cable routes the D-Channel signals to the backplane and the I/O panel. The PC Card connector is keyed to allow insertion only in the correct direction. The J-14 pin header connector is not keyed. Be careful to align the connector with the pin header.

Figure 34
DCHIP PC Card and NTCW84EA pigtail cable



5 Pull the top and bottom locking devices away from the IP trunk card faceplate. Insert the IP trunk card into the card slots and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

Note: When the IP trunk cards are installed, the red LED on the faceplate is lit if: the card has rebooted; the card is active, but there are no trunks configured on it; or the card is active and has trunks, but the trunks are disabled. If the LED does not follow the pattern described (such as remaining continuously flashing or weakly lit), replace the card.

Note 1: Observe the IP trunk card Faceplate Maintenance display to see startup self-test results and status messages. A display of the type “F:xx” indicates a failure. Some failures indicate that the card must be replaced. “F:10” temporarily appears on the display, which indicates a Security Device test failure. Since IP Trunk 3.01 (and later) does not use Security Devices, ignore this error.

Refer to “Media Card 32-port trunk card faceplate maintenance display codes” on page 560 and “ITG-Pentium 24-port trunk card faceplate maintenance display codes” on page 563 for a complete listing of the codes.

End of Procedure

Install NTCW84JA Large System I/O Panel 50-Pin filter adapter

For Large Systems, the standard filtering is provided by the 50-Pin filter adapters mounted in the I/O Panel on the back of the IPE shelf. The filter adapter connects externally to the MDF cables and internally to the NT8D81AA Backplane to I/O Panel ribbon cable assembly. Within the adapter, all Tip and Ring pairs, including the TLAN subnet pairs, are filtered. For 100BaseT operation, the standard adapter must be replaced with the NTCW84JA adapter which is identical to the existing adapter but has unfiltered TLAN Tip and Ring pairs.

For Cabinet systems, the standard I/O filter connector already supports 100BaseTX.

CAUTION

For Large Systems manufactured during 1998-1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon cable assembly with a non-removable Filter Connector. The NT8D81BA is compatible with a 10BaseT TLAN subnet, but if a 100BaseT TLAN subnet is required, order the NT8D81AA Backplane to I/O Panel ribbon cable assembly to replace it. Do not try to install the NTCW84JA Filter Connector onto the existing non-removable Filter Connector.

Note: The NTCW84JA filter connector is required for separate subnets using 100BaseTX for the TLAN subnet connection.

Remove existing I/O panel filter adapter

The standard I/O filter adapter is shielded metal with a black plastic insert connector. The NTCW84JA adapter uses yellow warning labels to indicate EMC filtering modifications and which MDF connection points can support 100BaseT connection.

Follow the steps in Procedure 8 to remove the existing I/O panel filter adapter.

Procedure 8
Removing the existing I/O panel filter adapter

1. Remove the ITG pack, or any other IPE pack, from the IPE shelf card slot corresponding to the I/O Panel connector to be removed.

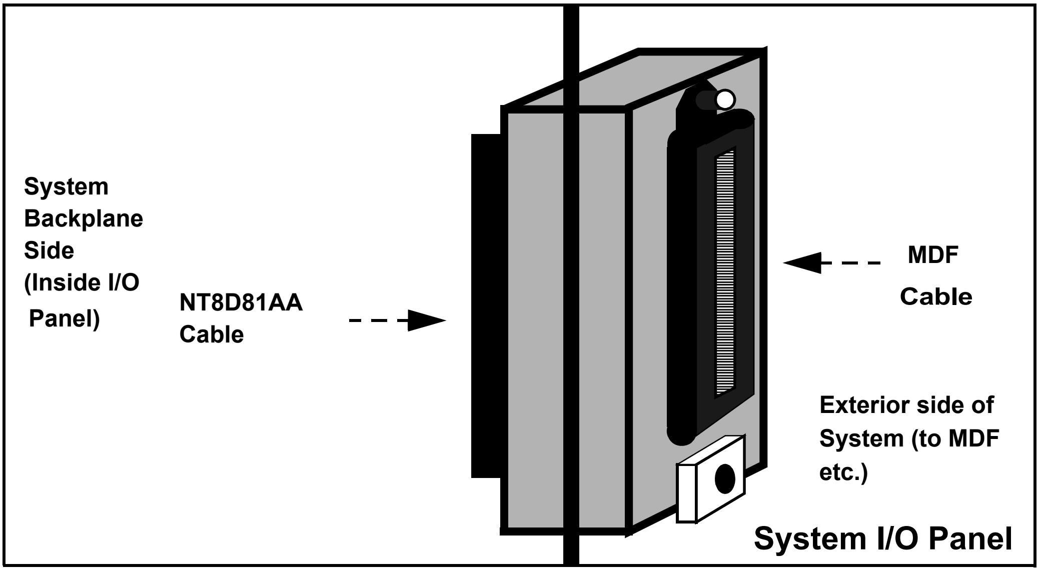
   Note: Make sure to use the I/O panel connector which corresponds to the left slot number of the DCHIP card.

2. Remove the NT8D81AA Backplane to I/O Panel ribbon cable assembly which is connected to the backplane side of the existing block by releasing the latching pins on the filter block and pulling the NT8D81AA cable away.

3. Unscrew the existing filter adapter from the I/O panel. There is one screw on the lower front of the adapter and one screw on the upper back of the adapter. Remove the adapter.
4. Re-position the new NTCW84JA filter adapter in the now vacant I/O panel opening. (See Figure 35 on page 263.)
5. Attach the new NTCW84JA to the I/O panel by securely fastening the top back screw and the bottom front screw.
6. Reconnect the NT8D81AA cable and secure it in place by snapping shut the locking latches provided on the NTCW84JA connector.

End of Procedure

Figure 35
NTCW84JA 50 pin I/O Panel Filter Connector Block


System Backplane Side (Inside I/O Panel)
NT8D81AA Cable
MDF Cable
Exterior side of System (to MDF etc.)
System I/O Panel

Note: Even though the ITG-Pentium 24-port trunk card is a two-slot card, only the leftmost slot is counted for the card slot number. Example: for an ITG-Pentium 24-port trunk card installed in slots 2 and 3, the slot number is 2.

For more detailed cabling information and procedures for replacing the NT8D81BA with the NT8D81AA, see “Patches and advisements” on page 571.

Install NTMF94EA and NTCW84KA cables

The Media Card 32-port and ITG-Pentium 24-port trunk card supports a one-cable solution for access to the TLAN network interface, ELAN network interface, and serial ports. The ELAN network interface supports 10BaseT operation and the TLAN network interface supports 10/100BaseT operation. If using a 100BaseT operation on the TLAN network interface, install a NTCW84JA 50-pin I/O panel filter connector block to replace the standard I/O connectors provided.

Cables that are provided for the ELAN and TLAN network interface functions include the following:

- the NTMF94EA ELAN, TLAN, and RS-232-port cable (for non-DCHIP cards)
- the NTCW84KA ELAN, TLAN, RS-232 and DCH Ports cable (for DCHIP cards)

Install the NTCW84KA cable (for DCHIP cards)

Follow the steps in Procedure 9 to connect the NTCW84KA cable for DCHIP cards.

Procedure 9
Installing the NTCW84KA cable

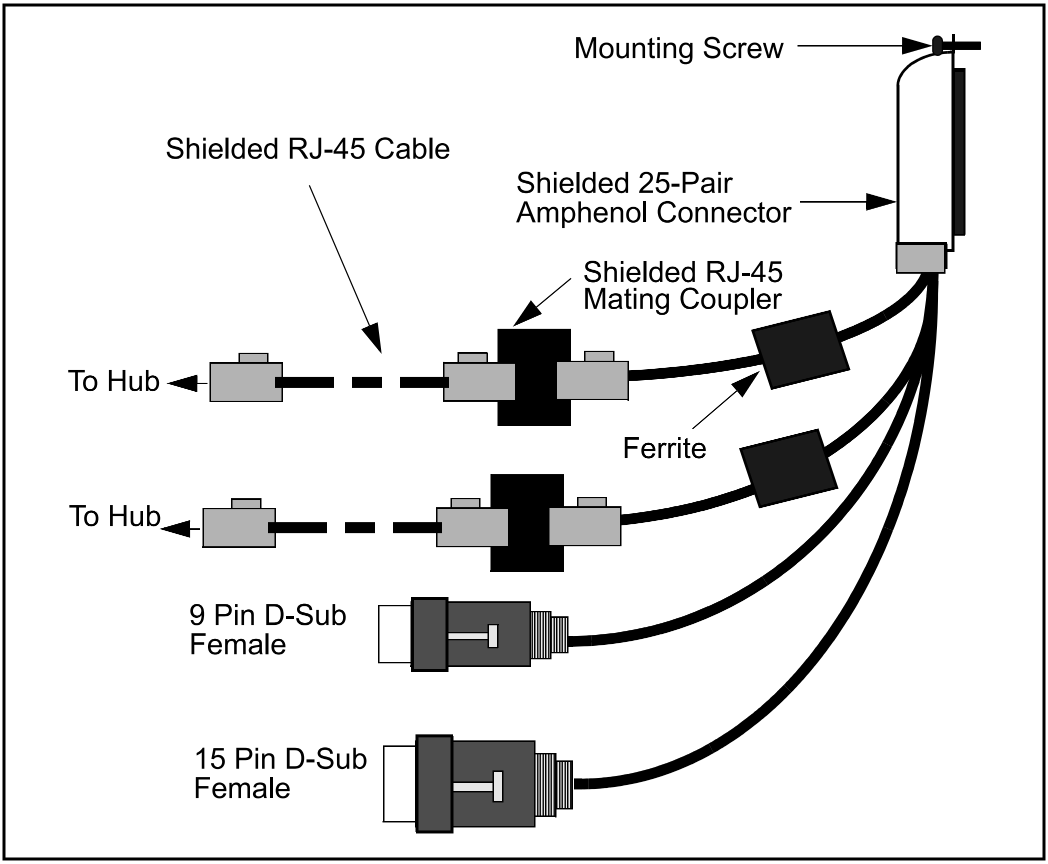
1 Connect the NTCW84KA cable see to the I/O panel connector (see Figure 36 on page 265).

Note: Make sure to connect to the I/O panel connector that corresponds to the left slot number of the DCHIP card.

2 Secure the mounting screw provided on the top of the Shielded 25-Pair Amphenol Connector to the I/O Panel filter connector in order to tie the shield of the LAN cable to the frame ground for EMC compliance.

End of Procedure

Figure 36
NTCW84KA ELAN, TLAN, DCH, and serial cable



Install the NTMF94EA cable (for non-DCHIP cards)

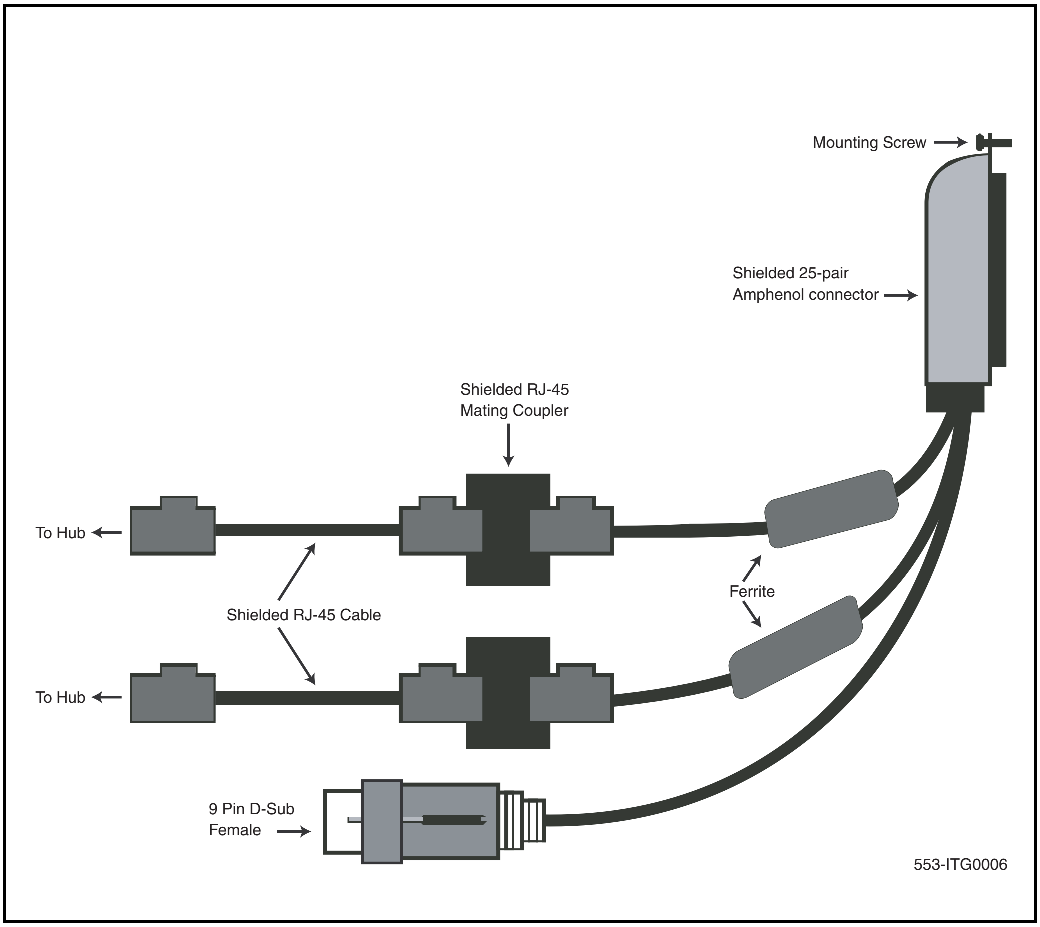
Follow the steps in Procedure 10 to install the NTMF94EA cable for non-DCHIP cards.

Procedure 10
Installing the NTMF94EA cable

1 Connect the NTMF94EA cable (see Figure 37 on page 267) to the I/O panel connector. Make sure to connect to the I/O panel connector which corresponds to the left slot number of the DCHIP card.

2 Secure the mounting screw provided on the top of the Shielded 25-Pair Amphenol Connector to the I/O Panel filter connector in order to tie the shield of the LAN cable to the frame ground for EMC compliance.

Figure 37
NTMF94EA ELAN, TLAN and serial port cable



End of Procedure

Install shielded TLAN network interface cable

Use Shielded CAT5 cable to connect to the ELAN and TLAN network interfaces on the NTCW84KA cable. To conduct a ground loop test, refer to page 589 and follow the test procedure.

For DCHIP cards

Connect a shielded CAT5 LAN cable from the TLAN subnet hub to the RJ-45 coupler on the NTCW84KA TLAN network interface.

For non-DCHIP cards

Connect a shielded CAT5 LAN cable from the TLAN subnet hub to the RJ-45 coupler on the NTMF94EA TLAN network interface.

> ***Note:*** When connecting the Media Card 32-port trunk card and/or ITG-Pentium 24-port trunk card to the TLAN subnet, the link status LED on the card faceplate associated with the TLAN network interface lights green when the connection is made. The link status LED on the hub port also lights green when connected to the IP trunk card.

Install shielded ELAN network interface cable

For DCHIP cards

Connect a shielded CAT5 LAN cable from the ELAN subnet hub to the RJ-45 coupler on the NTCW84KA ELAN network interface.

For non-DCHIP cards

Connect a shielded CAT5 LAN cable from the ELAN subnet hub to the RJ-45 coupler on the NTMF94EA ELAN network interface.

> ***Note:*** There are no ELAN network status LEDs for the ELAN network interface on the Media Card 32-port trunk card and ITG-Pentium 24-port trunk card. When connected to the IP trunk card ELAN network interface, the port status LED indicator on the ELAN subnet hub lights green to indicate a good connection.

D-channel cabling for the NT0961AA ITG-Pentium 24-Port trunk card

In this section, check, and reset if necessary, MSDL switch settings, install a filter (if required for the installation) and install the cable that connects the MSDL or SDI/DCH card to the IP trunk card that provides the DCH interface.

Required cables and filters for Large Systems

Large Systems require the following:

- the NTCW84KA ELAN, TLAN, RS-232 and DCH Ports cable
- the NTND26AA MSDL DCH cable

Configure NT6D80 MSDL switches

Configure the switches in the NT6D80 MSDL card as shown in Table 45.

Table 45
NT6D80 MSDL settings for ITG-Pentium 24-port trunk card DCHIP

	Port 0 – SW4	**Port 0 – SW8**
RS-422-A DTE	all off	all on
	Port 1 – SW3	**Port 1 – SW7**
RS-422-A DTE	all off	all on
	Port 2 – SW2	**Port 2 – SW6**
RS-422-A DTE	all off	all on
	Port 3 – SW1	**Port 3 – SW5**
RS-422-A DTE	all off	all on
Note: The device number for the MSDL card is configured in LD 17 at the prompt DNUM. Also configure the device number, using switches S9 and S10, on the MSDL card. S9 designates ones and S10 designates tens. To configure the device number as 14, for example, set S10 to 1 and S9 to 4.		

Install filter and NTND26 cable (for MSDL and DCHIP cards in same Large System equipment row)

Follow the steps in Procedure 11 to install the filter and NTND26 cable for MSDL and DCHIP cards in same Large System equipment row.

Procedure 11
Installing the filter and NTND26 cable for MSDL and DCHIP cards in the same Large system equipment row

1 Install the bracket for the 15-pin I/O panel filter connector in one of the two smaller openings (J2, J3, J4, J5) of the I/O panel of the IPE Module that contains the DCHIP card.

2 Install the 15-pin I/O panel filter connector on the inward side of the bracket.

3 Obtain the correct length of the NTND26 DCHI Interface Cable Assembly to reach from the D-Channel port connector on the faceplate of the MSDL card to the outward side of the 15-pin filter connector installed in the I/O panel of the IPE module that contains the DCHIP card. See Figure 38 on page 271.

The NTND26 DCHI Interface Cable Assembly is available in the following lengths:

- NTND26AA – 6 ft
- NTND26AB – 18 ft
- NTND26AC – 35 ft
- NTND26AD – 50 ft

4 Connect the appropriate NTND26 cable assembly to the D-Channel port connector on the faceplate of the MSDL card and to the inward side of the 15-pin filter connector installed in the I/O panel of the IPE Module that contains the DCHIP card (see Figure 39 on page 272).

Figure 38
15-pin filter connector installation

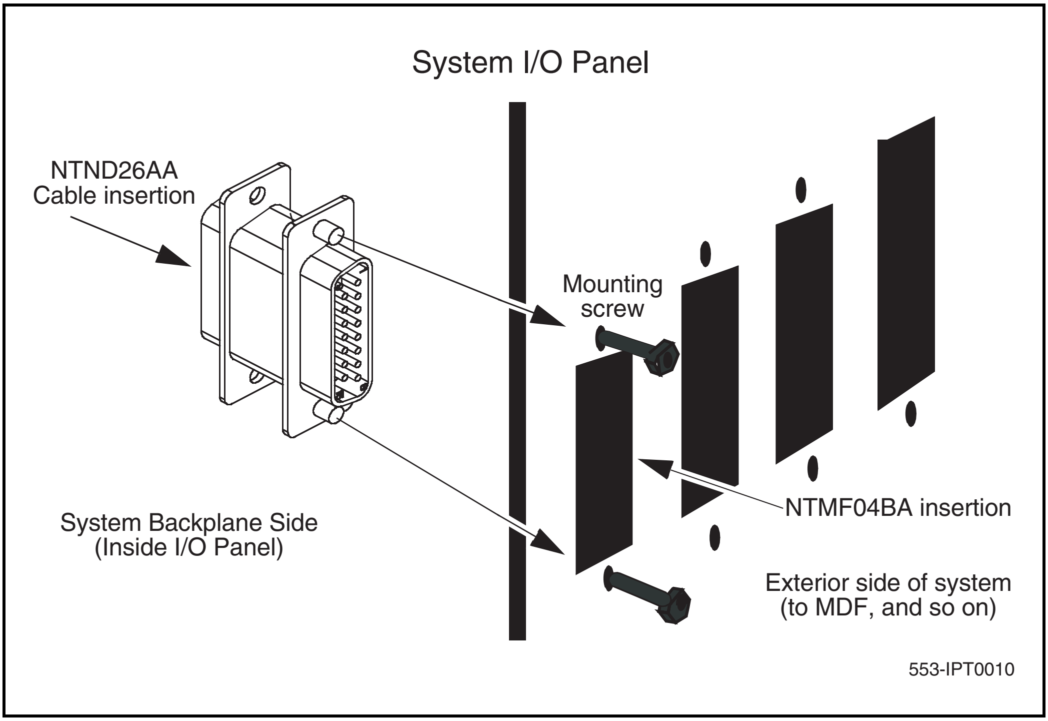
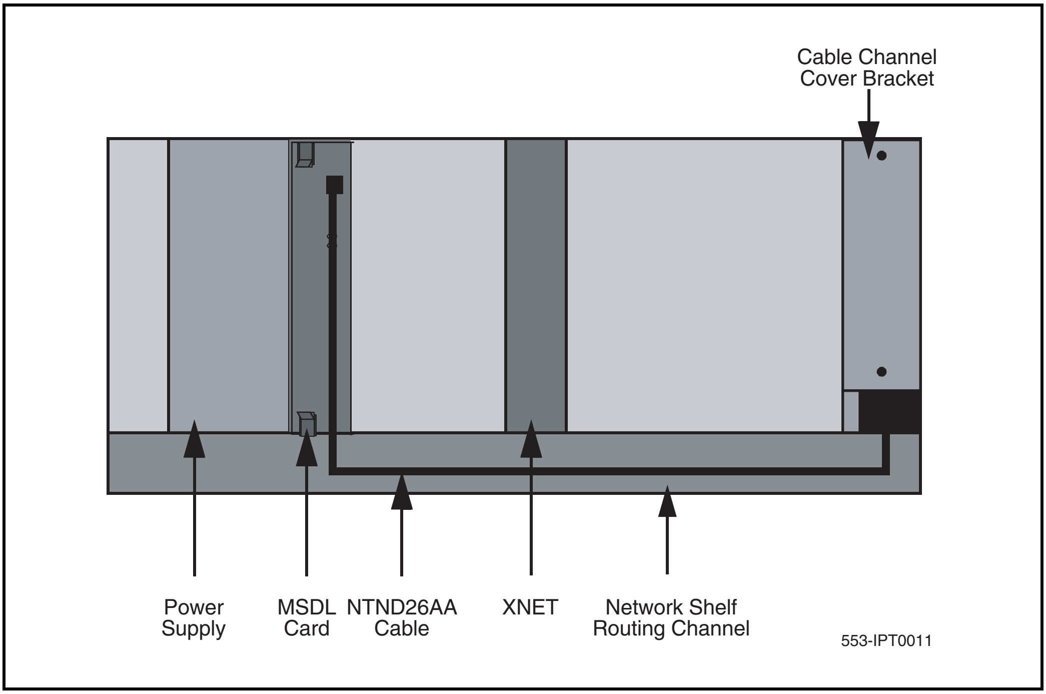


Figure 39
NTND26 cable routing diagram



5 Connect the DCH (P5) connector of the NTCW84KA to the outward side of the 15-pin I/O panel filter connector.

End of Procedure

Install filter and NTND26 cable (for MSDL and DCHIP cards in different Large System equipment rows)

Follow the steps in Procedure 12 on page 273 to install the filter and NTND26 cable for MSDL and DCHIP cards in different Large System equipment rows.

Procedure 12
Installing the filter and NTND26 cable for MSDL and DCHIP cards in different Large System equipment rows

1. Install the bracket for the 15-pin I/O panel filter connector in the J16, J17, J37 or J38 I/O panel opening of the I/O panel of the Network Module or Core/Net Module that contains the MSDL card.

2. Install the 15-pin I/O panel filter connector on the inward side of the bracket.

3. Obtain the correct length of the NTND26 DCHI Interface Cable Assembly to reach from the D-Channel port connector on the faceplate of the MSDL card to the outward side of the 15-pin filter connector installed in the I/O panel of the IPE Module that contains the DCHIP card.

   The NTND26 DCHI Interface Cable Assembly is available in the following lengths:

   - NTND26AA – 6 ft.
   - NTND26AB – 18 ft.
   - NTND26AC – 35 ft.
   - NTND26AD – 50 ft.

4. Connect the appropriate NTND26 cable assembly to the D-Channel port connector on the faceplate of the MSDL card and to the outward side of the 15-pin filter connector installed in the I/O panel of the IPE Module that contains the DCHIP card.

5. Use the NTMF04BA Extension Cable to connect the DCH (P5) connector of the NTCW84KA to the inward side of the 15-pin I/O panel filter connector.

End of Procedure

Small System cable installation

Follow the steps in Procedure 13 on page 274 for Small System cable installation.

Procedure 13
Installing cables on Small Systems

1 Set the switches and jumper plugs in the NTAK02 SDI/DCH card as shown. See Table 46 and Table 47.

Table 46
NTAK02 SDI/DCH switch settings for IP Trunk 3.01 (and later) DCHIP

Port 1	**SW 1-1**	**SW 1-2**
DCH	OFF	OFF
Port 3	**SW 1-3**	**SW 1-4**
DCH	OFF	OFF

Table 47
NTAK02 SDI/DCH jumper settings for the IP Trunk 3.01 (and later) DCHIP

Port	Jumper location	Strap for DTE	Jumper location	RS422
Port 1	J7	C – B	J9	C – B
	J6	C – B	J8	C – B
Port 3	J4	C – B	J2	C – B
	J3	C – B	J1	C – B

2 Connect the NTAK19FB Quad Serial I/O SDI/DCH Cable (or equivalent) to the I/O connector for the card slot in which the SDI/DCH card is installed.

3 If the DCHIP card is installed in the main cabinet with the SDI/DCH card, then use NTWE04AD SDI/DCH Extension Cable (1 ft) from the NTCW84KA DCH (P5) connector to the NTAK19FB D-Channel port connector for Port 1 or Port 3.

4 If the DCHIP card is installed in the expansion cabinet, then use NTWE04AC SDI/DCH Extension Cable (10 ft) from the NTCW84KA DCH (P5) connector to the NTAK19FB D-Channel port connector for Port 1 or Port 3.

End of Procedure

Install the serial cable

Follow the steps in Procedure 14 to install the serial cable.

Procedure 14
Installing the serial cable

1 To make a temporary connection to the IP Trunk 3.01 (and later) maintenance port from a local RS-232 TTY terminal or a modem, use the NTAG81CA PC Maintenance cable.

a. Connect the DIN-8 connector to the maintenance port on the faceplate of the IP trunk card.

b. Connect the DB9 connector to the COM port of a local PC running TTY terminal emulation.

If required, use an NTAG81BA Maintenance Extender cable to provide an extension between the NTAG81CA PC Maintenance cable and the PC COM port. For remote dialup access from a remote PC, use a null modem adaptor between the NTAG81CA (or NTAG81BA) maintenance cable and the modem.

2 To make a more permanent connection to the maintenance port:

a. Connect the NTAG81BA Maintenance Extender cable to the female DB9 connector of the NTCW84KA I/O cable for DCHIP cards, or the NTMF94EA I/O cable for non-DCHIP cards.

b. Connect the other end of the NTAG81BA Maintenance Extender cable to the PC COM port, or through a null modem cable to a modem.

Note: Only a single maintenance port connection can be made at a time. Do not connect a terminal or modem to the faceplate maintenance port and the NTCW84KA or the NTMF94EA.

End of Procedure

Cabling for the Media Card 32-port trunk card

This section describes the cabling necessary to install the Media Card 32-port trunk card.

ELAN and TLAN network interfaces

The Media Card 32-port trunk card supports a single connector solution for access to the TLAN and ELAN network interfaces. This ITG Card ELAN/TLAN Adapter solution (L-adapter) replaces the ITG-Pentium 24-port product which requires a single ‘octopus’ cable. The L-adapter can also be used on the ITG-Pentium 24-port trunk card. Refer to “Patches and advisements” on page 571 for more information on cabling the ITG-Pentium 24-port trunk card.

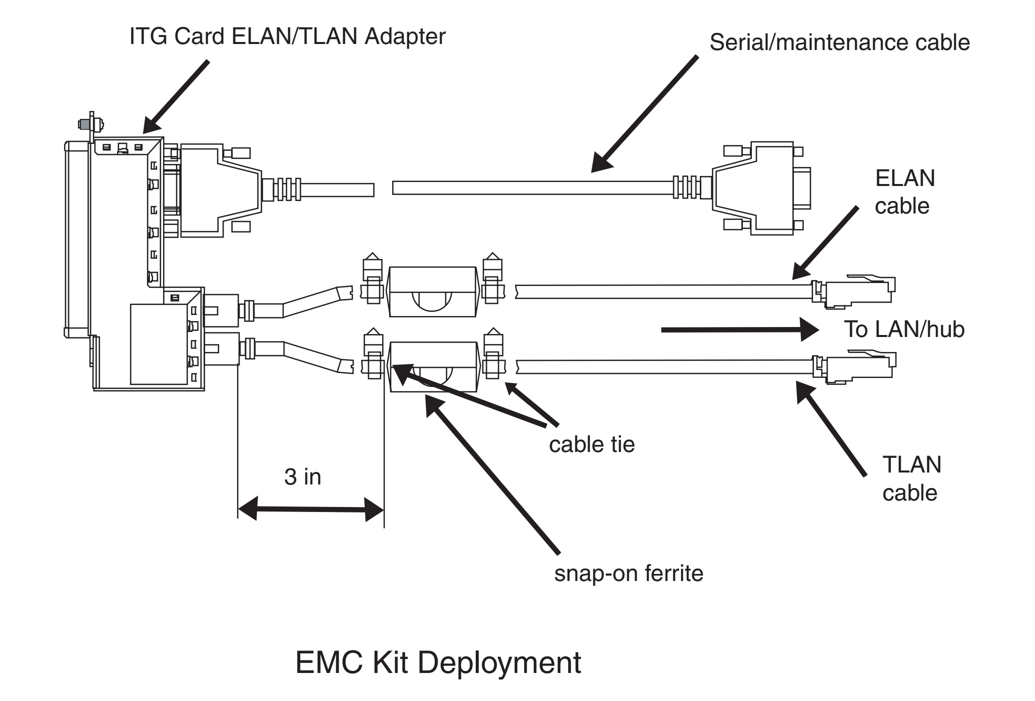
The ELAN network interface supports 10BaseT operation. The TLAN network interface supports 10/100BaseT operation. To support the 100BaseT operation on Large Systems, the TLAN network interface requires specialized I/O panel mounting connectors. These connectors replace the standard connectors provided on the system.

Cables and connectors for the ELAN and TLAN network interface include the following:

- the NTCW84JA Large System I/O panel filter block
- the network interface ITG Card ELAN/TLAN Adapter, for use with both D-Chip and non-D-Chip equipped cards. Standard shielded, CAT 5 LAN cables (<100 meters) are recommended to attach the LAN ports to the local network.

An ITG EMC shielding kit (NTVQ83) must be installed on the ELAN and TLAN network interface cables to meet regulatory requirements at the installation site. As shown in Figure 40 on page 277, a ferrite must be placed on both the ELAN and TLAN network interface cables during installation. Cable ties are then placed to retain the ferrites in the correct position. This applies to both Small Systems and Large Systems.

Figure 40
EMC kit deployment



ITG Card ELAN/TLAN Adapter (L-adapter)

The L-adapter routes the signals to the following network interfaces:

- ELAN
- TLAN
- one RS-232 port

On Large Systems, the NT8D81AA cable is used to bring all 24 Tip & Ring pairs to the I/O panel. The NTCW84JA I/O panel mounting block must be installed on Large Systems before the ITG Card ELAN/TLAN Adapter (L-adapter) is installed. Refer to Figure 41 on page 278.

Install the adapter securely to ensure an active connection.

Figure 41
ITG card ELAN/TLAN adapter (L-adapter)

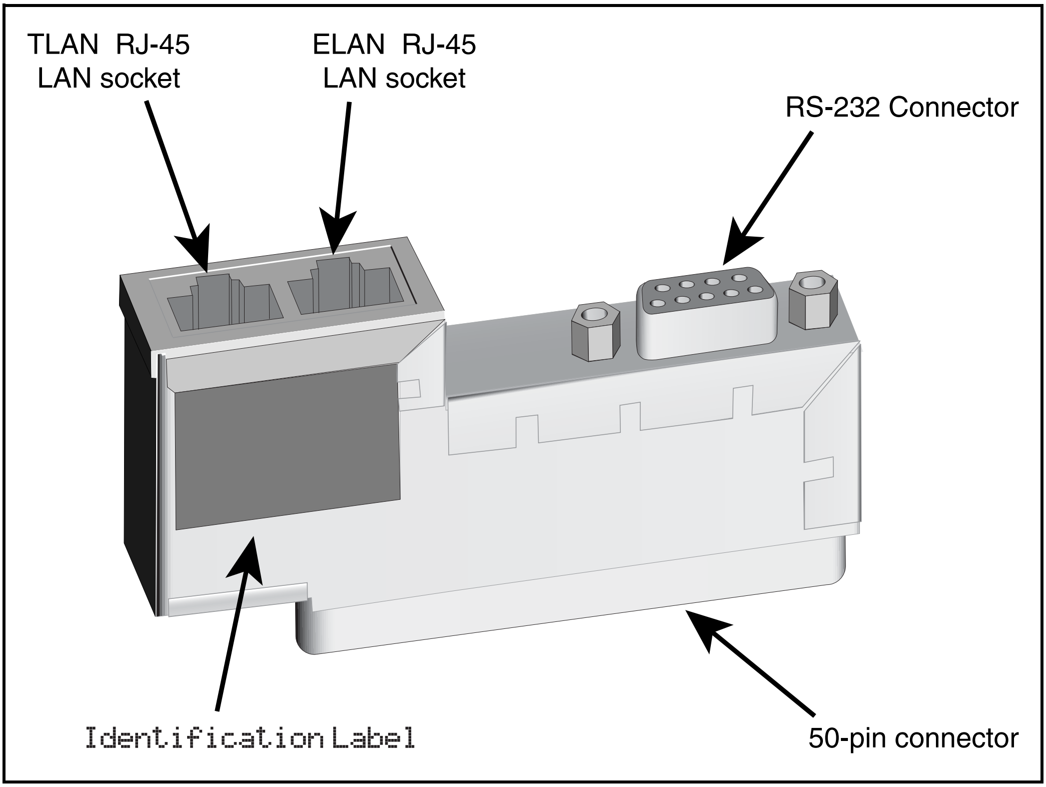
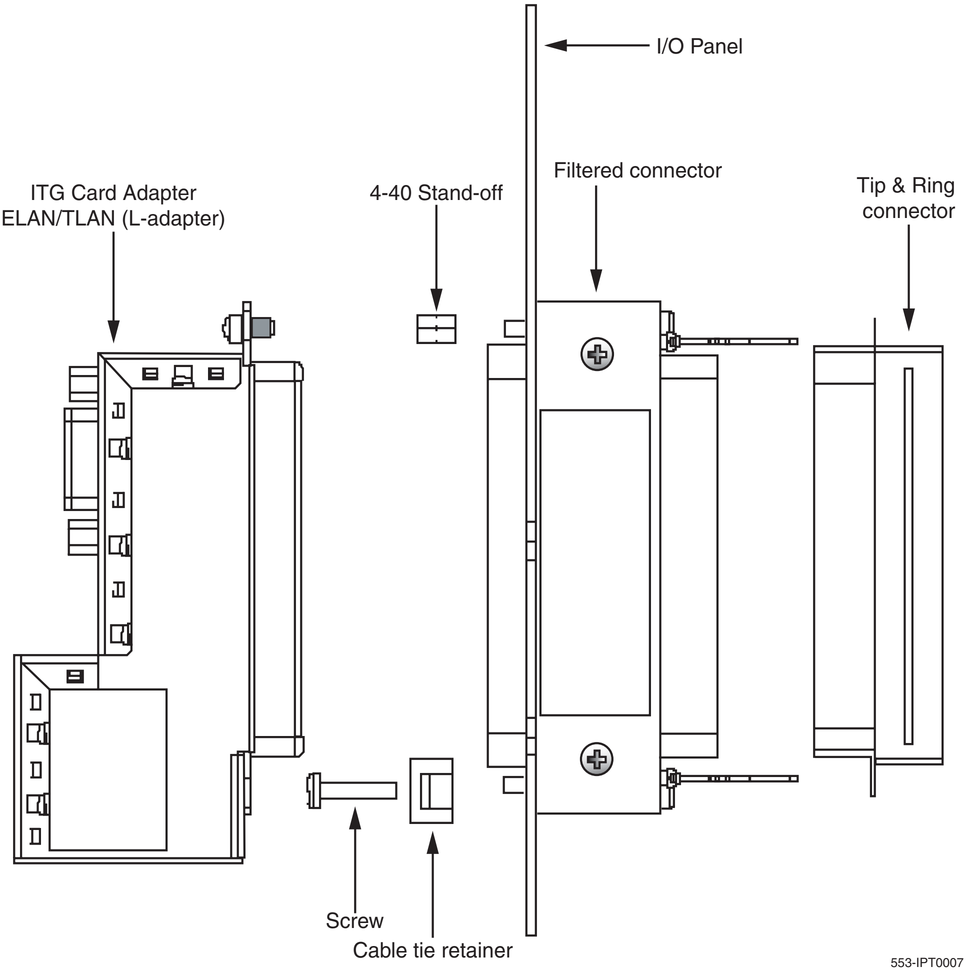


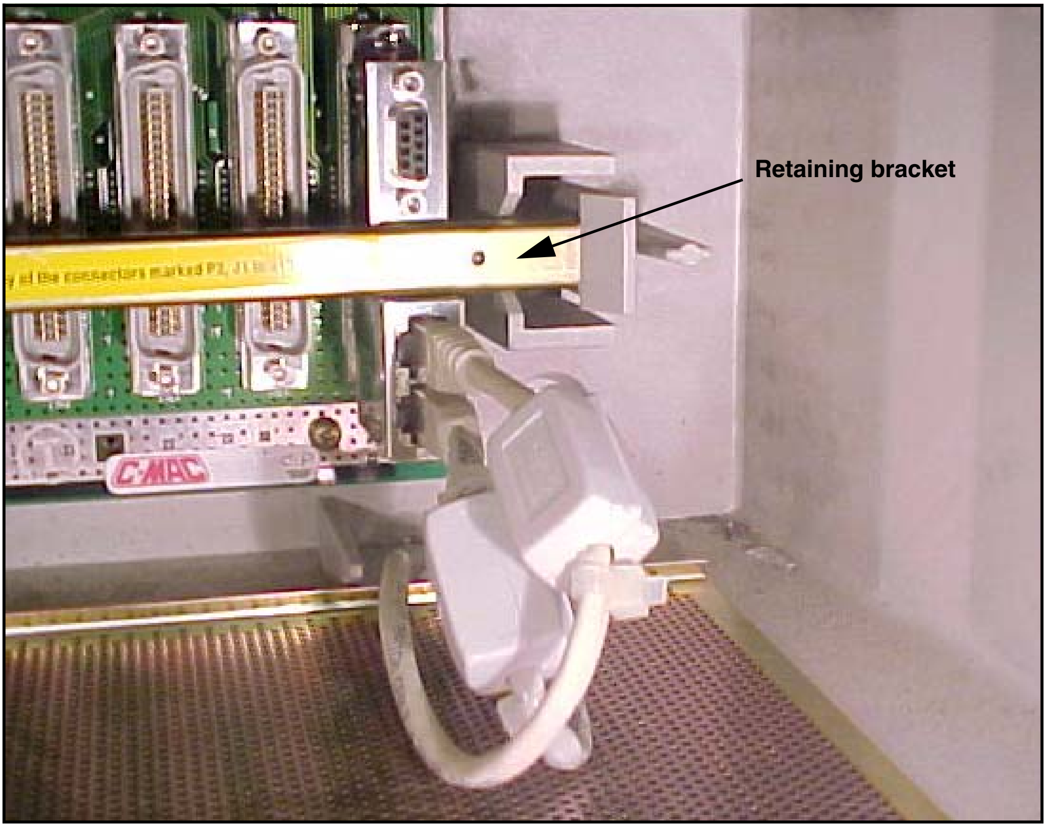
Figure 42 shows the adapter installed in a Large System with a securing screw and tie wrap.

Figure 42
ITG card ELAN/TLAN adapter (Large system)



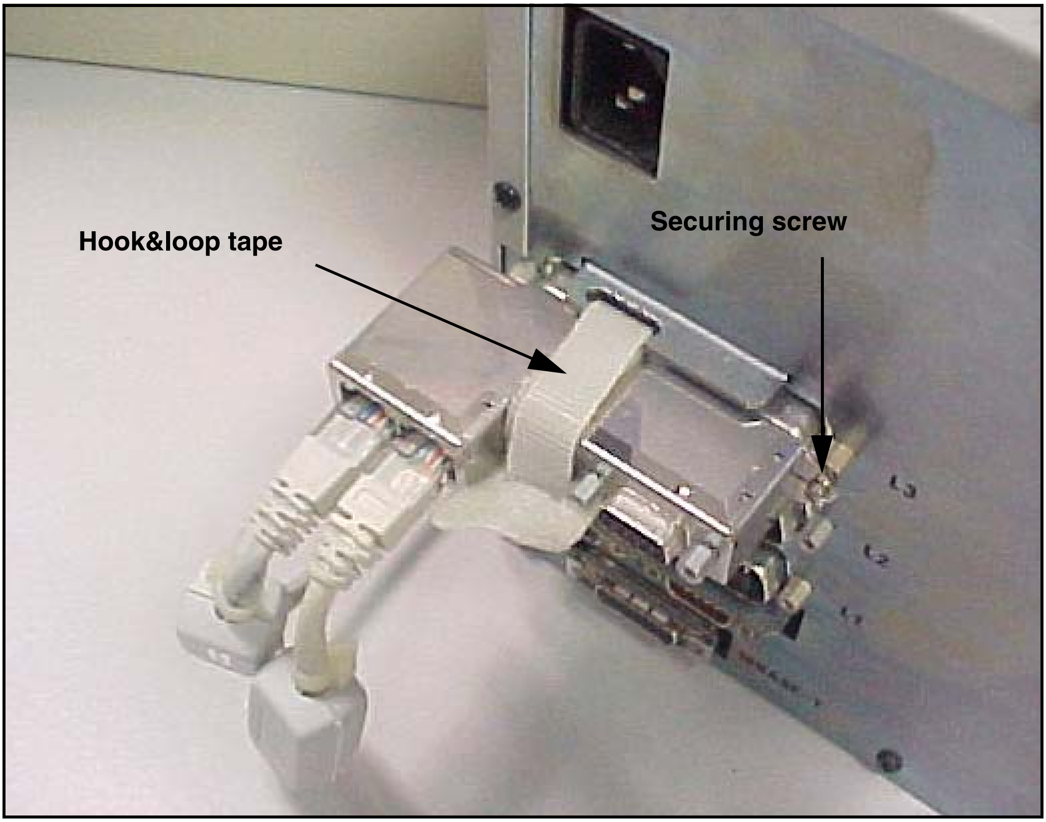
To install the L-adapter in a Small System, use a securing screw and retaining bracket. See Figure 43.

Figure 43
ITG card ELAN/TLAN adapter fitted to a Meridian 1 Option 11C Cabinet/ CS 1000M Cabinet



To install an adapter in a Meridian 1 PBX 11C Chassis / CS 1000M Chassis, use a securing screw and hook&loop tape. See Figure 44.

Figure 44
ITG card ELAN/TLAN adapter fitted to a Meridian 1 PBX 11C Chassis/CS 1000M Chassis



Note 1: When Media Card 32-port trunk cards are used to replace ITG-Pentium 24-port trunk cards, the existing NTMF94EA or NTCW84KA cabling can be used.

Note 2: The DCHIP connection on the NTCW84KA cable does not function with the Media Card 32-port trunk card. To connect the DCHIP where the NTCW84KA cable is being used, follow the instructions in Procedure 15 on page 283.

RS-232 maintenance port

The RS-232 maintenance port provides access to the Media Card 32-port trunk card command prompt for monitoring and maintenance purposes, such as upgrades and debugging. This port is available at the 9-pin connector on the ITG Card ELAN/TLAN Adapter (L-adapter) subnet and at the mini-DIN socket on the faceplate.

The serial port settings are as follows:

- 9600 baud
- 8 data bits
- 1 stop bit, no parity
- no flow control

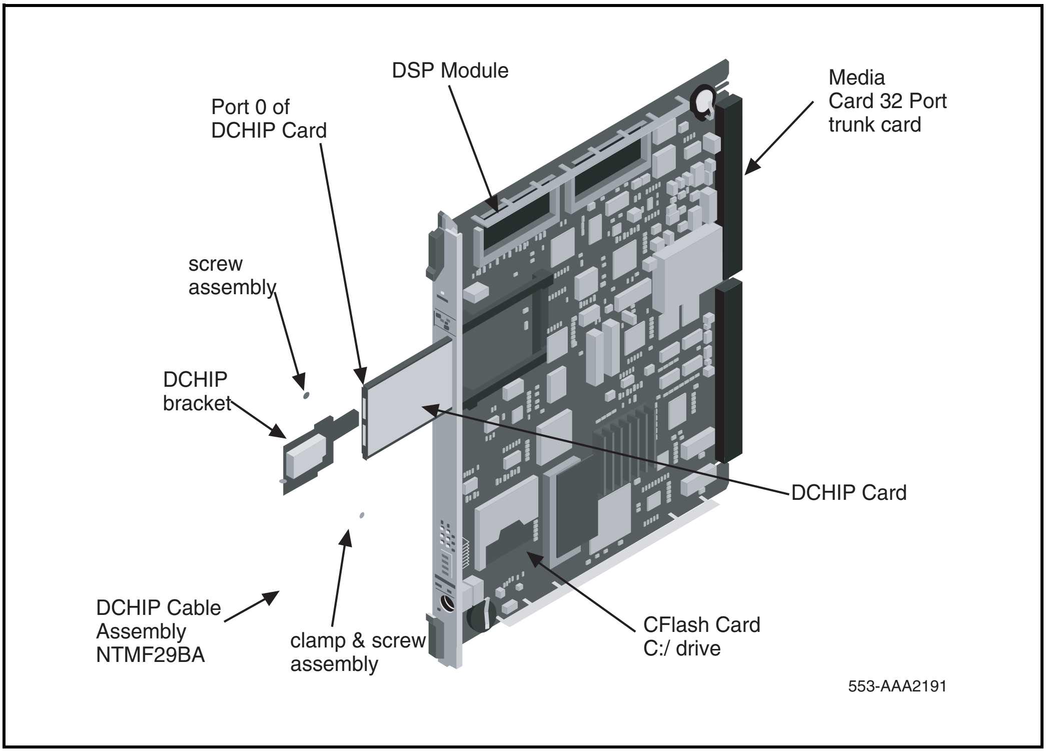
NTMF29BA DCHIP cable

The NTMF29BA DCHIP cable connects to port 0 of the DCHIP PC Card and the MSDL/SDI DCHIP cable.

> ***Note:*** Port 1 on the DCHIP PC Card is not used.

The DCHIP PC Card, which connects to NTMF04BA and NTND26AA Cable, is keyed to allow insertion only in the correct direction. Refer to Figure 45 on page 283.

Figure 45
NTMF29BA PC Card DCHIP cable installation



To assemble the DCHIP cable, follow the steps in Procedure 15.

Procedure 15
Assembling the DCHIP cable

1. Insert the DCHIP bracket through the small slot to the left of the PC Card opening in the faceplate, as shown in Figure 45.
2. Fit the screw through the secondary side of the Media Card 32-port trunk card into the threaded hole in the bracket and tighten.
3. Fit the DCHIP PC Card NTMF29BA cable assembly through the faceplate slot and push it home into the header.
4. Fit the DCHIP PC Card connector of the NTMF29BA cable assembly into Port 0 (the upper socket) on the DCHIP card.

5 Fit the clamp over the PC Card connector and into the bracket. Ensure that the cable is fitted through the clamp, then secure it to the bracket with the attached screw.

6 Make sure the eject button protrudes when the card is fully inserted. Do not use excessive force when inserting the DCHIP PC Card.

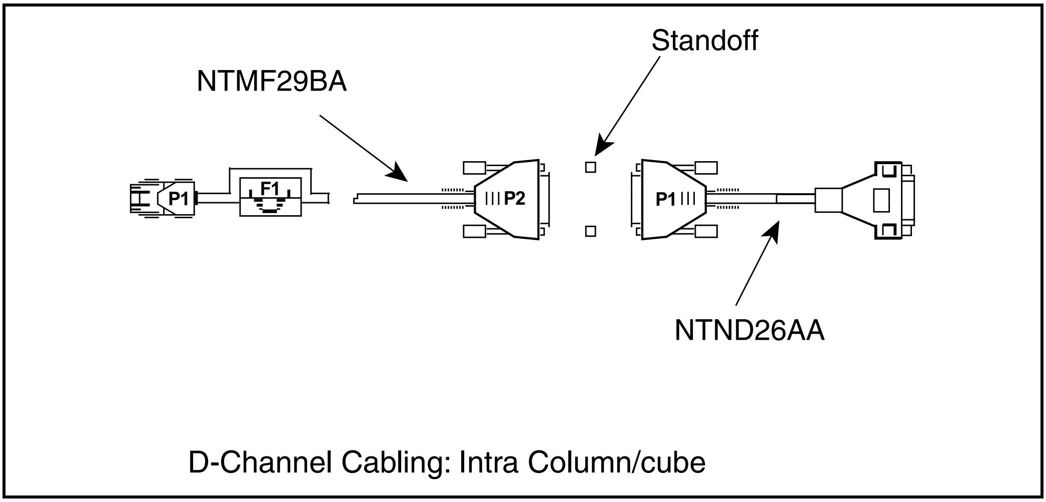
End of Procedure

DCHIP cable routing – Large Systems

NTMF29BA/NTND26AA cable routing

The NTND26AA cable from the MSDL forms a direct flying lead connection to the NTMF29BA cable from the DCHIP card. The cables must be routed internally to the system along the cabling channels, as shown in Figure 46. The NTND26 cable is available in various lengths.

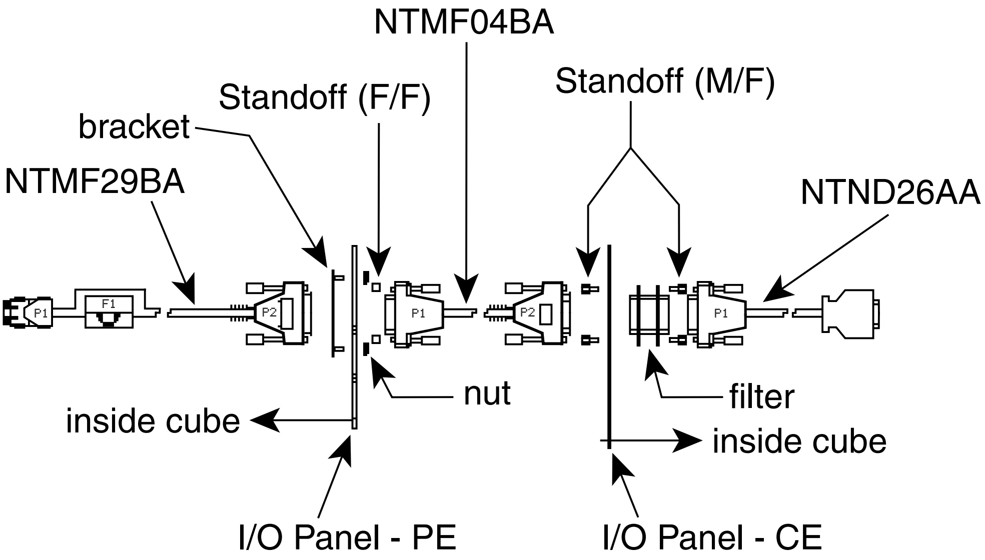
Figure 46
Large System DCHIP cabling setup: intra-column/cube



NTMF04BA MSDL extension cable

The NTMF04BA cable connects the NTND26AA MSDL cable and the NTMF29BA DCHIP cable, when the Common Equipment shelf and the IPE shelf are in separate columns and not connected by internal cabling channels. A 15-way mounting block (A03511331) is shipped with the NTMF04BA cable. The mounting block, when mounted on the Common Equipment shelf I/O panel, allows the connection of the NTND26AA and the NTMF04BA cables. The NTMF04BA cable is then routed externally to the IPE I/O panel to connect with the NTMF29BA DCHIP. See Figure 47.

Figure 47
Large system DCHIP cabling setup: inter-column

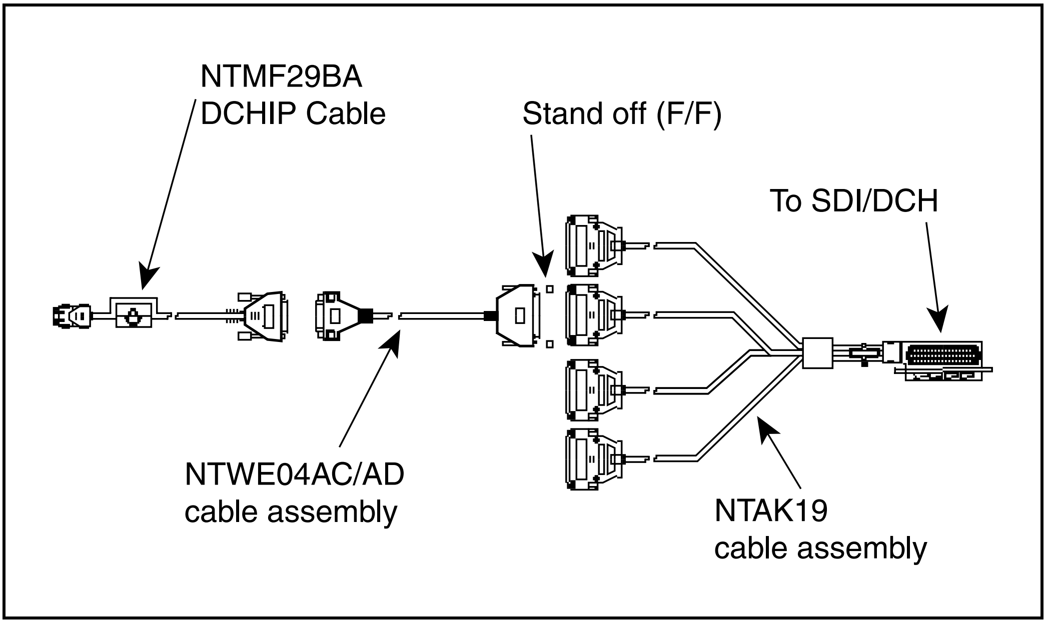


When the Universal Equipment Modules (UEM) are stacked vertically, or the UEM columns are bolted together, they are cabled in an inter-column configuration. See Figure 47. This applies when the UEM system columns are physically separated and the DCHIP must exit the systems through the I/O panel.

DCHIP Cable Routing Meridian 1 Option 11C Cabinet/CS 1000M Cabinet

The following cables are specific to Meridian 1 Option 11C Cabinet/CS 1000M Cabinets. Cable connection details are shown in Figure 48.

Figure 48
Option 11C DCHIP system cabling



NTWE04AC/AD SDI/DCH Meridian 1 Option 11C Cabinet/CS 1000M Cabinet extension cable

The NTWE04AC and the NTWE04AD are 10-ft and 1-ft DCHIP extension cables, respectively. They connect Port 1 or Port 3 of the DCHIP SDI/DCH cable used on the Meridian 1 Option 11C Cabinet/CS 1000M Cabinet (NTAK19BA or equivalent) with the DCHIP NTMF29Bx face-plate cable.

NTAK19BA four-port SDI/DCH cable

The NTAK 19BA cable is an Option 11C MDF cable for interfacing to the 4-port NTAK02 SDI/DCH card.

Other components

For Large Systems, I/O panel 50-pin filtered adapters NTCW84JA are required for 100BaseT TLAN subnet operation.

IP Trunk 3.01 (and later) uses the ITG Card ELAN/TLAN adapter to route Ethernet signals through the system I/O panel and through system filtering. For standard 10BaseT operation, this inherent filtering in the system does not pose a functional concern.

For 100BaseT Ethernet links, the system filtering does impact functionality. Special consideration has been given to the routing of the TLAN network interface Tip and Ring pairs. On a Meridian 1, some of the Tip and Ring pairs have been left free of filtering. The TLAN subnet has been routed on the Media Card 32-port trunk card to take advantage of this. By default, 100BaseT operation is fully functional on Small Systems.

Install ITG EMC shielding kit NTVQ83 with Small and Large System types. Refer to “ELAN and TLAN network interfaces” on page 276 for additional information on the cabling requirements.

Media Card 32-port trunk card modem connection

To provide remote access to the CLI for support and remote maintenance, a modem can be connected to the serial port of the Media Card 32-port trunk card. To configure a working interface, follow the steps in Procedure 16 on page 288.

Procedure 16
Connecting the Media Card 32-port trunk card modem

1 Use a standard serial cable and establish communication with the modem from a PC. Use the following settings:

- 9600 baud
- 8 data bits, 1 stop bit
- no parity
- no flow control

2 Ensure that a Hayes-compatible modem is used. From the command line, type the following:

AT <return>

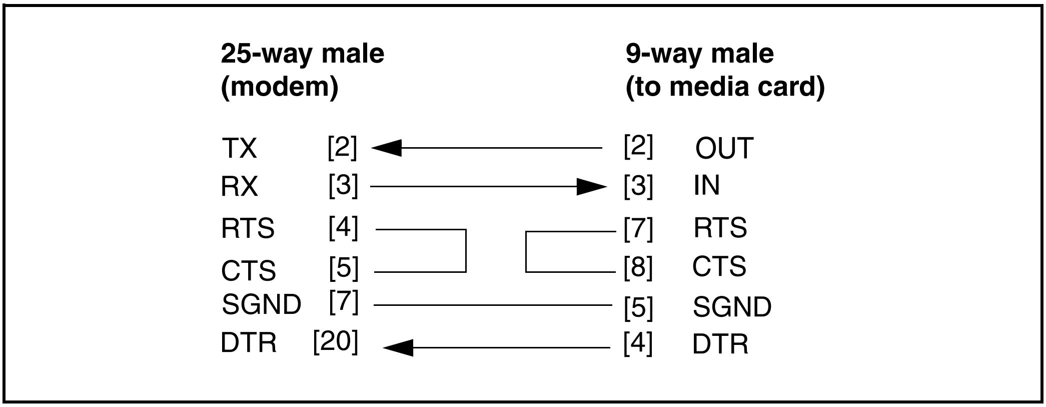
3 When the OK prompt appears, enter the required settings from Table 48.

Table 48
Modem Settings

Setting	Action
ATS0=1 <return>	Set to auto-answer on first ring.
ATQ1 <return>	Disable result codes.
ATE0 <return>	Disable local echo.
AT&W0 <return>	Save settings.

4 Connect the modem to the Media Card 32-port trunk card, using the 9-pin connector on the ITG Card ELAN/TLAN Adapter (L-adapter) or the legacy ITG cable. The interface cable must conform to the wiring specifications listed in Figure 49 on page 289 for compatibility with existing ITG modem connections.

Figure 49
Wiring specifications



End of Procedure

Configure IP Trunk 3.01 (and later) data

First, configure D-channels, Route Data Blocks, and trunks through the system TTY. Then configure the ESN data blocks to implement the network dialing plan and translations. Record the D-Channel, CHIDs, and TNs for the IP Trunk 3.01 (and later) trunks on the IP Trunk 3.01 (and later) Installation Summary Sheet.

> ***Note:*** To configure IP Peer Networking Virtual Trunks, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213). Record the first CHID for the Virtual Trunks on the Virtual Trunk Installation Summary Sheet.

Configure the ISL D-channel on the system for the DCHIP card for IP Trunk 3.01 (and later)

For the IP Trunk 3.01 (and later) application, use LD 17 to configure the ISL D-channel for the DCHIP card in Large Systems.

LD 17 – Configure the ISL D-channel for the DCHIP card (Large Systems) (Part 1 of 3)

Prompt	Response	Description
REQ	CHG	Add new data.
TYPE	ADAN	Type of data block.
ADAN	NEW DCH x	Action Device and Number, where: x = 0-255
CTYP	MSDL	Multi - purpose Serial Data Link card type. Set MSDL switch settings for the ISL DCH port to RS-422.
GRP	x	Network Group number, where: x = 0 – 4
DNUM	x	Device Number for I/O ports, where: x = 0 – 15

LD 17 – Configure the ISL D-channel for the DCHIP card (Large Systems) (Part 2 of 3)

Prompt	Response	Description
PORT	x	Port number for MSDL card, where: x = 0 – 3
DES	IP TRUNK	16 character designator is “IP TRUNK” Specific description if more than one IP Trunk 3.01 (and later) route exists.
...		
USR		User.
	ISLD	Dedicated Mode ISDN Signaling Link.
IFC		Interface type for D-channel:
	SL1	Meridian Customer Defined Network (MCDN)
	ESGF	ESIG interface with GF platform (QSIG)
	ISGF	ISIG interface with GF platform (QSIG) ***Note 1:*** The ESGF and ISGF responses are allowed if the QSIG and QSIG GF packages are both equipped. ***Note 2:*** The IFC entry must match the protocol entered in OTM 2.1 (and later) Node Properties, Card Configuration, Protocol pull-down menu.
ISLM	xxx	Integrated Service Signaling Link Maximum CHIDs, where: x = 1 – 382 ISLM is the maximum number of ISL trunks controlled by the D-channel. There is no default value.
BPS	(64000)	64000 is the default and is required for the IP Trunk 3.01 (and later) DCHIP.

LD 17 – Configure the ISL D-channel for the DCHIP card (Large Systems) (Part 3 of 3)

Prompt	Response	Description
PARM	(RS422 DTE)	The RS-422 parameters are established with switch settings on the MSDL card. This prompt is used to verify those settings prior to enabling the card.
RCAP	ND2	Remote Capabilities Network Name Display type 2 signaling. All nodes must use same RCAP.
...		
SIDE	(USR)	MSDL acts as User side of ISL. The IP Trunk 3.01 (and later) DCHIP card acts as the Network side of ISL.
RLS	25	Release ID of PBX at the far end of the D-Channel. If the far end has an incompatible release, it prevents sending of application messages.

Use LD 17 to configure the ISL D-channel for the DCHIP card in Small Systems.

LD 17 – Configure the ISL D-channel for the DCHIP card (Small Systems) (Part 1 of 3)

Prompt	Response	Description
REQ	CHG	Add new data
TYPE	ADAN	Type of data block
ADAN	NEW DCH x	Action Device and Number, where: x = 0 – 79

LD 17 – Configure the ISL D-channel for the DCHIP card (Small Systems) (Part 2 of 3)

Prompt	Response	Description
CTYP		Card Type.
	DCHI	SDI/DCH card (configure the option switches and jumper straps on the SDI/DCH for RS422 DTE mode operation.
CDNO	xx	Card Number where DCHI resides for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T.
PORT	1 or 3	Port Number must be 1 or 3.
USR		User.
	ISLD	Dedicated Mode ISDN Signaling Link
IFC		Interface type for D-channel:
	SL1	Meridian Customer Defined Network (MCDN) ***Note:*** The IFC entry must match the protocol entered in OTM's ITG Node Properties, Card Configuration, Protocol pull-down menu.
ISLM	xxx	Integrated Service Signaling Link Maximum CHIDs, where: x = 1 – 382 ISLM is the maximum number of ISL trunks controlled by the D-channel. There is no default value.
...		
SIDE	(USR)	Meridian 1 Option 11C Cabinet/CS 1000M Cabinet SDI/DCH card acts as User side of ISL. The DCHIP card acts as the Network side of ISL.

LD 17 – Configure the ISL D-channel for the DCHIP card (Small Systems) (Part 3 of 3)

Prompt	Response	Description
RLS	25	Release ID of PBX at the far end of the D-Channel. If the far end has an incompatible release, it prevents sending of application messages.
RCAP	ND2	Network Name Display type signalling. All nodes must use same RCAP.
...		

Configure the ISL D-channel on the Meridian 1/CS 1000M for the DCHIP card for IP Trunk 3.01 (and later)

Because CS 1000S and IP Peer Networking do not support QSIG, only the MCDN protocol (SL1) is supported. Use LD 17 to configure the ISL D-channel for the DCHIP card for Large and Small Systems.

LD 17 – Configure the ISL D-channel for the DCHIP card (Large and Small Systems) (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ADAN	Type of Data Block
ADAN	NEW DCH x	Action Device and Number
CTYP	DCHI	Card Type – Meridian 1 PBX 11C Cabinet/CS 1000M Cabinet and Meridian 1 PBX 11C Chassis/CS 1000M Chassis. Optional for Large Systems.
	MSDL	Card Type – recommended for all other systems

LD 17 – Configure the ISL D-channel for the DCHIP card (Large and Small Systems) (Part 2 of 2)

Prompt	Response	Description
GRP	x	Network Group number = 0 – 4. Applies to Meridian 1 PBX 81C CP PII/CS 1000M MG without Fiber Network Fabric (FNF) only. Network Group number = 0 – 7. Applies to Meridian 1 PBX 81C CP PII/CS 1000M MG with FNF only
DNUM	xx	Device Number for I/O ports= 0 – 15. Applies to MSDL cards only.
CDNO	xx	Card Number where DCHI resides for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T.
PORT	x	Port number = 0 – 3 for MSDL card = 1 or 3 for DCHI on Meridian 1 PBX 11C Chassis/CS 1000M Cabinet
...		
USR	ISLD	User
IFC	SL1	Interface type for D-channel
ISLM	382	Maximum number of Integrated Service Signaling Links
...		
SIDE	USR	Meridian 1/CS 1000M node type

Note: The IFC response entry must have the protocol entered in OTM's ITG Node Properties – Card Configuration Protocol pull-down menu.

The MSDL card does not apply to Meridian 1 PBX 11C Cabinet/CS 1000M Cabinet and Meridian 1 PBX 11C Chassis/CS 1000M Chassis; therefore the DCGI prompts and responses apply. The feature requires the option switches on the Cabinet system SDI/DCH card to be set for RS-422 mode operation.

Configure ISDN feature in Customer Data Block

Use LD 15 to configure the ISDN feature in the Customer Data Block.

LD 15 – Configure ISDN feature in Customer Data Block (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change customer data block.
TYPE	NET_DATA	Gate-opener for networking features
CUST		Customer number
	0-99	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-31	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
OPT	a....a	Options
AC2	aaa bbb ccc	ESN call types under AC2 for the INAC feature. For example, NPA NXX INTL SPN LOC. INAC stands for automatic insertion of the ESN access code on incoming calls. ***Note:*** By default, the INAC feature puts all ESN call types except for CDP under AC1. Enable or disable INAC per trunk route in LD 16 in the ISDN section of the Route Data Block.
ISDN	(NO) YES	Enter YES to configure IP Trunk 3.01 (and later) routes.

LD 15 – Configure ISDN feature in Customer Data Block (Part 2 of 2)

Prompt	Response	Description
- PNI	(0) – 32700	Private Network Identifier. Configure the PNI to 1 or other non-zero value to support Meridian Customer Defined Network (MCDN) features that use non-call-associated signaling, such as Network Ring Again (NRAG) Network Message Services (NMS), Network ACD (NACD). Each feature needs ISDN signaling to be sent across the Meridian 1/CS 1000M network in the absence of a call. ***Note:*** The PNI in the Customer Data Block must be the same as the PNI configured in the Route Data Block at the far end for outgoing calls from the far end toward this Meridian 1/CS 1000M node.
...	...	...

Configure IP Trunk 3.01 (and later) TIE trunk routes

Use LD 16 to configure the IP Trunk 3.01 (and later) TIE trunk routes.

Note: Trunk routes must be configured as TIE routes.

LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block (Part 1 of 5)

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	RDB	Route Data Block. Configuration parameters that apply to all trunks in this route.
CUST	xx	Customer number as defined in LD 15.
ROUTE	xxx	Route Number, where: x = 0 – 511

LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block (Part 2 of 5)

Prompt	Response	Description
DES	IP TRUNK	16-character designator is “IP TRUNK” Specific description if more than one IP Trunk 3.01 (and later) route exists.
...		
TKTP		Trunk Type.
	TIE	The trunk type for IP Trunk 3.01 (and later) trunks must be set to TIE.
SAT	(NO) YES	Satellite control (SAT) must be set to NO to enable Trunk Optimization before answer (TRO) and Trunk Anti-Tromboning (TAT). For IP Trunk 3.01 (and later), fallback to circuit-switched trunks does not depend on SAT=YES.
...		
DTRK		Digital Trunk Route.
	(NO)	IP Trunk 3.01 (and later) trunks are analog only. They do not support circuit-switched data from MCA or ISDN BRI terminal adaptors.
ISDN	YES	Integrated Services Digital Network.
MODE		Mode of Operation.
	ISLD	Route uses ISDN Signaling Link in dedicated mode. ***Note:*** ISLD is allowed when ISDN = YES and the ISL package 147 is equipped. ISLD is allowed only on ISA and TIE trunks.

DCH	xxx	D-channel number, where:
		x = 0 – 255 for Large Systems.
		x = 0 – 79 for Small Systems.

LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block (Part 3 of 5)

Prompt	Response	Description
IFC	SL1 ESGF ISGF	Meridian Customer Defined Network (MCDN) is required for Small systems. ESIG interface with GF platform (QSIG) ISIG interface with GF platform (QSIG) The IFC of the Route Data Block must match the IFC of the ISL D-Channel in the configuration record.
PNI	(0) – 32700	Private Network Identifier. Configure the PNI to 1 or other non-zero value to support MCDN features that use non-call-associated signaling, such as Network Ring Again (NRAG) Network Message Services (NMS), Network ACD (NACD). Each feature needs ISDN signaling to be sent across the Meridian 1/CS 1000M network in the absence of a call. ***Note:*** The PNI in the Customer Data Block must be the same as the PNI configured in the Route Data Block at the far end for outgoing calls from the far end toward this Meridian 1/CS 1000M node.
NCNA	(YES) NO	Network Calling Name allowed
NCRD	(NO) YES	Network Call Redirection allowed
CTYP		Call Type for outgoing call dialed with the route access code (ACOD). Set to appropriate call type for IP Trunk 3.01 (and later) node numbering plan in order to make test calls using ACOD.

LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block (Part 4 of 5)

Prompt	Response	Description
INAC	(NO) YES	INAC stands for automatic insertion of the ESN access code on incoming calls, according to ISDN call types corresponding to NPA NXX INTL SPN LOC, for example. ***Note:*** Using INAC=YES can simplify the configuration of the ESN RLBs and DGT. It is recommended for MCDN features with non-call-associated signalling; for example, NMS, NACD, NRAG. ***Note:*** By default, the INAC feature puts all ESN call types except for CDP under AC1. If any call types must go under AC2 for INAC, use LD 15 to configure them at the AC2 prompt at the Customer Data Block.
...		
ICOG		Incoming and/or Outgoing trunk.
	IAO	Incoming and Outgoing.
SRCH	LIN	Linear search method. See Note 1.
SIGO	(STD) ESN5	Standard signaling arrangement ESN 5 signaling ***Note:*** Unless ESN5 is used, SIGO (outgoing signaling protocol) must be set to STD. ***Note:*** If SIGO equals ESN5: (1) Select SL1ESN5 from the pull-down list in the Protocol field in the ITG Node Properties configuration tab. (2) Select SL1ESN5 from the pull-down list in the Remote Capabilities field in the OTM Node Dialing plan General tab for each destination node that uses ESN5.

LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block (Part 5 of 5)

Prompt	Response	Description
CNTL	YES	
NEDC	ETH	Near End Disconnect Control from either originating or terminating side.
FEDC	ETH	Far End Disconnect Control from either originating or terminating side.

Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units for IP Trunk Route

Use LD 14 to configure the Media Card 32-port and ITG-Pentium 24-port trunk cards and units. Record the first CHID for each IP trunk card on the IP Trunk 3.01 (and later) Installation Summary Sheet.

LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units (Part 1 of 5)

Prompt	Response	Description
REQ	NEW XX	Add new data, where: xx = 1 – 24 for ITG-Pentium 24-port trunk card xx = 1 – 32 for Media Card 32-port trunk card When using REQ = NEW XX, configure only one IP trunk card at a time. When using REQ = NEW XX, CHID is incremented for each of the new units created. It might be necessary to configure partial IP trunk cards due to WAN traffic capacity limitations, or Leader and DCHIP card real-time capacity for very large nodes and networks.
TYPE	IPTI	Trunk Type IPTI is the only supported trunk type for IP Trunk 3.01 (and later) trunks. Error message SCH5787 is printed if an attempt is made to configure non-IPTI trunks as IP Trunk 3.01 (and later) trunks.

LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units (Part 2 of 5)

Prompt	Response	Description
TN		Terminal number
	l s c u	Format for Large System, Call Server 1000E, and Media Gateway 1000E, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
DES		16 character descriptive designator for the IP trunk card. **See Note 1.**
	hhhh:hh:hh:hh:hh	For unit 0. The IP trunk card ELAN network interface MAC address.
	xxx.xxx.xxx.xxx	For units 1 – 23. The IP trunk card ELAN network interface IP address.
XTRK		Extended Trunk Type: IP trunk card (1-slot or 2-slot assembly).
	MC32	Single slot, 32-port StrongArm (SA) processor Media Card.
	MC24	Double slot, 24-port Pentium processor Media Card.

MAXU	xx	Maximum number of ports on this IP trunk card, where:
		xx = 32 for the Media Card 32-port trunk card
		xx = 24 for the ITG-Pentium 24-port trunk card
		Note: A warning message is printed if a number larger than 24 is entered for MAXU. Ignore this warning for the Media Card 32-port trunk card.

LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units (Part 3 of 5)

Prompt	Response	Description
CUST	xx	Customer number as defined in LD 15.
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System, Call Server 1000E, and Media Gateway 1000E
	0-127 1-4000	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T

LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units (Part 4 of 5)

Prompt	Response	Description
CHID	xxx	First Channel ID for unit 0 on this IP trunk card, where: xxx = 1 - 382 for the ITG-Pentium 24-port trunk card and the Media Card 32-port trunk card Standard First CHID Configuration (24-port and 32-port): Leader 0: - 1 Leader 1: - 25 (24-port card) or 33 (32-port card) Follower: - 49 (24-port card) or 65 (32-port card) Follower: - 73 (24-port card) or 97 (32-port card) Follower: - 97 (24-port card) or 129 (32-port card) Follower: - 121 (24-port card) or 161 (32-port card) ***Note:*** For nodes containing a mixture of 24-port and 32-port IP trunk cards, determine the starting CHID by adding the number of channels (ports) on the previous card to the CHID of the previous card. **Example:** Leader 0: - 1 (24-port card) Leader 1: - 25 (1 + 24) (32-port card) Follower: - 57 (25 + 32) (32-port card) The same First CHID must be entered in OTM 2.1 (and later) ITG ISDN IP Trunk Node Properties, Card Configuration, “First CHID” field for this card. If this is not done, the trunk unit seized by the core switch does not match the trunk unit seized on the IP trunk card and the calls fall. The standard First CHID matches the trunk route member number for the trunk unit 0 in order to facilitate administration and maintenance.
...		

LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units (Part 5 of 5)

Prompt	Response	Description
STRI	WNK	Start Arrangement Incoming. Wink Start is preferred for IP Trunk 3.01 (and later).
STRO	WNK	Start Arrangement Outgoing. Wink Start is preferred for IP Trunk 3.01 (and later).
SUPN	YES	Answer supervision is required.
CLS	DIP	Class of Service. Dial Pulse is required for IP Trunk 3.01 (and later) to avoid busying multiple Digitone receivers when IP trunk card faults occur. ***Note:*** Trunks must always be set to DIP. If SIG0 = ESN5 in the RDB, the Meridian 1/CS 1000M does not allow CLS = DIP in LD 14. To avoid this problem and retain ESN5 signaling, set SIG0 = STD in RDB (LD 16). Then provision CLS = DIP in LD 14 for IP Trunk 3.01 (and later). After all trunks have been programmed, in LD 16 change the RDB back to SIG0 = ESN5.
...		

Note: Use the “NEW XX” command to assign DES equal to the IP trunk card ELAN network interface IP address; for example: 10.1.1.1. For unit 0, use CHG command to assign DES equal to the IP trunk card ELAN network interface MAC address; for example: 00:60:38:01:06:C6.
To find the ELAN network interface MAC address, refer to the IP Trunk 3.01 (and later) Installation Summary Sheet. The ELAN network interface MAC address is labeled on the IP trunk card faceplate as the “motherboard Ethernet address.” Alternatively, use the ITG shell command “ifShow” to display the Ethernet address for lnIsa (unit number 0).

Configure dialing plans within the corporate network

Configure the dialing plan by programming LDs 86, 87, and 90 as required.

Configure the Meridian 1/CS 1000M ESN by creating or modifying data blocks in LDs 86, 87, and 90, as required. The Meridian 1/CS 1000M and OTM IP Trunk 3.01 (and later) dialing plan information must correspond.

Make the IP Trunk 3.01 (and later) the first-choice, least-cost entry in the Route List Block

When adding IP Trunk 3.01 (and later) TIE trunks to an existing ESN, a common practice is to create a new Route List Block (RLB) for ESN translations that are to be routed by the IP Trunk 3.01 (and later) network. Insert the new IP Trunk 3.01 (and later) route ahead of the existing alternate routes for circuit-switched facilities, which are therefore shifted to the next higher entry number. Increment the ISET (initial set) if Call-Back Queueing or Expensive Route Warning tone are being used.

Turn on Step Back on Congestion for the IP Trunk 3.0 (and later) trunk route

For the IP Trunk 3.01 (and later) trunk route entry in the Route List Block (RLB), enter RRA at the Step Back on Congestion (SBOC) prompt. This enables fallback to alternate circuit-switched trunk routes in the following situations:

- due to network QoS falling below the defined threshold for the IP Trunk 3.01 (and later) node
- when there are no ports available at the destination IP Trunk 3.01 (and later) node

Turn off IP Trunk 3.01 (and later) route during peak traffic periods on the IP data network

Based on site data, if fallback routing occurs frequently and consistently for a data network during specific busy hours (for example, every Monday 10-11am, Tuesday 2-3pm), these hours should be excluded from the RLB to maintain a high QoS for voice services. By not offering voice traffic to a data network during known peak traffic hours, the incidence of conversation with marginal QoS can be minimized.

The time schedule is a 24-hour clock which is divided up the same way for all 7 days. Basic steps to program Time of Day for IP Trunk 3.01 (and later) routes are as follows:

1. Go to LD 86 ESN data block to configure the Time of Day Schedule (TODS) for the required IP Trunk 3.01 (and later) control periods.
2. Go to LD 86 RLB and apply the TODS on/off toggle for that route list entry associated with an IP Trunk 3.01 (and later) trunk route.

ESN5 network signaling

The original ITG-T ISDN application had two major categories of endpoints:

- ISDN-capable endpoints
- Non-ISDN endpoints

ESN5 information transmission is a mechanism allowing the transmission of NCOS information. ESN5 digit transmission was added when the ISDN capability was added to ITG Trunks.   ITG Trunk ISDN endpoints were able to insert the ESN5 prefix in an outgoing message if necessary, and did so based on the information in the dialing plan tables. This was the only possible alternative, since the flag indicating the type of ESN5 prefix and the two prefix digits were also legitimate dialed digits. Non-ISDN endpoints were, by definition, unable to handle ISDN, and therefore were not ESN5-capable.

IP Trunk 3.01 (or later) and ITG Trunk 2.x support a mixed network of remote nodes with ESN5 and standard (non-NCOS broadcasting) signaling.

ESN5 inserts the NCOS prefix ahead of the dialed numbers. If ESN5 signaling is to be used, it must be provisioned on both the IP Trunk cards and the Meridian 1/CS 1000 M Route Data Block (RDB) for that node.

However, this does not guarantee a satisfactory NCOS value. For example, the network may contain some ITG Trunk 1.0 basic trunk signaling nodes or other IP telephony gateways that use H.323 V2 instead of SL-1 (MCDN) signaling, and therefore do not support ESN5. An ESN5 node that interworks with one of these non-ESN5, non-ISDN IP telephony gateways and can receive an H.323 SETUP from them must have the default ESN prefix correctly provisioned.

The application defaults to an NCOS of “0”. If this is unsatisfactory, you must configure an ESN5 prefix for the non-ESN5 IP telephony gateways by using the CLI command **esn5PrefixSet** at the ITG shell on all IP Trunk cards in the ESN5 node. To verify the default ESN5 value that will be added for all incoming calls from non-ESN5 IP telephony gateways, use the CLI command **esn5PrefixShow** at the ITG shell.

If ESN5 is provisioned for an IP Trunk 3.01 (or later) node (both in the RDB and on the node cards), you must configure that node as “SL1 ESN5” in the dialing plan for all other ITG 2.x and IP Trunk 3.01 (or later) nodes. If these other nodes are also ESN5-capable, when originating a call they will pass the ESN5 prefix that they receive in the messages from the Meridian 1 to the destination node. Otherwise, a default NCOS is inserted by a non-ESN5 node sending the SETUP to the ESN5 destination. Only when the originator is not ISDN-capable is a default NCOS inserted by the ESN5 node receiving the call from the non-ESN5 VoIP gateway.

IP Trunk 3.01 (or later) nodes that are to support ESN5 signaling are configured in OTM at the ITG Node Properties window, in the Configuration tab in the Protocol field. Select **SL1 ESN5** from the drop-down list.

There are three possible scenarios where ESN5 prefixes are inserted:

1 A non-ESN5-compatible node calling an ITG Trunk 2.x node or calling an IP Trunk 3.01 (or later) node provisioned in the dialing plan table as SL1 ESN5. In this case, the originator inserts the ESN5 prefix.

2 Remote nodes calling an ESN5 IP Trunk 3.01 (or later) node using the Nortel interoperability non-standard data format, if the originating call does not use ESN5. In this case, the destination (IP Trunk or IP Peer) inserts the ESN5 prefix.

3 Remote nodes calling an ESN5 IP Trunk 3.01 (or later) node that does not support the MCDN protocol, since MCDN includes ESN5 capability. In this case, because the ISDN data is missing, the receiving node can identify that ESN5 data is required.

When an IP Trunk 3.01 (or later) node is configured as an ESN5 node and a call is received from a remote node that cannot send ESN5 data and does not provide the ESN5 data, the configured ESN5 prefix is inserted in front of the called number by the destination. (The remote node can be an IP Trunk 3.01 (or later), CS 1000S, or other gateway using the interoperability format. It can also be "H.323 only".) When the IP Trunk 3.01 (or later) node is configured to use standard signaling and the dialing plan entry indicates ESN5 capability, the ESN5 prefix is inserted in front of the called number by the originator.

For more information see "Non-Gatekeeper-resolved (local) dialing plan" on page 427.

Special dial 0 ESN translations

Special dial 0 ESN translations are not supported on IP Trunk 3.01 (and later) trunks because they are not leftwise-unique.

Use IP Trunk 3.01 (and later) route as first choice for Group 3 fax

The IP Trunk 3.01 (and later) gateway supports Group 3 fax modems by means of T.38 protocol.

Use the traditional PSTN for general modem traffic

General modem traffic (for example, V.36, V.90) cannot be supported on ITG. The Meridian 1/CS 1000M routing controls must be configured to route modem traffic over circuit-switched trunks instead of over IP Trunk 3.01 (and later).

Use the ESN TGAR, NCOS, and facility restriction levels to keep general modem traffic off of the IP Trunk 3.01 (and later) route. Use caution before setting TGAR=YES in the ESN block in LD 86 since this will impact all trunk access for ESN calls. New Flexible Code Restriction (NFCR) can be used to block direct access to trunk routes for stations with CLS = CTD.

Note: When adding IP Trunk 3.01 (and later) trunks to an existing Meridian 1/CS 1000M system, changes to ESN translation should be made last, after the IP Trunk 3.01 (and later) dialing plan and the entire IP Trunk 3.01 (and later) network is tested with calls dialed using the Route Access Code. In LD 16, for prompt CTYP, set to appropriate call type for the IP Trunk 3.01 (and later) node numbering plan in order to make test calls using ACOD. After the correct operation of the entire IP Trunk 3.01 (and later) network has been verified, ESN translations that are intended to be routed through IP Trunk 3.01 (and later) TIE trunks are then changed so as to use the new RLI.

Use the following overlay tables to configure ESN, Route List Block with Step Back on Congestion on ISDN, dialing plan, and Co-ordinated Dialing Plan.

LD 86 – Configure Electronic Switched Network (ESN) (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	ESN	Electronic Switched Network data block.
...		
CDP	YES	Co-ordinated Dialing Plan
...		
AC1	xx	One-or-two digit NARS/BARS Access Code 1.

LD 86 – Configure Electronic Switched Network (ESN) (Part 2 of 2)

Prompt	Response	Description
AC2	xx	One-or-two digit NARS Access Code 2.
TGAR	(NO) YES	Check for Trunk Group Access Restrictions on ESN calls. Set TGAR = YES if required to block non-fax modem traffic from the IP Trunk 3.01 (and later) route. Caution: This will impact all trunk access for ESN calls. TGAR and TARG values must be carefully coordinated for all stations, trunks, and routes when setting TGAR = YES in the ESN block.

LD 86 – Configure Route List Block with Step Back on Congestion on ISDN (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	RLB	Route List Data Block.
RLI	xxx	Route List Index to be accessed, where xxx is: 0-127 for BARS 0-255 for NARS 0-999 for FNP
ENTR	xx	Entry number for NARS/BARS Route List, where xx is: 0-63 for BARS/NARS
...		
ROUT		Route number
	0-511	Range for Large System, Call Server 1000E, and Media Gateway 1000E

LD 86 – Configure Route List Block with Step Back on Congestion on ISDN (Part 2 of 2)

Prompt	Response	Description
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
TOD		Time of Day Schedule If required, turn off IP Trunk 3.01 (and later) trunk route during peak traffic periods on the IP data network.
FRL		Facility Restriction Level Set FRL appropriately to control access to the IP Trunk 3.01 (and later) route.
DMI	0	Do not use a Digit Manipulation table in the RLB entry for the IP Trunk 3.01 (and later) route. For ESN translations that are not used for non-call-associated signalling, digit manipulation can be defined on the IP Trunk 3.01 (and later) node dialing plan in the Digits dialed tab.
SBOC		Step Back on Congestion.
	RRA	Re-route all. Enter RRA at the SBOC prompt to enable Fallback to alternate circuit-switched trunk route

Note: IP Trunk 3.01 (and later) must have SBOC=RRA for QoS fallback to work.

LD 87 – Configure the Co-ordinated Dialing Plan (CDP)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	CDP	Coordinated Dialing Plan.
TYPE	DSC TSC	Distant Steering Code. Trunk Steering Code.
...		
RLB	xx	Route List Entry created in LD 86.

LD 90 – Configure dialing plan (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	 NET	Feature. Network translation tables.
TRAN	 AC1 AC2	Translator. Access Code 1 (NARS/BARS). Access Code 2 (NARS).
TSC	 NPA NXX LOC SPN	Type of data block. Numbering Plan Area Code. Central Office Translation. ESN Location Code Translation. Special Code Translation.

LD 90 – Configure dialing plan (Part 2 of 2)

Prompt	Response	Description
...		
RLI	xxx	Route List Index created in LD 86.

Disable the Media Card 32-port and ITG-Pentium 24-port trunk cards

In order to transmit the card properties from OTM 2.1 (and later) to the Media Card 32-port and ITG-Pentium 24-port trunk cards, the IP Trunk 3.01 (and later) trunks must be in the disabled state.

To disable a Media Card 32-port and ITG-Pentium 24-port trunk card, use the following command in LD 32 or in OTM Maintenance Windows:

```
DISI l s c u
```

Wait for the system message NPR0011 to be displayed.

```
Requested pack is no longer busy and has been
disabled. Indication that the DISI L S C command
has been completed.
```

This indicates that the DISI command has been completed.

The status of the Media Card 32-port and ITG-Pentium 24-port trunk card in OTM is updated to disabled.

The IP trunk cards must be enabled later after the card properties and optionally, the IP Trunk 3.01 (and later) software, has been transmitted from OTM to the IP trunk cards.

Configure IP Trunk 3.01 (and later) data in OTM 2.1 (and later)

Before the IP Trunk 3.01 (and later) data is configured in OTM, obtain all the IP addresses for the new IP Trunk 3.01 (and later) node from the network administrator and add them to the installation summary sheet. Use an IP Trunk 3.01 (and later) Installation Summary Sheet to facilitate data entry into OTM 2.1 (and later). Obtain the node IP addresses of any existing IP Trunk 3.01 (and later) nodes in the network.

> ***Note:*** Refer to "ITG engineering guidelines" on page 125 for information on IP Trunk 3.01 (and later) IP address requirements.

An IP Trunk 3.01 (and later) node is a collection of Media Card 32-port and ITG-Pentium 24-port trunk cards in a Meridian 1/CS 1000M system for a selected customer. Each node in the IP Trunk 3.01 (and later) network has a property sheet that configures the options that apply to the node's IP trunk cards.

OTM stores the Node Properties data. This data generates the BOOTP.1 file. The data is transmitted to the Active Leader.

> ***Note:*** The bootptab file is a configuration file that downloads to the Active Leader card. It contains the list of cards and related IP and MAC addresses for the node. Bootptab is short for "bootp table". When transmitted to the IP Trunk 3.01 (and later) Active Leader IP trunk card, it is renamed "BOOTP.1".

Add an IP Trunk 3.01 (and later) node in OTM 2.1 (and later) manually

This section uses the OTM 2.1 (and later) ITG ISDN IP Trunk application to manually add and configure an IP Trunk 3.01 (and later) node and add IP trunk cards to the node. A network of multiple IP Trunk 3.01 (and later) nodes can be configured and managed from the same OTM PC. Every IP Trunk 3.01 (and later) node must first be added manually on the OTM PC and the OTM IP Trunk 3.01 (and later) configuration data must be transmitted to the IP Trunk 3.01 (and later) node during installation.

After adding a new IP Trunk 3.01 (and later) node on the OTM PC, the dialing plans for all existing IP Trunk 3.01 (and later) nodes must be manually updated to include the destination node dial plan digits entries for the new IP Trunk 3.01 (and later) node.

There are several tabs across the top of the ITG Node Properties window. The following sections describe the windows that appear when each of these tabs is clicked.

Add an IP Trunk 3.01 (and later) node and configure general node properties

Follow the steps in Procedure 17 to add an IP Trunk 3.01 (and later) node and configure general node properties.

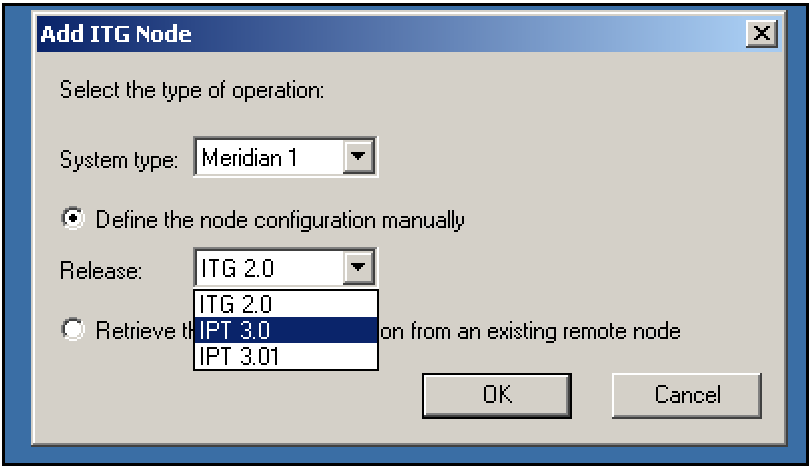
Procedure 17
Adding a node and configuring general node properties

1 Launch OTM 2.1 (and later) on the OTM PC.

2 From the **OTM Navigator** window, double-click the Services folder and double-click the **ITG ISDN IP Trunks** icon. The **IP Telephony Gateway-ISDN IP Trunk** window opens.

3 Select **Configuration > Node > Add** in the **IP Telephony Gateway – ISDN IP Trunk** window. The **Add ITG Node** window opens. See Figure 50 on page 318.

Figure 50
Add ITG Node window



Add ITG Node

Select the type of operation:

System type: Meridian 1

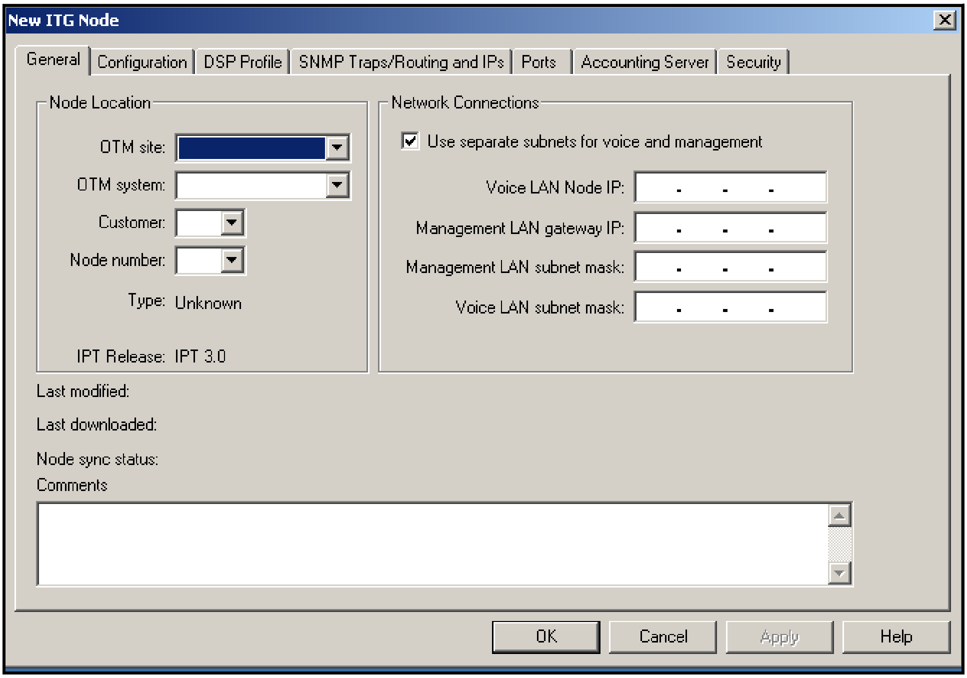
● Define the node configuration manually

Release: ITG 2.0

○ Retrieve th on from an existing remote node

4 In the **Add ITG Node** window, keep the default selections **Meridian 1** and **Define the node configuration manually**. Click **OK.** The **New ITG Node – General** window appears. See Figure 51 on page 319.

Figure 51
General tab


New ITG Node
General | Configuration | DSP Profile | SNMP Traps/Routing and IPs | Ports | Accounting Server | Security
OK
Cancel
Apply
Help

Node Location

OTM site:

OTM system:

Customer:

Node number:

Type: Unknown

IPT Release: IPT 3.0

Network Connections

☑ Use separate subnets for voice and management

Voice LAN Node IP: . . .

Management LAN gateway IP: . . .

Management LAN subnet mask: . . .

Voice LAN subnet mask: . . .

Last modified:

Last downloaded:

Node sync status:

Comments

Configure node location properties

5 Define the Node Location properties: select the **OTM site**, **OTM system**, **Customer**, and **Node number** from the drop-down lists.

Note: The site name, system name, and Customer must exist in the OTM Navigator before a new IP Trunk 3.01 (and later) node can be added.

End of Procedure

Single vs. separate TLAN and ELAN subnets

IMPORTANT!

Nortel recommends that separate TLAN and ELAN subnets be used for the IP Trunk 3.01 (and later) voice and management networks (TLAN and ELAN subnets).

Separate subnets implies the following:

- separate TLAN and ELAN network interface groups into respective Virtual LANS (VLANs) or connect them to separate Layer 2 switches
- two default gateway routers (can be the same physical Layer 3 router)

For traffic reasons, use separate subnets for nodes consisting of multiple ITG-Pentium 24-port trunk cards and Media Card 32-port trunk cards.

Refer to the Engineering Guidelines sections “Configure a system with separate subnets for voice and management” on page 212 and “Single subnet option for voice and management” on page 215.

If the single subnet option is selected, the ELAN subnet is used for the voice and management network and all voice and management data goes through the 10BaseT ELAN network interface (lnIsa0) on the motherboard of the IP trunk card.

Configure Network Connections

Follow the steps in Procedure 18 to configure the network connections.

Procedure 18
Configuring network connections

1 Decide subnet settings:

a. If using separate subnets for the voice (TLAN subnet) and management (ELAN subnet) networks, accept the default setting **Use separate subnets for voice and management** check box.

b. If using the same subnet for the voice and management network (ELAN subnet), uncheck the **Use separate subnets for voice and management** check box. The window changes.

2 If using the default setting **Use separate subnets**, perform steps a-d.

a. Enter the TLAN node IP address in the **Voice LAN Node IP address** field**.**

b. Enter the ELAN network interface gateway IP address in the **Management LAN gateway IP address** field.

c. Enter the ELAN network interface subnet mask in the **Management LAN subnet mask** field**.**

d. Enter the TLAN network interface subnet mask in the **Voice LAN subnet mask** fields

The **Voice LAN Node IP** address on the **General** tab and the **Voice IP** and **Voice LAN gateway IP** addresses for Leader 0 and Leader 1 on the **Card Configuration** tab must be on the same subnet.

3 If **Use separate subnets** was unchecked**,** perform steps a-c as follows.

a. Enter the ELAN node IP address in the **Management LAN Node IP** field**.**

b. Enter the ELAN network interface gateway IP address in the **Management LAN gateway IP address** field. The ELAN network interface gateway (router) also functions as the voice gateway (router).

c. Enter the ELAN subnet mask in the **Management LAN subnet mask** field**.**

The Management LAN Node IP and Management gateway IP addresses on the **General** tab and the **Management IP** for Leader 0, Leader 1 and all Follower cards on the card **Configuration** tab must be on the same subnet.

Note: Do not click **OK** or **Apply** until the **Configuration** tab has been completed.

End of Procedure

Configure card properties

Procedure 19 explains how to configure the IP trunk card roles, IP addresses, TN, card density and D-Channel settings.

Each IP Trunk 3.01 (and later) node requires a Leader 0 card and one DCHIP card (which can be Leader 0) and can have a Leader 1 card, one or more Follower cards, and additional DCHIP cards (which can be Leader 1 or Follower cards). Either Leader 0 or Leader 1 can have the Active Leader status. On system power-up, Leader 0 normally functions as the Active Leader and Leader 1 as the Backup Leader.

At other times, the Leader card functions can reverse with Leader 1 working as the Active Leader and Leader 0 working as the Backup Leader.

Procedure 19
Configuring the IP trunk card

1 Click the **Configuration** tab. See Figure 52 on page 323. If the single subnet option in the **General** tab was selected earlier, the Voice IP and Voice LAN gateway IP fields are greyed-out.

2 Select the **Card role** from the drop-down list.

When adding the first card, select the card role **Leader 0**. When adding the second card, select the card type **Leader 1**. When adding additional cards, select the card type **Follower**. Configure the DCHIP and D-Channel information.

3 If **Use separate subnets** in the **General** tab was checked earlier, perform steps a-d.

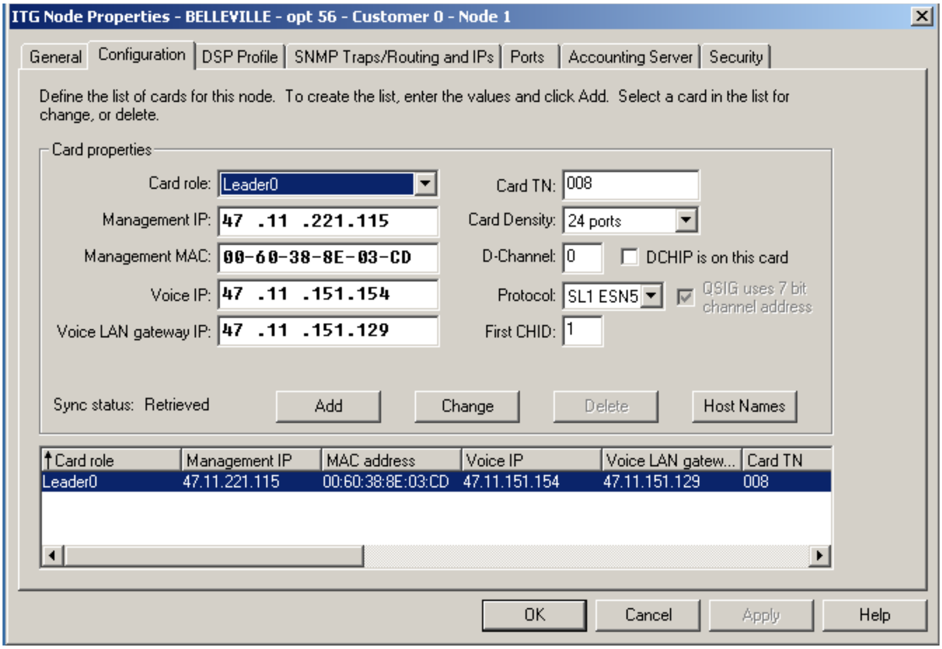
a. Enter the **Management IP** address (ELAN network interface IP address).

b. Enter the **Management MAC address** (ELAN network interface MAC address). It is the motherboard Ethernet address. Find it on the faceplate label of the card currently being configured. It is also identified as lnIsa0 on the card startup messages and by the **ifShow** command in the ITG shell.

c. Enter the **Voice IP address** (TLAN network interface IP address). See Notes 1 and 2.

d. Enter the **Voice LAN gateway IP address**. (TLAN network interface gateway IP address), See Notes 1 and 2.

Figure 52
Configuration tab



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

Card role: Leader0
Management IP: 47 .11 .221.115
Management MAC: 00-60-38-8E-03-CD
Voice IP: 47 .11 .151.154
Voice LAN gateway IP: 47 .11 .151.129
Card TN: 008
Card Density: 24 ports
D-Channel: 0 □ DCHIP is on this card
Protocol: SL1 ESN5 ☑ QSIG uses 7 bit channel address
First CHID: 1

Sync status: Retrieved

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008

Note 1: The TLAN Node IP address on the **General** tab and the TLAN network interface IP address and TLAN network interface gateway IP addresses for Leader 0 and Leader 1 on the **Card Configuration** tab must be on the same TLAN subnet.

Note 2: Each Follower card can optionally have its TLAN network interface IP address and TLAN network interface gateway IP address on a different TLAN subnet than Leader 0 and Leader 1.

4 If **Use separate subnets** in the **General** tab was unchecked earlier**,** perform steps a and b:

a. Enter the **Management IP** address (ELAN network interface IP address).

b. Enter the **Management MAC** address ELAN network interface MAC address). It is the motherboard Ethernet address. Find it on the faceplate label of the IP trunk card currently being configured. It is also identified as lnIsa0 on the card startup messages and by the **ifShow** command in the ITG shell.

The TLAN Node IP and ELAN network interface gateway IP addresses on the **General** tab and the ELAN network interface IP address for Leader 0, Leader 1 and all Follower cards on the **Card Configuration** tab must be on the same ELAN subnet.

5 Enter the **Card TN**. For Large Systems, the card TNs are validated for loop, shelf and card separated by dashes. For Small Systems, only the card number is required.

6 Select the **Card Density** from the drop-down list: 24 ports for an ITG-P 24-port card; 32 ports for the Media Card.

7 Enter the ISL **D-channel** logical device number. The range is 0 – 255 for Large Systems; 0 – 79 for Small Systems.

8 If the card will be a DCHIP card, select the **DCHIP is on this Card** check box. The DCHIP card must have an NTWE07AA DCHIP PC Card with an NTCW84EA Pigtail cable installed and must be connected to the ISL DCH port on the MSDL or SDI/DCH card.

Note: The standard configuration is to put the first DCHIP PC Card on Leader 1 and additional DCHIP PC cards on Follower cards.

9 Select a **Protocol** for the DCHIP card from the drop-down list. The protocol selected must match the protocol configured in LD 16 in the Route Data Block at the IFC prompt with respect to SL1, or ESGF/ISGF QSIG interface (IFC), and in LD 17 at the IFC prompt under ADAN DCH.

In LD 16, if SIGO is set to STD, select the SL1 protocol. If SIGO is set to ESN5, select SL1 ESN5 protocol. In a mixed ESN5 and non-ESN5 network, configure an ESN5 prefix for the non-ESN5 IP telephony gateways by using the **esn5PrefixSet** command from the ITG shell CLI. See “Change default ESN5 prefix for non-ESN5 IP telephony gateways” on page 360.

The choices are SL1, SL1 ESN5, ESIG and ISIG for networks consisting of Large Systems. For networks that include Small Systems, the choices are SL1 or SL1 ESN5.

In addition to IP Trunk 3.01 (and later) nodes, the IP telephony trunk network might also contain ITG Trunk 1.0 Basic Trunk nodes or Nortel IP Telephony Connection Manager. Use H.323 V2 node capability for these nodes.

Once a DCHIP for the IP Trunk 3.01 (and later) node is defined, the protocol field is greyed out when other cards in the same IP Trunk 3.01 (and later) node are selected.

Note: The **QSIG** checkbox enables IP Trunk 3.01 to be configured with a QSIG channel address length of 7 bits for Primary Rate D-Channels or 8 bits for an ISL D-Channel used in prior releases of IP Trunk software. The **QSIG** checkbox is checked or unchecked by default, depending on the software release running on the system. The checkbox is enabled only when the selected protocol is QSIG (ESGF or ISGF) and the node version is IP Trunk 3.01.

10 Enter the **First CHID** (Channel ID) for this IP trunk card in the First CHID edit box. The First CHID range is:

- 1 – 382 for the NT0961AA ITG-Pentium 24-port trunk card
- 1 – 382 for the NTVQ90BA Media Card 32-port trunk card

The First CHID is the ISL Channel ID of Unit 0 on this IP trunk card, as configured in LD 14 for the IP trunk cards and units. Consecutive CHIDs are assigned to remaining units on the card when configuring trunks in LD 14 using the **NEW xx** command.

11 Click **Add** and then click **Apply**.

Note: In most cases, do not click OK until all cards are added to the IP Trunk 3.01 (and later) node and all configuration tasks completed. If OK is clicked before completing configuration, OTM exits the node property configuration session and displays the **IP Telephony Gateway – ISDN IP Trunk** window. To complete the configuration tasks, double-click the new IP Trunk 3.01 (and later) node in the list in the upper part of the window.

12 Repeat steps 1 – 10 for Leader 1 and each Follower in the IP Trunk 3.01 (and later) node.

End of Procedure

Configure DSP profiles for the IP Trunk 3.01 (and later) node

Follow the steps in Procedure 20 to select a DSP profile, set Profile Options and Codec Options and, if required, modify default DiffServ/TOS values from 0. Set these profiles once for the IP Trunk 3.01 (and later) node. In a later step, download the DSP profiles card properties to each card.

Procedure 20
Configuring DSP profiles for the IP Trunk 3.01 (and later) node

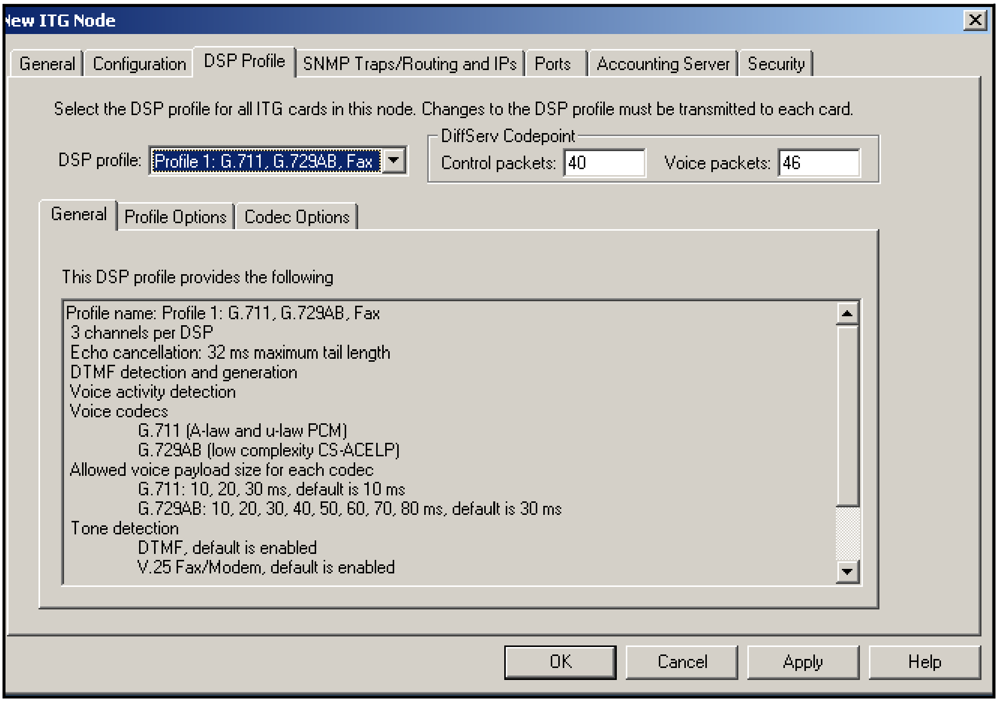
1 Click the **DSP Profile** tab. See Figure 53 on page 327. The **General** tab displays a detailed description of the default DSP Profile 1.

2 Change the default **DSP profile** from the drop-down list, if required. There are three DSP profiles. Each profile contains two or more codecs. All IP trunk cards in the same node share the same DSP profile.

CAUTION

The default DSP profile is Profile 1, which is appropriate for most applications. Only an expert in VoIP should modify the default DSP profile. See “IP Trunk 3.01 (and later) DSP profile settings” on page 222.

Figure 53
DSP Profile – General tab



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint

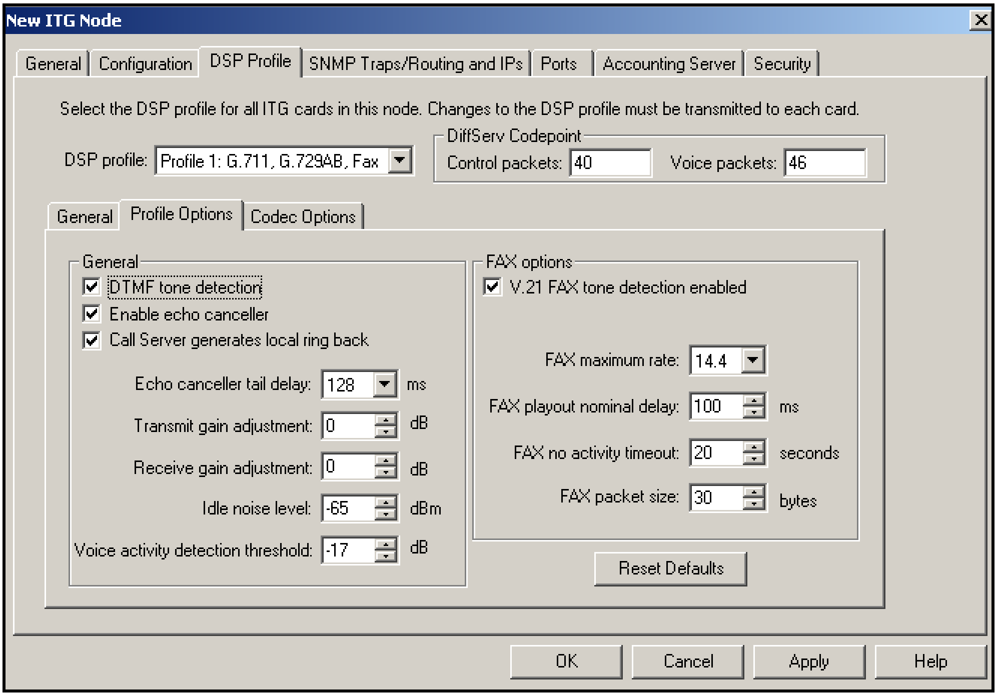
Control packets: 40 Voice packets: 46

This DSP profile provides the following

Profile name: Profile 1: G.711, G.729AB, Fax
3 channels per DSP
Echo cancellation: 32 ms maximum tail length
DTMF detection and generation
Voice activity detection
Voice codecs
G.711 (A-law and u-law PCM)
G.729AB (low complexity CS-ACELP)
Allowed voice payload size for each codec
G.711: 10, 20, 30 ms, default is 10 ms
G.729AB: 10, 20, 30, 40, 50, 60, 70, 80 ms, default is 30 ms
Tone detection
DTMF, default is enabled
V.25 Fax/Modem, default is enabled

3 Click the **Profile Options** tab. See Figure 54 on page 328. This tab displays the default **General** and **FAX options** values according to the selected DSP profile.

Figure 54
DSP Profile – Profile Options tab



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40 Voice packets: 46

General
☑ DTMF tone detection
☑ Enable echo canceller
☑ Call Server generates local ring back

Echo canceller tail delay: 128 ms
Transmit gain adjustment: 0 dB
Receive gain adjustment: 0 dB
Idle noise level: -65 dBm
Voice activity detection threshold: -17 dB

FAX options
☑ V.21 FAX tone detection enabled

FAX maximum rate: 14.4
FAX playout nominal delay: 100 ms
FAX no activity timeout: 20 seconds
FAX packet size: 30 bytes

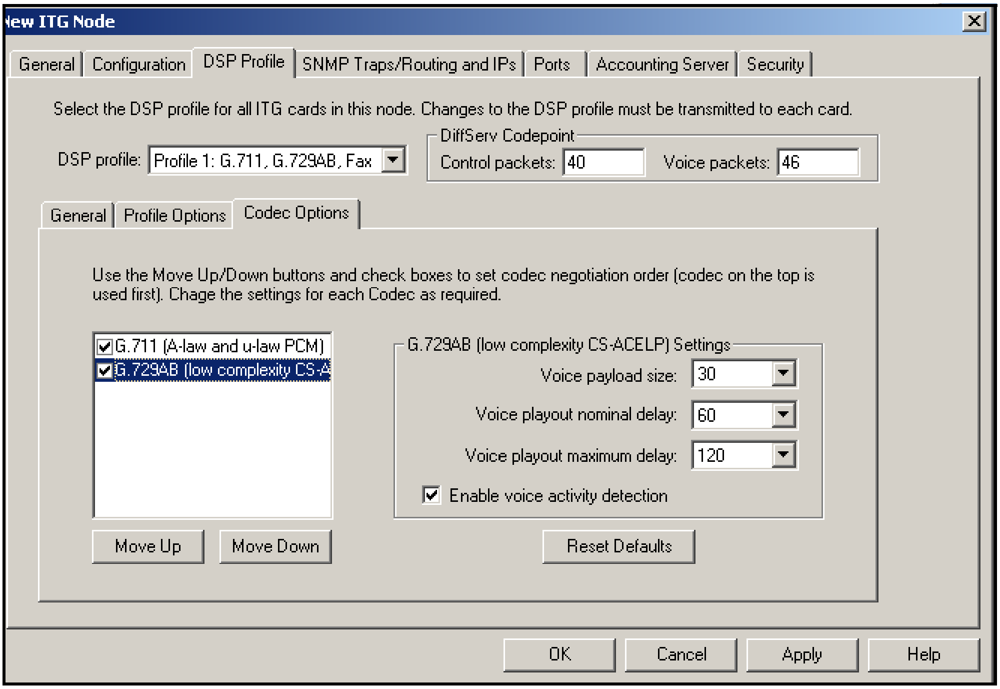
4 Change the **General** and **FAX option** parameters, if required. To revert to the default settings, click **Reset Defaults**.

CAUTION

The default DSP Profile Option settings for each codec are appropriate for most applications. Only an expert in VoIP should modify the Profile Options parameters. See “IP Trunk 3.01 (and later) DSP profile settings” on page 222.

5 Click the **Codec Options** tab. See Figure 55 on page 329. This tab displays the default order of the preferred codec selection for outgoing calls and shows advanced codec parameters for the selected codec.

Figure 55
DSP Profile – Codec Options tab



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40
Voice packets: 46

Use the Move Up/Down buttons and check boxes to set codec negotiation order (codec on the top is used first). Chage the settings for each Codec as required.

☑ G.711 (A-law and u-law PCM)
☑ G.729AB (low complexity CS-A

G.729AB (low complexity CS-ACELP) Settings
Voice payload size: 30
Voice playout nominal delay: 60
Voice playout maximum delay: 120
☑ Enable voice activity detection

6 Perform steps 7 and 8 if required. To revert to the default settings, click **Reset Defaults**.

CAUTION

The default Codec Options are appropriate for most applications. Only an expert in VoIP should modify the Codec Options parameters. See “IP Trunk 3.01 (and later) DSP profile settings” on page 222.

7 To turn off a codec, click the codec and uncheck the checkbox.

8 To change the preferred order of codec selection, for outgoing calls, if required, select the codec and click the **Move Up** and **Move Down** buttons. The IP Trunk 3.01 (and later) node requests the codec at the top of the list first on outgoing calls.

9 To enable Voice Activity Detection (VAD) for Silence Suppression, check the appropriate box. To disable VAD for Silence Suppression, uncheck the box.

End of Procedure

Change default DiffServ/ToS value for Control and Voice

Follow the steps in Procedure 21 to change the default DiffServ/ToS value for Control and Voice.

Procedure 21
Changing the default DiffServ Codepoint (DSCP) value for Control and Voice

1 Enter the **DSCP** value for **Control packets** and **Voice packets**, if required, to obtain better QoS over the IP data network (LAN/WAN). Do not change from default value of 0 unless instructed by IP network administrator.

The DSCP determines the priority of the control and voice packets in the network router queues. The values entered in these two boxes must be coordinated across the entire IP data network. Do not change them arbitrarily.

DSCP values must first be converted to a decimal value of the DiffServ/TOS byte in the IP packet header. For example, the 8-bit TOS field value of 0010 0100 which indicates “Precedence = Priority”; “Reliability = High” is converted to a decimal value of 36 before being entered in the Control or Voice fields.

2 Click **Apply**.

End of Procedure

Configure SNMP Traps/Routing and IP addresses tab

In this procedure, a maximum of eight SNMP Trap destination IP addresses and subnet masks and a maximum of eight Card Routing Table Entry IP addresses and subnet masks can be defined. These SNMP Trap and Card Routing table settings become active when the IP trunk card properties are transmitted to the IP trunk cards.

The IP trunk card assumes that the SNMP traps are sent through the ELAN subnet, since there is no SNMP Gateway address configured in OTM 2.1 (and later). If the SNMP traps are to be sent through the ELAN subnet, then there will be no problem However, if the OTM 2.1 (and later) workstation is on the TLAN subnet, SNMP traps might not reach the OTM PC. This is because the provisioned subnet of the SNMP client, based on the IP address and subnet mask, defaults the traps to be sent to the ELAN router. The only way SNMP traps can be sent to the TLAN subnet is if the SNMP client subnet is the same as the IP trunk card TLAN subnet.

Example:
SNMP IP = 23.11.42.52
Subnet mask = 255.255.255.0
Subnet = 23.11.42.0

IP Trunk card TLAN IP = 23.11.42.121
Subnet mask = 255.255.255.0
Subnet = 23.11.42.0

23.11.42.0 = 23.11.42.0.
Therefore, the SNMP traps will be sent to the TLAN router.

WARNING

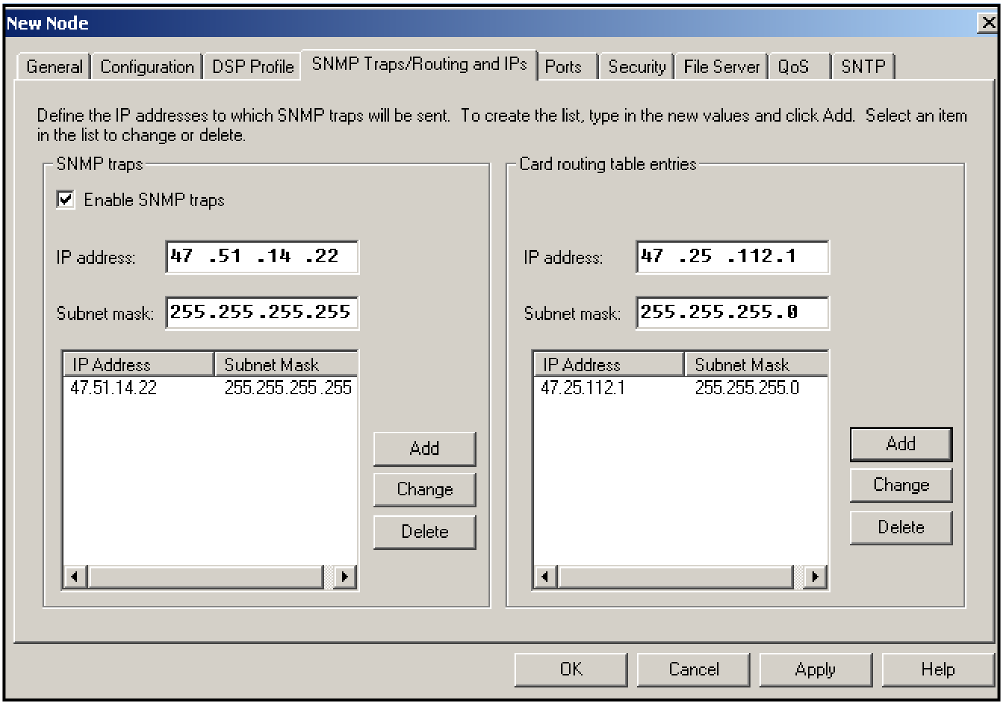
Nortel recommends the SNMP client (that is, the OTM 2.1 [and later] PC) **not** be put on the TLAN subnet.

Placing the OTM PC on the ELAN subnet is a more secure configuration. Additionally, incorrectly configuring the SNMP trap IP address can adversely affect routing on the IP trunk card, which can prevent the IP trunk card from sending or receiving calls.

Procedure 22
Configuring SNMP Traps/Routing and IP addresses tab

1 Click **SNMP Traps/Routing and IPs** tab. See Figure 56.

Figure 56
SNMP trap addresses/Routing table IP addresses tab



Define the IP addresses to which SNMP traps will be sent. To create the list, type in the new values and click Add. Select an item in the list to change or delete.

SNMP traps

☑ Enable SNMP traps

IP address: 47 .51 .14 .22

Subnet mask: 255.255.255.255

IP Address	Subnet Mask
47.51.14.22	255.255.255.255

Card routing table entries

IP address: 47 .25 .112.1

Subnet mask: 255.255.255.0

IP Address	Subnet Mask
47.25.112.1	255.255.255.0

2 Check the **Enable SNMP traps** check box to enable sending of SNMP traps to the SNMP trap destinations that appear in the list. Enter at least one SNMP trap destination IP address if this option is checked. The SNMP trap destination IP addresses determine where event and alarm messages are sent

Refer to “Configure OTM Alarm Management to receive SNMP traps from the IP trunk cards” on page 367 to configure OTM Alarm Notification to monitor SNMP traps for IP trunk cards.

3 Enter the SNMP trap destination IP address in the IP Address field.

4 The subnet mask for the IP address of the trap destination must **always** be configured as 255.255.255.255.(This subnet mask configuration forces a host route entry).

WARNING

Do not enter the actual value of the subnet mask on the network interface of the SNMP trap destination. Doing so can cause misrouting of RTP media and signaling, leading to no speech path between the IP Phones and the cards.

5 Click **Add**. The new IP address and subnet mask appears in the SNMP Manager IP address list.

Enter SNMP trap destination IP addresses for OTM PCs on local and remote subnets and any other SNMP manager PCs for alarm monitoring:

- local or remote OTM PC
- PPP IP address configured in the router on the ELAN subnet for the remote support OTM PC
- SNMP manager for remote alarm monitoring

Note: All OTM PCs must have the Alarm Notification feature.

Note: Up to eight SNMP trap destinations can be defined.

In the next step, add the SNMP trap IP addresses for remote subnets in the Card Routing Table entries IP address field.

6 Configure the **Card routing table entries.**

Enter the IP address and subnet mask for management hosts on remote subnets, such as SNMP manager, Radius accounting server, Management PC, Telnet and FTP clients. Click **Add**. In a later step, this information is transmitted to each IP trunk card.

The IP trunk card uses the addresses in the routing table entries to route signaling packets over the ELAN network interface gateway (router) on the ELAN subnet. Without routing table entries, the IP trunk card routes signaling traffic over the TLAN network interface gateway. Sending signaling traffic over the TLAN subnet can affect voice quality.

7 Click **Apply**.

8 Click **OK** to exit the window.

9 To transmit the information to the node, from the menu select **Configuration > Synchronize > Transmit**.

End of Procedure

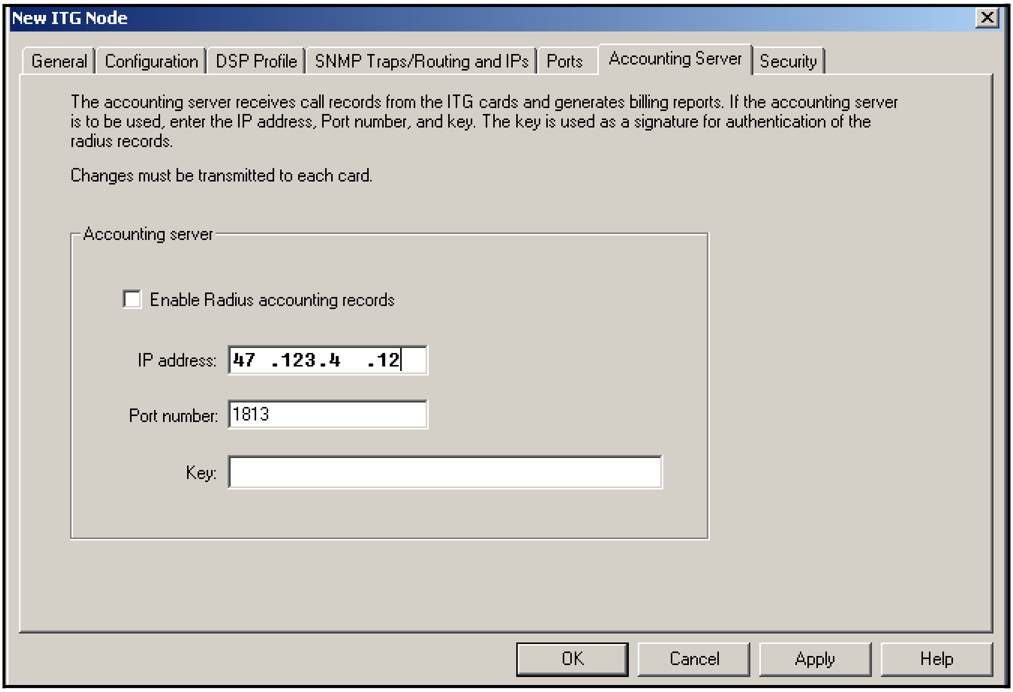
Configure Accounting server

If a Radius Accounting Server is not used, skip this step. A Radius Accounting Server collects call records from the IP trunk cards and generates billing reports. Follow the steps in Procedure 23 on page 336 to configure a Radius Accounting Server.

Procedure 23
Configuring a Radius Accounting Server

1 Click the **Accounting Server** tab. See Figure 57.

Figure 57
Accounting Server tab



The accounting server receives call records from the ITG cards and generates billing reports. If the accounting server is to be used, enter the IP address, Port number, and key. The key is used as a signature for authentication of the radius records.

Changes must be transmitted to each card.

Accounting server

□ Enable Radius accounting records

IP address: 47 .123.4 .12

Port number: 1813

Key:

2 Click the **Enable Radius accounting records** checkbox.

3 Enter the Radius accounting server IP address. Add the same Accounting Server IP address that was configured in the Card Routing Table entries as discussed in “Configure SNMP Traps/Routing and IP addresses tab” on page 331.

4 Change the default port number from the default (1813), if required.

5 Enter the key. The key is a signature for authentication of the Radius records. It can be a maximum of 64 alpha-numeric characters.

6 Click **Apply**.

End of Procedure

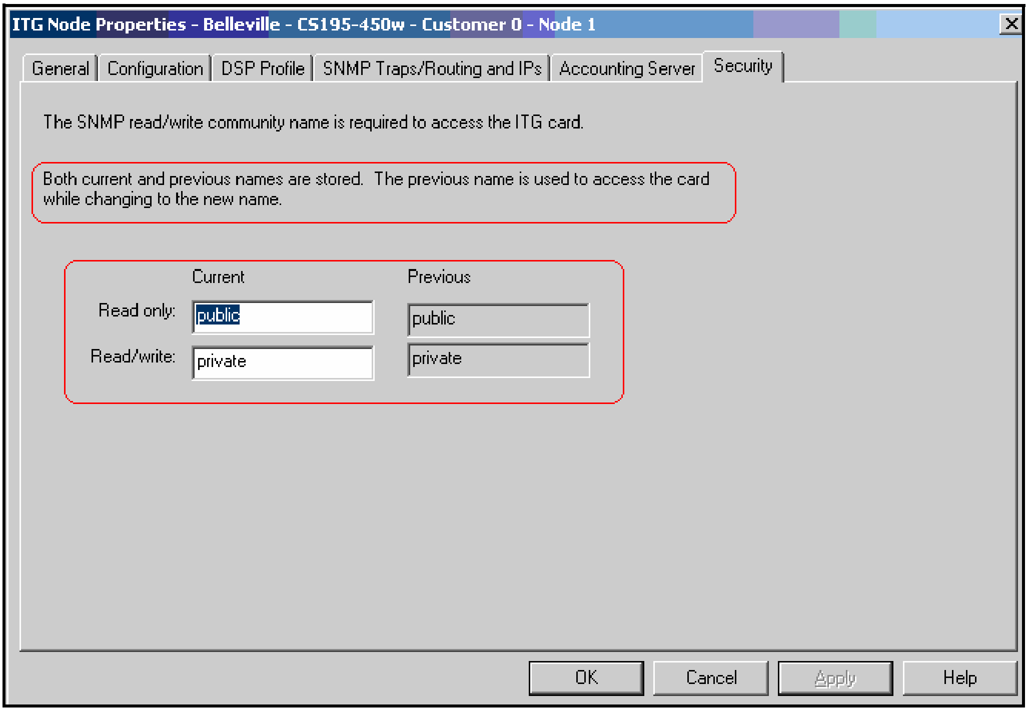
Control node access with SNMP community name strings

Change the SNMP community name strings to control access to the IP Trunk 3.01 (and later) node. OTM uses the community name strings to refresh the IP Trunk 3.01 (and later) node and card status and to control the transmitting and retrieving of files for database synchronization.

> ***Note:*** To retrieve the community names if forgotten, connect a TTY to the IP trunk card maintenance port. Restart the IP trunk card. The IP trunk card displays the community name on the TTY during startup.

The community name strings are configured on the Security tab. These are not picked up from the System Properties – General tab.

Figure 58
Node Properties – Security tab



ITG Node Properties - Belleville - CS195-450w - Customer 0 - Node 1
General
Configuration
DSP Profile
SNMP Traps/Routing and IPs
Accounting Server
Security

The SNMP read/write community name is required to access the ITG card.

Both current and previous names are stored. The previous name is used to access the card while changing to the new name.

	Current	Previous
Read only:	public	public
Read/write:	private	private

Change the current System Mgmt Read and System Mgmt Read/Write community name strings as per the Card. OTM uses the previous read/write community name to transmit the card properties. The first time data is transmitted after changing the password, OTM uses the previous read/write password. OTM uses the changed password for all following data transmissions.

End of Procedure

For more information on SNMP, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

Exit node property configuration session

The procedure to add an IP Trunk 3.01 (and later) node manually in OTM is complete. Click **OK** to save the node and card properties configuration and exit. OTM displays the IP Telephony Gateway - ISDN IP Trunk window. If a network of IP Trunk 3.01 (and later) nodes is to be managed from this OTM PC, add the remaining IP Trunk 3.01 (and later) nodes before configuring the dialing plan for the new IP Trunk 3.01 (and later) nodes on OTM.

Create the IP Trunk 3.01 (and later) node dialing plan using OTM

Follow the steps in Procedure 24 on page 340 to configure the IP Trunk 3.01 (and later) node dialing plan in OTM. Use this procedure to create the dialing plan for the first node in the network. This procedure also can be used to create a dialing plan for a new node in a very small network. If adding a new node to a large existing network, it is more efficient to retrieve the IP Trunk 3.01 (and later) node dialing plan from an existing node.

A dialing plan consists of a number of IP Trunk 3.01 (and later) destination nodes and one or more dialing plan entries for each destination node. Select a destination node, define the destination node protocol capability, decide if QoS monitoring is to be enabled for this destination node, and enter one or more ESN dialing plan entries for each destination node. Repeat this procedure for all destination nodes in the IP Trunk 3.01 (and later) network.

The dialing plan information entered in OTM must match the ESN data entered in the LD 15, LD 16, LD 86, LD 87 and LD 90. Keep the dialing plan entries consistent between the Meridian 1/CS 1000M and the IP Trunk 3.01 (and later) node. Transmit the dialing plan from OTM to the IP Trunk 3.01 (and later) node during installation, card replacement, when IP Trunk 3.01 (and later) nodes are added to the network, or whenever the dialing plan on OTM IP Trunk 3.01 (and later) is changed.

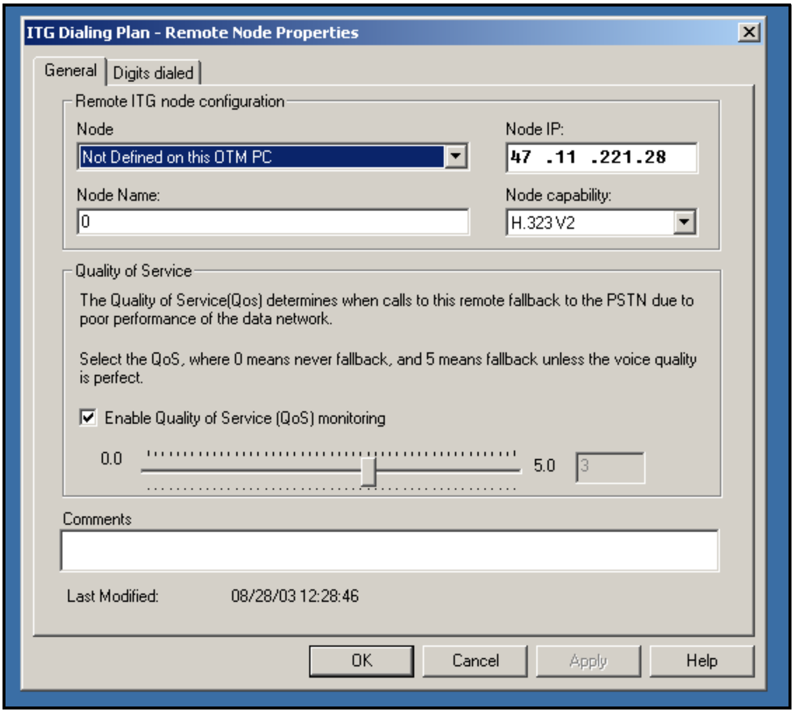
Each IP Trunk 3.01 (and later) trunk node shares one dialing plan for all cards in the node. The IP Trunk 3.01 (and later) node dialing plan translates the dialed digits in the system ISDN Signaling Call Setup message, according to ESN translation type, into the Node IP addresses of the IP Trunk 3.01 (and later) destination nodes.

Procedure 24
Configure the ITG Dialing Plan – General tab

1 In the **IP Telephony Gateway – ISDN IP Trunk** window, select the new IP Trunk 3.01 (and later) node for which a dialing plan is to be built. Select menu **Configuration > Node > Dialing Plan**. The **ITG Dialing Plan** window opens.

2 In the **ITG Dialing Plan** window, select the menu **Configuration > Add Remote Node.** The **ITG Dialing Plan – Remote Node Properties** window opens and displays the **General** tab. See Figure 59. The default **Node** drop-down list reads “Not defined on this OTM PC” and the Node IP address field is blank. Click the drop-down list to see a list of all the other IP Trunk 3.01 (and later) nodes configured on this OTM PC. The IP Trunk 3.01 (and later) node for which the dialing plan is being created is not seen.

Figure 59
ITG Dialing Plan Remote Node Properties window – General tab



ITG Dialing Plan - Remote Node Properties

Remote ITG node configuration

Node: Not Defined on this OTM PC

Node IP: 47 .11 .221.28

Node Name: 0

Node capability: H.323 V2

Quality of Service

The Quality of Service(Qos) determines when calls to this remote fallback to the PSTN due to poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments

Last Modified: 08/28/03 12:28:46

3 Select the destination **Node** to be added from the list. OTM provides the IP Trunk 3.01 (and later) **Node IP** address in a greyed-out box and fills in the node name in the Node Name field.

4 Define **Node capability** for the destination node.

The default setting is **SL1**, which supports MCDN features. The Node capability field defines the D-channel protocol used by the destination IP Trunk 3.01 (and later) node. The protocol must match the protocol configured in LD 16 in the Route Data Block at the IFC prompt with respect to SL1 vs. ESGF or ISGF QSIG interface (IFC), and in LD 17 at the IFC prompt under ADAN DCH. In LD 16, if SIGO is set to STD, then select the SL1 node capability. If SIGO is set to ESN5, then select SL1ESN5 node capability. In a mixed ESN5 and non-ESN5 network, configure an ESN5 prefix for the non-ESN5 IP telephony gateways by using the "esn5PrefixSet" command from the ITG shell CLI. See "Change default ESN5 prefix for non-ESN5 IP telephony gateways" on page 360.

The choices are SL1, SL1 ESN5, ESIG, and ISIG for networks consisting of Large Systems. For networks that include Small Systems, the choices are H.323 V2, ISGF, ESGF, SL1, and SLI ESN5.

New for IP Trunk 3.01 (and later), the node capability choices also include "CS 1000S". This is for testing purposes between IP Trunk 3.01 (and later) and a CS 1000S endpoint.

In addition to IP Trunk 3.01 (and later) nodes, the IP telephony trunk network may contain ITG Trunk 1.0 Basic Trunk nodes or Nortel IP Telephony Connection Manager. Use H.323 V2 node capability for these nodes.

Quality of Service section

The default setting enables Quality of Service (QoS) monitoring. QoS monitoring allows new calls to fallback to alternate circuit-switched trunk routes when the IP network QoS falls below the configured threshold. If the default setting is changed and QoS monitoring is disabled, then the IP Trunk 3.01 (and later) node attempts to complete new calls over the IP network regardless of the IP network QoS. There can still be alternate routes, but IP Trunk 3.01 (and later) only uses them if the D-Channel connection to the local IP Trunk 3.01 (and later) node fails, if the destination node fails to respond, or if the destination node responds that all trunks are busy.

5 To disable QoS monitoring of a destination node, uncheck the **Enable Quality of Service (QoS) monitoring** checkbox.

6 Slide the Quality of Service control bar to set the QoS level. The default setting is 3 (=Good).

See “E-Model” on page 108 and Table 34 on page 206 for more details on QoS levels and MOS values.

End of Procedure

Configure Digits dialed tab

Follow the steps in Procedure 25 to configure the Digits dialed tab. Use the Digits dialed tab to configure one or more ESN translations for the current destination node. Figure 60 on page 343 shows the Dialed Digits tab fields.

Procedure 25
Configuring the Digits dialed tab

1 Click the **Digits dialed** tab.

OTM displays the **Digits dialed** tab.

2 Select the ESN translation type from the **Dial Plan** drop-down list. Add every ESN translation configured for this destination node in the ESN (LD 86, LD 87 and LD 96) one at a time.

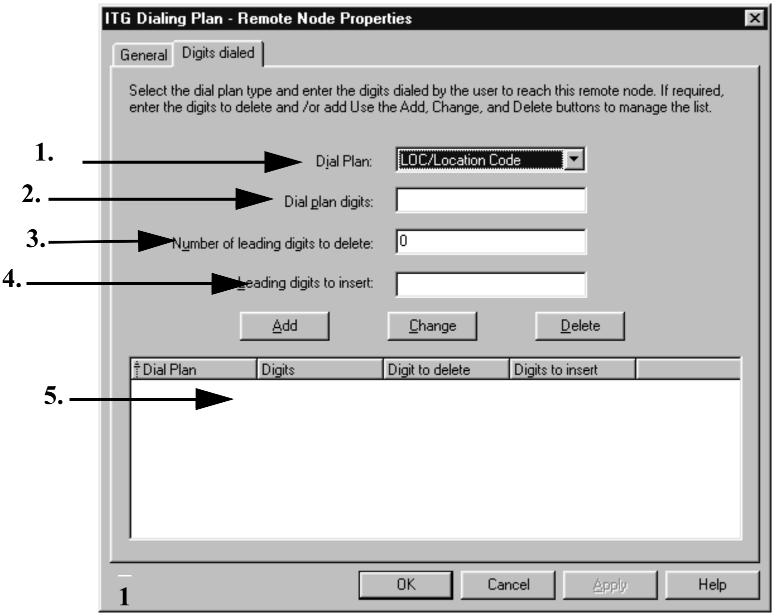
3 Enter the Called Number digits for the ESN translation type in the **Dial plan digits** field. See #2 in Figure 60 on page 343.

Note: The digits must be leftwise unique within the ESN translation types that correspond to given pair of NPI and TON values. Every ESN translation type generates a unique pair of NPI and TON values by default. The default values can be manipulated in the ESN digit manipulation tables. The CTYP in the route data block defaults to Unknown (UKWN).

Note: Two sets of digits are “leftwise unique” if one set of digits is not identical to the leading digits of the second set of digits. For example, 011 and 0112 are not leftwise unique; 011 and 012 are leftwise unique.

4 Enter the number of leading digits to delete or insert, if required, for digit manipulation on outgoing calls using this ESN translation to this destination node.

Figure 60
ITG Dialing Plan Remote Node Properties window – Digits dialed tab



ITG Dialing Plan - Remote Node Properties

General | Digits dialed

Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: LOC/Location Code

Dial plan digits:

Number of leading digits to delete: 0

Leading digits to insert:

Add | Change | Delete

Dial Plan	Digits	Digit to delete	Digits to insert

OK | Cancel | Apply | Help

1

.

Dial Plan – Click the pull-down list to display ESN translation types/ISDN call types.

2. **Dial plan digits** – Dial plan digits are the Called Number digits in the ISDN Signalling Call Setup message sent by the Meridian 1/CS 1000M system after digit absorption, insertion, and manipulation by the system

3. **Number of leading digits to delete** – The number of leading digits to delete from the Called Number digits in the Call Setup message sent by Meridian 1 before the IP trunk card sends the Call Setup message on outgoing calls.

4. **Leading digits to insert -** The leading digits to insert before the ITG Trunk card sends the Call Setup message on outgoing calls.

Note 1: The digit manipulation defined in the Digits dialed tab of the **ITG Dialing Plan – Remote Node Properties** window does not apply to the Destination Number of the Facility messages for non-call-associated signalling for MCDN features. These features include: NRAG, NMS, NACD, and NAS.

Note 2: Digit manipulation in the Digits dialed tab can be used as required for destination nodes with node capability H.323 V2, and also for destination nodes with node capability SL1, SL1 ESN5, ESGF, or ISGF for ESN translation Dial Plan digits that are not used for non-call-associated signalling.

5 To add the ESN translation Dial Plan digits for this destination node, click **Add**.

6 Click **Apply**.

7 Repeat steps 7 through 11 until all the ESN translation Dial Plan digits for this destination node have been added.

8 Click **OK**.

The **Dialing Plan** window appears with the added dialing plan entries.

9 Repeat steps 2 through 13 until dialing plan entries for all the destination nodes in the drop down list and all destination nodes Not Defined on this OTM PC have been added.

End of Procedure

Retrieve the IP Trunk 3.01 (and later) node dialing plan using OTM

If adding a new node to a large existing network, it is more efficient to retrieve the IP Trunk 3.01 (and later) node dialing plan from an existing node. Make the necessary modifications before transmitting the dialing plan to the new node. Follow the steps in Procedure 26 to retrieve the IP Trunk 3.01 (and later) node dialing plan.

Important

When OTM 2.1 (and later) is launched, it launches its own FTP service. Other FTP services, such as those found in Windows NT4 and Windows 2000 (which are launched by default) must be turned off, or OTM 2.1 (and later) will not work properly.

Procedure 26
Retrieving the IP Trunk 3.01 (and later) node dialing plan using OTM

1 In the **IP Telephony Gateway – ISDN IP Trunk** window, select an existing IP Trunk 3.01 (and later) node which has a dialing plan similar to one to be created for the new IP Trunk 3.01 (and later) node.

2 Ensure that OTM can monitor the card state of Leader 0 in the existing node from which the dialing plan is being retrieved. Record the Management IP address of Leader 0 on the existing node.

3 Select the new node and double-click to open its Node Properties sheet.

4 Click the **Configuration** tab. Record the Management IP address of Leader 0 on the new node.

5 On the **Configuration** tab, change the Management IP address of Leader 0 on the new node. Enter the Management IP address of the Leader 0 card on the existing node recorded in Step 2.

6 Click **Change** and then click **OK**.

7 Select the new node in the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window.

8 Select menu **Configuration > Synchronize > Retrieve** to open the **ITG Retrieve Options** window.

9 Check only the **Dialing Plan** check box if the community name for both the existing and new nodes is the same.

Check the **Dialing Plan** check box and the **Prompt user for community name** check box if the community name for both the existing and new nodes are different. A dialog box appears. Enter the new node's community name.

10 Click **Start Retrieve** and monitor progress in the Retrieve control field. Ensure the dialing plan is retrieved successfully and added to the OTM database.

11 Click **Close** to close the **ITG Retrieve Options** window and return to the **IP Telephony Gateway - ISDN IP Trunk** window.

12 Select the new node and double-click to open its Node Properties sheet.

13 On the **Configuration** tab, change the Management IP address of Leader 0 on the new node. Enter the correct Management IP address of the Leader 0 card on the new node.

14 Click **Change** and then click **OK**.

15 Select menu **Configuration > Node > Dialing Plan** to open the **ITG Dialing Plan** window.

16 Inspect the retrieved dialing plan for the new node and make any necessary modifications. Double-click a dialing plan entry to inspect its property sheet. To save modifications, click **Apply** and then **OK**.

From the **View** menu, the option is available to view by **Digits dialed** or **Remote Nodes**.

End of Procedure

Transmit IP trunk card configuration data from OTM 2.1 (and later) to the IP trunk cards

IP Trunk 3.01 (and later) nodes and IP trunk cards are configured in the OTM ITG ISDN IP Trunk application and then transmitted to the IP trunk cards. The configuration data is converted by OTM to text files. The IP trunk cards then obtain the configuration files from OTM using an FTP server on OTM 2.1.

Important

When OTM 2.1 (and later) is launched, it launches its own FTP service. Other FTP services, such as those found in Windows NT4 and Windows 2000 (which are launched by default) must be turned off, or OTM 2.1 (and later) will not work properly.

Before configuration data is transmitted

Perform the following procedures in any order before transmitting configuration data:

- Install the IP trunk cards in the system IPE modules or cabinets and cable them to the TLAN and ELAN Ethernet hubs, Ethernet Layer 2/Layer 3 switches, and IP routers.
- Configure the IP Trunk 3.01 (and later) data in the system. Disable the IP trunk cards in LD 32.
- Configure the IP Trunk 3.01 (and later) data in OTM 2.1 (and later).
- Connect a local RS-232 terminal to the serial maintenance port to configure the Leader 0 IP address. Under certain conditions, the local terminal is required to configure IP routing table entries in the Leader 1 IP trunk card and each of the Follower cards.
- Connect the OTM PC to the local ELAN subnet or to a remote subnet across the LAN/WAN from a remote subnet.

Configure the Leader 0 IP address

Follow the steps in Procedure 27 to configure the IP address of the Leader 0 IP trunk card, using the ITG shell Command Line Interface (CLI).

Procedure 27
Configure the Leader 0 IP address

1 To access the ITG shell, connect an OTM 2.1 (and later) PC to the RS-232 serial maintenance port on the faceplate of the Leader 0 IP trunk card through an NTAG81CA PC Maintenance cable. If required, use an NTAG81BA Maintenance Extender cable to provide an extension between the NTAG81CA PC Maintenance cable and the OTM 2.1 (and later) PC.

Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTCW84KA Management Port, DCH, and Serial I/O cable for DCHIP cards, or the NTMF94EA ELAN, TLAN, RS-232-ports cable for non-DCHIP cards, to create a more permanent connection to the IP trunk card serial maintenance port.

Note: Never connect two terminals to the faceplate and I/O panel breakout cable serial maintenance port connectors at the same time.

2 Use the following communication parameters for the TTY terminal emulation on the OTM PC:

- 9600 baud
- 8 bits
- no parity bit
- 1 stop bit

When a new IP trunk card starts up and displays “T:20” on the 4-character display, the IP trunk card begins sending BOOTP requests on the ELAN subnet. A series of dots appears on the TTY.

3 Type **+++** to bring up the ITG shell CLI prompt:

```
...+++
```

When prompted to login, enter the default username and password as:

VxWorks login: **itgadmin**
Password: **itgadmin**

```
ITG>
```

4 When the ITG shell prompt appears on the TTY, enter the IP address for the Leader card:

Wait until the display shows “T:21,” then enter:
ITG> **setLeader “xxx.xxx.xxx.xxx”, “yyy.yyy.yyy.yyy”,”zzz.zzz.zzz.zzz”**

Where:

- “xxx.xxx.xxx.xxx” is the ELAN network interface IP address of Leader 0 on the ELAN subnet,
- “yyy.yyy.yyy.yyy” is the ELAN network interface gateway (router) IP address on the ELAN subnet. If the OTM PC is connected locally to the LAN and there is no ELAN gateway, then the gateway IP address is “0.0.0.0”.
- “zzz.zzz.zzz.zzz” is the subnet mask for the ELAN network interface IP address of Leader 0 on the ELAN subnet.

Note: All ITG shell commands are case-sensitive. A space separates the command from the first parameter. The three parameters must each be enclosed in quotation marks and there must be a comma and no spaces separating the three parameters.

Note 3: The **ELAN gateway (router) IP address** is used on reboot to create the IP route table default network route only if
(1) there is no active leader that has this card's ELAN network interface MAC address in its node properties file and
(2) this card's node properties file is empty (size 0 Kb).

Note 4: IP addresses and subnet masks must be entered in dotted decimal format.

Note 5: If the network administrator has provided the **subnet mask** in CIDR format, convert it to dotted decimal format before entering it. For example: 10.1.1.1/20 must be converted to IP address 10.1.1.1 with subnet mask 255.255.240.0. To convert subnet mask from CIDR format to dotted decimal format refer to "Subnet mask conversion from CIDR to dotted decimal format" on page 601.

5 Press **Enter**.

6 Press the **Reset** button on the faceplate to reboot the Leader 0 IP trunk card.

After the reboot is completed, the Leader 0 card is in a state of "backup leader". The faceplate display shows "BLDR." It cannot yet be in a state of "active leader", until the node properties have been successfully transmitted from OTM 2.1 (and later) to the Leader 0 card.

End of Procedure

Backup Leader installation for IP Trunk 3.01 (and later)

To install a Backup Leader in an IP Trunk 3.01 (and later) node, follow the steps in Procedure 28.

Procedure 28
Installing a Backup Leader in IP Trunk 3.01 (and later)

1. Ensure both IP trunk cards are running the same version of software. The software version is displayed when logging into the IP trunk cards. The software version can also be displayed by typing the command **swVersionShow** at the ITG CLI interface.

2. If the software versions are different, follow the upgrade erase procedure. Download the software from www.nortel.com home page. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support. If problems are encountered, please contact the support group or GNTS.

3. Ensure the D-channel is configured to handle the extra B-channels that are installed. ISLM = 382 max.

4. Use NTMF94 cables for ITG-Pentium 24-port trunk cards with a DCHIP card installed. Use NTCW84 cables for ITG-Pentium 24-port trunk cards that do not have a DCHIP card installed.

   Use an A0852632 L-adapter for Media Card 32-port trunk cards. If the Media Card 32-port trunk card has a DCHIP card installed, use the DCHIP cable assembly NTMF29BA along with the L-adapter.

5. In OTM, in the same Node as Leader 0, configure Leader 1. Ensure the correct MAC address, ELAN network interface IP address, and TLAN network interface IP address assigned for the Backup Leader (Leader 1) are used, and add them. The ELAN network interface IP addresses must be on the same subnet for all cards. Though on a different subnet than the ELAN network interface IP addresses, TLAN network interface IP addresses must also be on the same subnet. The MAC address used must always be for the ELAN network interface. The MAC address for the Media Card 32-port trunk card is printed on the IP trunk card faceplate under the ELAN network interface. The MAC address for the ITG-Pentium trunk card is printed on the card faceplate under MOTHERBOARD.

6. If the card (Leader1) has been configured previously, perform the **Clear Leader** command at the ITG CLI interface. When this IP trunk card is rebooted, it comes up as a Follower/BLDR card. All configuration data is cleared on the card. It is not necessary to use the **setLeader** command.

7 Disable Leader 0 and Leader 1 from the system interface. Disable the IP trunk card at the system CLI to ensure it is disabled, even if the LED on the IP trunk card is lit. For information on how to disable the IP trunk card from the system interface, see “System commands – LD 32” on page 509.

8 From OTM, transmit the NODE PROPERTY, CARD PROPERTY, and Dialing Plan to the active leader and to all disabled IP trunk cards. This action is successful to Leader 0, but fails to Leader 1, as Leader 1 does not yet have an IP address.

9 Remove Leader 1 from the system backplane.

10 Reboot Leader 0.

11 When Leader 0 is fully rebooted, push Leader 1 back into position.

12 Leader 1 sends a BOOTP request to Leader 0. Leader 0 then sends a message back to Leader 1 which contains Leader 1’s IP address. Leader 1 reboots itself. Leader 1 then comes back as a BLDR. Depending on the network and configuration, Leader 1 can reboot itself up to 3 times.

13 Enable the Leader 0 in the system interface.

14 Transmit the Card Property and Dialing Plan (but not NODE Property) to Leader 1 from OTM. Reboot Leader 1 again.

15 When fully rebooted, enable Leader 1. If D-channel messaging is enabled, all the channels associated with this card give a Restart message.

All channels should now be IDLE on the LDR and BLDR in the system.

16 If both IP trunk cards become the LDR, then a network problem has occurred, as BLDR is not receiving/responding to a PING message. To verify, connect the TLAN network interface of both IP trunk cards to a basic hub and reboot the card. The IP trunk card must be BLDR. The LDR pings from the TLAN Node IP address to BLDR almost continuously. The Link light is continuously lit on the front of the IP trunk card. The traffic light blinks when the Ping message is sent (with no other traffic active on the cards). The lights on the front of an IP trunk card represent the state of the TLAN network interface.

End of Procedure

Transmit the node properties, card properties and dialing plan to Leader 0

Verify that the IP trunk cards are disabled in LD 32 before transmitting card properties.

> *Note:* Disable IP trunk cards whenever transmitting card properties or new software.

Use the OTM Maintenance Windows, the OTM System Passthru terminal, or a system management terminal directly connected to a TTY port. Use the LD 32 DISI command to disable the IP trunk cards when idle. In the OTM IP Telephony Gateway – ISDN IP Trunk window, select **View > Refresh** and verify that the card status is showing “Disabled”. If the card status is showing “unequipped”, configure the card in LD 14.

To transmit the node properties, card properties, and dialing plan to Leader 0, follow the steps in Procedure 29.

Procedure 29
Transmitting the node properties, card properties and dialing plan to Leader 0

1. From the **OTM Navigator** window, double-click the **ITG ISDN IP Trunks** icon from the **Services** folder. The **IP Telephony Gateway - ISDN IP Trunk window** opens.
2. Select the IP Trunk 3.01 (and later) node for which the properties are to be transmitted from the list in the upper part of the window.
3. Select Leader 0 from the list in the lower part of the window.
4. In the **IP Telephony Gateway - ISDN IP Trunk** window, select menu **Configuration > Synchronize > Transmit**.
5. Leave the radio button default setting of **Transmit to selected nodes**. Check the **Node Properties**, **Card Properties** and **Dialing Plan** check boxes.
6. Click the **Start Transmit** button.

   Monitor progress in the **Transmit Control** window. Confirm that the Node Properties, Card Properties and Dialing Plan are transmitted successfully to the Leader 0 IP trunk card TN. At this point, it is normal for transmission to Leader 1 and Follower cards to fail.

7 When the transmission is complete, click the **Close** button.

8 Reboot the Leader 0 IP trunk card.

End of Procedure

Verify installation and configuration

To verify installation and configuration, check the IP trunk card faceplate displays.

After successfully rebooting, the Leader 0 card is now fully configured with the Node Properties of the node and enters a state of "Active Leader". The faceplate display shows "LDR".

The Leader 1 card is now autoconfigured as a Leader, reboots automatically, and enters the state of "Backup Leader". The faceplate display shows "BLDR".

Any Follower cards are now auto-configured with their IP addresses and their display shows "FLR".

If an OTM PC is on the local ELAN subnet, it should now be in communication with all cards in the IP Trunk 3.01 (and later) node.

Observe IP Trunk 3.01 (and later) status in OTM 2.1 (and later)

Follow the steps in Procedure 30 to observe the IP Trunk 3.01 (and later) status in OTM 2.1 (and later).

Procedure 30
Observing the IP Trunk 3.01 (and later) status in OTM 2.1 (and later)

1 From the **OTM IP Telephony Gateway - ISDN IP Trunk** window, select menu **View > Refresh** and verify that the card status is showing "enabled" or "disabled", depending on the card status in the system. See Figure 61 on page 355. If any cards show "not responding", verify the following:

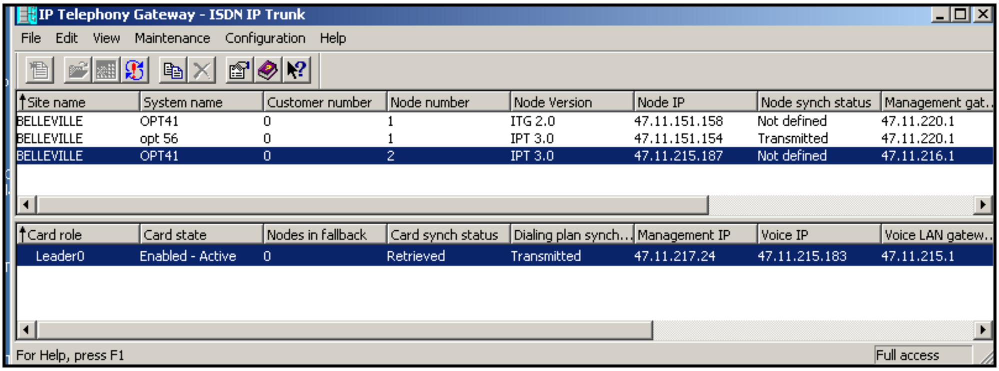
a. the ELAN network interface cable connection to the ELAN subnet

b. the TLAN network interface cable connection to the TLAN subnet

c. the ELAN MAC addresses that were entered previously on the **Configuration** tab of the Node Properties, while adding the IP Trunk 3.01 (and later) node on OTM 2.1 (and later)

d. IP addresses

Figure 61
IP trunk card status



Site name	System name	Customer number	Node number	Node Version	Node IP	Node synch status	Management gat...
BELLEVILLE	OPT41	0	1	ITG 2.0	47.11.151.158	Not defined	47.11.220.1
BELLEVILLE	opt 56	0	1	IPT 3.0	47.11.151.154	Transmitted	47.11.220.1
BELLEVILLE	OPT41	0	2	IPT 3.0	47.11.215.187	Not defined	47.11.216.1

Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...
Leader0	Enabled - Active	0	Retrieved	Transmitted	47.11.217.24	47.11.215.183	47.11.215.1

For Help, press F1

Full access

Note: If the (a) IP Trunk 3.01 (and later) Node is being installed from an OTM 2.1 (and later) PC on a remote subnet, and (b) communication with the Leader 1 and the Follower cards is not possible after transmitting the node properties, card properties and dialing plan to Leader 0 and rebooting the Leader 0 card, this means that the Leader 1 and the Follower cards are unable to communicate with the remote OTM PC. This is usually due to the fact that the IP trunk card no longer defaults to communicating with the same router as the one used by OTM 2.1 (and later). By default, IP traffic is directed to the TLAN router, as most IP traffic uses the TLAN subnet. If the OTM 2.1 (and later) PC is on the ELAN subnet, which is separate from the TLAN subnet, there probably is no routing table entry to route IP traffic meant for the OTM 2.1 (and later) PC IP address to that ELAN router.

This can be corrected by connecting a local terminal to the maintenance port on the faceplate of the Leader 1 and Follower cards. Use the ITG shell command **routeAdd** on Leader 1 and each Follower card to add a new IP route for the remote OTM PC subnet that points to the ELAN network interface gateway (router) IP address. Repeat this step every time a card is reset until the card properties, which contain the card routing table entry IP addresses, have been successfully transmitted to each card.

ITG> routeAdd "xxx.xxx.xxx.xxx", "yyy.yyy.yyy.yyy",

where:
xxx.xxx.xxx.xxx is the IP address of the remote OTM PC and
yyy.yyy.yyy.yyy is the IP address of the ELAN network interface gateway.

Press **Enter**.

2 Verify that the TN, ELAN network interface MAC addresses, and IP addresses are configured correctly for each IP trunk card. Select any card in the IP Trunk 3.01 (and later) node in the **OTM ITG – ISDN IP Trunk** window and select menu **Configuration > Node > Properties** from the drop-down lists. Compare the values displayed on the **General** tab and the **Card Configuration** tab with those on the IP Trunk 3.01 (and later) Installation Summary Sheet. The **ITG – Transmit Options** dialog box appears.

3 Correct errors and retransmit Node Properties.

4 Reboot all cards for which Node Properties have changed.

End of Procedure

Transmit card properties and dialing plan to Leader 1 and Follower cards

Verify that the IP trunk cards are disabled before transmitting card properties.

> ***Note:*** Disable IP trunk cards when transmitting card properties or new software.

Use the OTM 2.1 (and later) Maintenance Windows, the OTM 2.1 (and later) System Passthru terminal, or use a system management terminal directly connected to a TTY port on the system. Wait for the NPR0011 message, which indicates that all units on each card are disabled.Use the LD 32 DISI command to disable the IP trunk cards when idle. In the IP Telephony Gateway - ISDN IP Trunk window, select **View > Refresh** and verify that the card status is showing "Disabled". If the card status shows "unequipped", configure the card in LD 14.

Follow the steps in Procedure 31 to transmit the card properties and dialing plan to the Leader 1 and Follower IP trunk cards.

Procedure 31
Transmit card properties and dialing plan to Leader 1 and Follower cards

1. Select the IP Trunk 3.01 (and later) node for which properties are to be transmitted from the list in the upper part of the window.
2. Select Leader 0 from the list in the lower part of the window.
3. In the **IP Telephony Gateway - ISDN IP Trunk** window, select **Configuration > Synchronize > Transmit**.
4. Keep the radio button default setting of **Transmit to selected nodes**. Check the **Card Properties** and **Dialing plan** check boxes.
5. Click the **Start transmit** button.
6. Monitor progress in the **Transmit Control** window. Confirm that the Card Properties and Dialing Plan are transmitted successfully to all the IP trunk cards, which are identified by TNs.
7. When the transmission is complete, click the **Close** button.
8. Use the LD 32 ENLC command to enable the IP trunk cards in the IP Trunk 3.01 (and later) node.
9. In the **IP Telephony Gateway - ISDN IP Trunk** window, select **View > Refresh**. The card status should now show "Enabled."
10. Verify the TN, ELAN network interface MAC address, IP addresses, and D-Channel for each Media Card 32-port and ITG-Pentium 24-port trunk card. Compare the configuration data with the data on the IP Trunk 3.01 (and later) Installation Summary Sheet.

End of Procedure

Once the Card Properties and Dialing Plan have been successfully transmitted, the new Card Properties and Dialing Plan are automatically applied to each IP trunk card. The IP Trunk 3.01 (and later) node is now ready to make test calls if IP Trunk 3.01 (and later) and the ESN data have been configured on the system.

Configure date and time for the IP Trunk 3.01 (and later) node

Follow the steps in Procedure 32 on page 358 to configure the date and time on the IP Trunk 3.01 (and later) node in order to have correct time and date stamps in Operational Measurement (OM) reports, RADIUS Call Accounting reports, error messages and error and trace logs.

Procedure 32
Configure the date and time for the IP Trunk 3.01 (and later) node

1. Select the IP Trunk 3.01 (and later) node for which the date and time is to be configured from the list in the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window.
2. Double-click **Leader 0** from the list in the lower part of the window. The **ITG Card Properties** window – **Maintenance** tab opens.
3. Click the **Set Node Time...** button.
4. Set the correct date and time.
5. Click **OK**.

   The clock is updated immediately on the Active Leader card (Leader 0 or Leader 1), which in turn updates the other cards in the IP Trunk 3.01 (and later) node.

End of Procedure

Change the default ITG shell password to maintain access security

Follow the steps in Procedure 33 to change the default user name and password when installing the IP Trunk 3.01 (and later) node to maintain access security. The ITG user name and password protects maintenance port access, Telnet, and FTP access to the Media Card 32-port and ITG-Pentium 24-port trunk cards over the LAN.

Procedure 33
Changing the default ITG shell password

1. Select the new IP Trunk 3.01 (and later) node in the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window.
2. For each card in the node, right-click the card and select **Telnet to ITG card** from the right-click menu.

   The **Telnet** window appears with the VxWorks prompt.
3. When prompted to login, enter the default username and password as:

   VxWorks login: **itgadmin**
   Password: **itgadmin**

   ITG>
4. Use the command **shellPasswordSet** to change the default user name and password for Telnet to ITG shell and FTP to the IP trunk card file system. The default user name is **itgadmin** and the default password is **itgadmin**.

   Enter the following information when prompted:

   Enter current username: **itgadmin**
   Enter current password: **itgadmin**
   Enter new username: *new username*
   Enter new password: *new password*
   Enter new password again to confirm: *new password*
5. Record the new user name and password and transmit to authorized network security personnel.
6. Repeat procedure for all cards in the node.

End of Procedure

If the entire sequence of commands is successfully entered, the system response `value = 0 = 0x0` is displayed. The new user name and password are now stored in the non-volatile RAM on the IP trunk card and are retained even if the card is reset, powered-off, or on.

To reset the ITG shell password to its default setting, see “Reset the default ITG shell password” on page 493.

Change default ESN5 prefix for non-ESN5 IP telephony gateways

Follow the steps in Procedure 34 to configure an ESN5 prefix for the non-ESN5 IP telephony gateways by using the “esn5PrefixSet” command from the ITG shell CLI. The default esn5 prefix (100) corresponds to NCOS 00. If NCOS 00 does not allow access to all the required trunk facilities, change the default ESN5 prefix to work with the established NCOS plan in the customer’s network. Refer to “ESN5 network signaling” on page 308. Perform this procedure on every card in the node.

Procedure 34
Changing the default ESN5 prefix for non-ESN5 IP telephony gateways

1. Select the new IP Trunk 3.01 (and later) node in the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window.

2. For each IP trunk card in the node, right-click the IP trunk card and select **Telnet to ITG Card** from the right-click menu.

   The **Telnet** window appears with the VxWorks prompt.

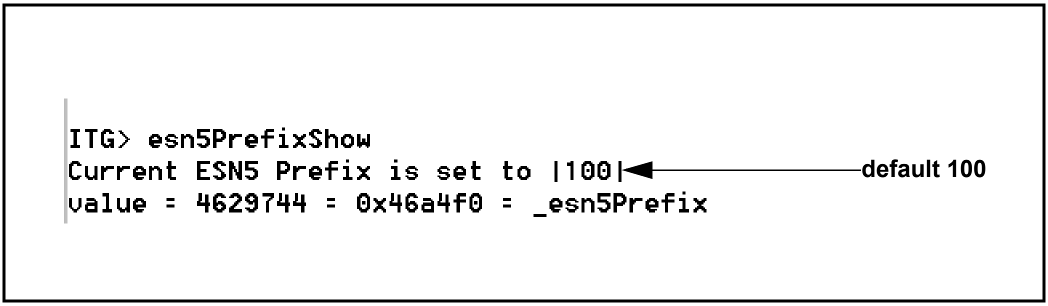
3. When prompted to login, enter the default (or user-modified) login and password.

   VxWorks login: **itgadmin**
   Password: **itgadmin**

   ITG> **esn5PrefixShow**

   See Figure 62.

Figure 62
esn5PrefixShow

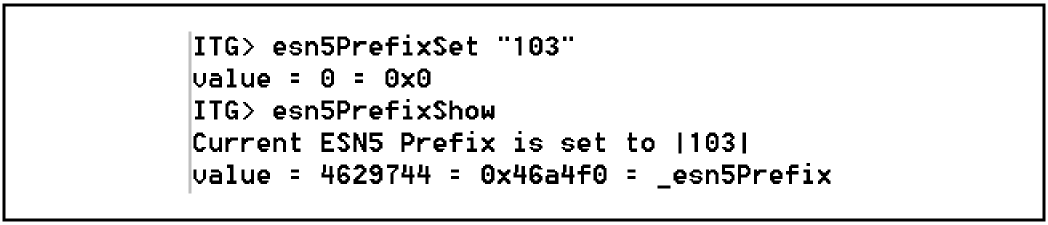


```
ITG> esn5PrefixShow
Current ESN5 Prefix is set to |100|
value = 4629744 = 0x46a4f0 = _esn5Prefix
```

default 100

4 At the ITG prompt, enter >esn5PrefixSet “1xx” where xx = the NCOS value. In Figure 63, the default value was changed from NCOS 00 to 03.

Figure 63
esn5PrefixSet



```
ITG> esn5PrefixSet "103"
value = 0 = 0x0
ITG> esn5PrefixShow
Current ESN5 Prefix is set to |103|
value = 4629744 = 0x46a4f0 = _esn5Prefix
```

End of Procedure

Check and download IP trunk card software in OTM 2.1 (and later)

Follow the steps in Procedure 35 to check the software version of the IP trunk cards in a new IP Trunk 3. 0 node. All cards must have same version. To ensure proper IP Trunk 3.01 (and later) network operation, Nortel recommends that all network nodes have the same software version. Verify that the software release on each card is the latest recommended software release for IP Trunk 3.01 (and later) by connecting to a Nortel website that contains the latest software versions for the Media Card 32-port and the ITG-Pentium 24-port trunk card.

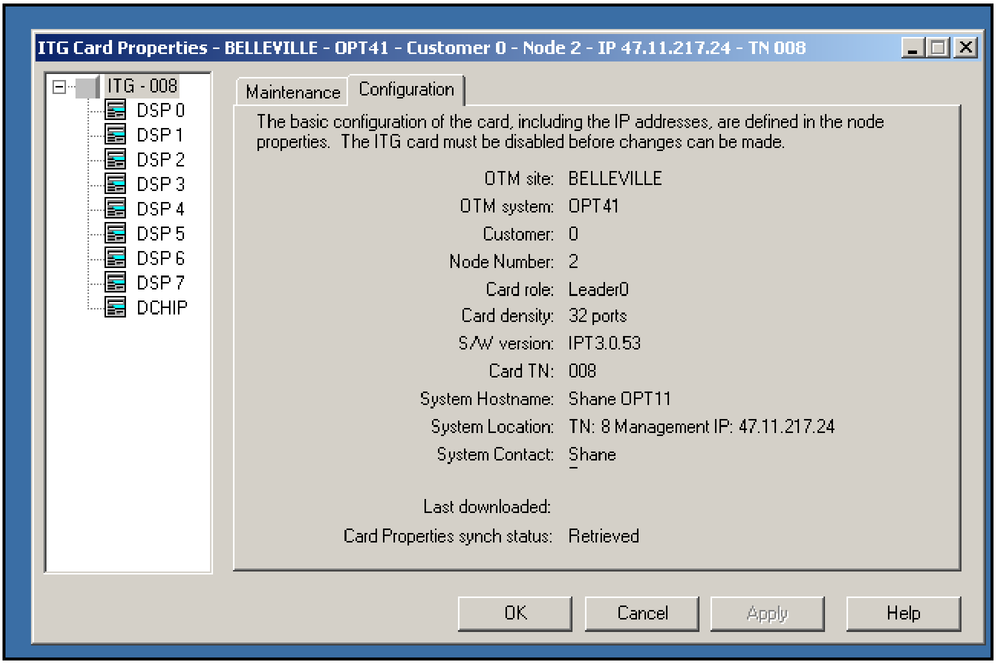
Procedure 35
Checking the IP trunk cards software version

1 From the **IP Telephony Gateway - ISDN IP Trunk** window, click the new node.

2 For each card in the node, starting with Leader 0, double-click the card entry in the lower half of the window. The **Card Properties** window appears.

3 Click the **Configuration** tab and record **S/W version**, **Card density** and **Card TN** for each card in the new node. See Figure 64 on page 362.

Figure 64
ITG Card Properties – Configuration tab



ITG Card Properties - BELLEVILLE - OPT41 - Customer 0 - Node 2 - IP 47.11.217.24 - TN 008

The basic configuration of the card, including the IP addresses, are defined in the node properties. The ITG card must be disabled before changes can be made.

OTM site: BELLEVILLE
OTM system: OPT41
Customer: 0
Node Number: 2
Card role: Leader0
Card density: 32 ports
S/W version: IPT3.0.53
Card TN: 008
System Hostname: Shane OPT11
System Location: TN: 8 Management IP: 47.11.217.24
System Contact: Shane

Last downloaded:
Card Properties synch status: Retrieved

4 Check the Nortel website to find the latest recommended IP Trunk 3.01 (and later) software release.

Go to www.nortel.com. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support.

5 Click **Download Software.** Compare the IP trunk card Properties software version to the version listed in the **Release** column.

- If versions match, software upgrade is not required. Turn to "Configure OTM Alarm Management to receive SNMP traps from the IP trunk cards" on page 367.
- If versions are different, go to step 6.

6 Fill in the **Name, Phone number** and **Company** fields. Click the **Download Current Release** button. The **ITG Software Download Request Form** window appears.

7 Download software packages and associated release notes as follows:

- For Media Card 32-port trunk cards, download the **Software Package for Release IP Trunk 3.01 (and later).**
- For ITG-Pentium 24-port trunk cards, download the **Software Package for Release IP Trunk 3.01 (and later).**

8 When prompted, select **Download**. Record the file name and location of downloaded software on the OTM 2.1 (and later) PC.

End of Procedure

Now the new IP trunk card software is ready to be transmitted from OTM 2.1 (and later) to the IP trunk cards.

Transmit new software to the IP trunk cards

Verify that the IP trunk cards are disabled before transmitting new card software.

> ***Note:*** Disable the IP trunk cards when transmitting card properties or new software.

Use the OTM Maintenance Windows, the OTM System Passthru terminal, or a system management terminal directly connected to a TTY port on the system.

Use the LD 32 DISI command to disable the IP trunk cards when idle. NPROG indicates that all units on the card have been disabled.

In the **OTM IP Telephony Gateway - ISDN IP Trunk** window, select **View > Refresh** and verify that the card status is showing "Disabled". If the card status shows "unequipped", configure the card in LD 14.

Follow the steps in Procedure 36 on page 364 to transmit the new software to the IP trunk cards.

Procedure 36
Transmitting new software to the IP trunk cards

1. Open OTM 2.1 (and later). Click **Services** and launch the ITG ISDN IP Trunks application.
2. Select the node to upgrade from the list in the upper half of the **IP Telephony Gateway - ISDN IP Trunk** window.
3. Select node or cards for software transmission according to card density:
   - If all cards in the node have same card density (24-port or 32-port), upgrade all the cards together by transmitting to the selected node. Click the new node in the upper half of the **IP Telephony Gateway - ISDN IP Trunk** window.
   - If a mix of Media Card 32-port and ITG-Pentium 24-port trunk cards is in the same IP Trunk 3.01 (and later) node, then select all cards of the same density in the lower half of the window. Hold down the **Ctrl** key while making individual card selections.
4. Select menu **Configuration/Synchronize/Transmit**. The **ITG - Transmit Options** dialog box appears.
5. If transmitting new software to a node, choose step a **or** b.
   - If transmitting new software to a node containing cards of the same density, ensure the following:

     Make sure **Transmit to selected nodes** is selected.

     Check **Card software** checkbox.

     Click **Browse** and locate the software file for the card density of the selected node.

     Click **Start Transmit**. The software is transmitted to each card in turn and burned into the flash ROM on the IP trunk card. Monitor the progress of the card software transmission in the **Transmit Control** window. IP Trunk 3.01 (and later) indicates success or failure of card software transmission by card TN. Scroll to verify that the transmission was successful for all card TNs. The cards continue to run the old software until rebooted.

Click the **Close** button and go to step 6.

- If transmitting new software to a node containing a mix of card densities, ensure the following:

  Make sure **Transmit to selected cards** is selected.

  Check **Card software** checkbox.

  Click **Browse** and locate the software file for the card density of the selected cards (24-port or 32-port).

  Click **Start Transmit**. The software is transmitted to each card in turn and burned into the flash ROM on the IP trunk card. Monitor the progress of the IP trunk card software transmission in the **Transmit Control** window. IP Trunk 3.01 (and later) indicates success or failure of card software transmission by card TN. Scroll to verify that transmission was successful for all card TNs. The IP trunk cards continue to run the old software until rebooted.

  Click **Close** button.

  Repeat steps 3b, 4 and 5b for the other card density.

6 Reboot each IP trunk card that received transmitted software, so that the new software can be applied. Start the rebooting with Leader 0, then Leader 1, and finally the follower cards.

Double-click the card in the lower part of the **IP Telephony Gateway - ISDN IP Trunk** window. The **Card Properties Maintenance** tab appears. Click **Reset** to reboot the card. Click **OK.**

Note: Alternatively, reset the cards by pressing the **Reset** button on the card faceplate, using a pointed object.

7 From the **IP Telephony Gateway - ISDN IP Trunk** window, select the new node. Select menu **View/Refresh/Selected** or press F5.

8 After all IP trunk cards have been reset and have successfully rebooted, the **Card state** column shows **disabled:active** for Leader 0, **disabled:standby** for Leader 1, and **disabled** for Followers.

9 Double-click each upgraded card. Click the **Configuration** tab of the **Card Properties** window and check the **S/W version**.

10 Use the LD 32 ENLC command to re-enable the IP trunk cards.

End of Procedure

The software upgrade procedure is complete.

Upgrade the DCHIP PC Card

Follow the steps in Procedure 37 to upgrade the DCHIP card.

Procedure 37
Upgrading the DCHIP card

1 Copy the DCHIP PC Card driver to the /C: drive of the Leader card using FTP.

2 In the **IP Telephony Gateway - ISDN IP Trunk** window, right-click the DCHIP card and select **Telnet to ITG Card** from the right-click menu.

The **Telnet** window appears with the VxWorks prompt.

3 When prompted to login, enter the default username and password as:

VxWorks login: **itgadmin**
Password: **itgadmin**

ITG>

4 Disable the ITG-Pentium 24-port or Media Card 32-port trunk card in LD 32 (DISI lsc). Wait for the NPRxx message.

5 Use the command **DCHdisable** to disable the D-channel function on the card.

6 Use the command **loader 1, "/C:pcmv32.bin"** to transfer the DCHIP PC Card software to the DCHIP PC Card.

Note: The '1' indicates the internal PC Card slot on the DCHIP Card. For the external PC Card Slot, use '0'.

The DCHIP card checks whether or not it is a Leader card.

- The DCHIP PC Card software is downloaded to the Leader card first.

If it is a Leader card, it copies the DCHIP PC Card software from its own /C: drive. If it is not a Leader card, it FTPs the DCHIP PC Card from the Active Leader card. Since the FTP server on the IP trunk card is password protected, enter the login and password when prompted. If correct, the upgrade of the DCHIP PC Card begins.

End of Procedure

Once the upgrade is complete, the DCHIP card reboots automatically.

Configure OTM Alarm Management to receive SNMP traps from the IP trunk cards

Follow the steps in Procedure 38 to configure OTM Alarm Management to receive SNMP traps from the IP trunk cards. The OTM Alarm Management option must be enabled to perform this procedure. For the procedure to activate SNMP trap generation on the IP Trunk 3.01 (and later) node, see "Configure SNMP Traps/Routing and IP addresses tab" on page 331. Enter the IP address of the OTM PC as described in that procedure.

Procedure 38
Configuring OTM ALarm Management to receive SNMP traps from the IP trunk cards

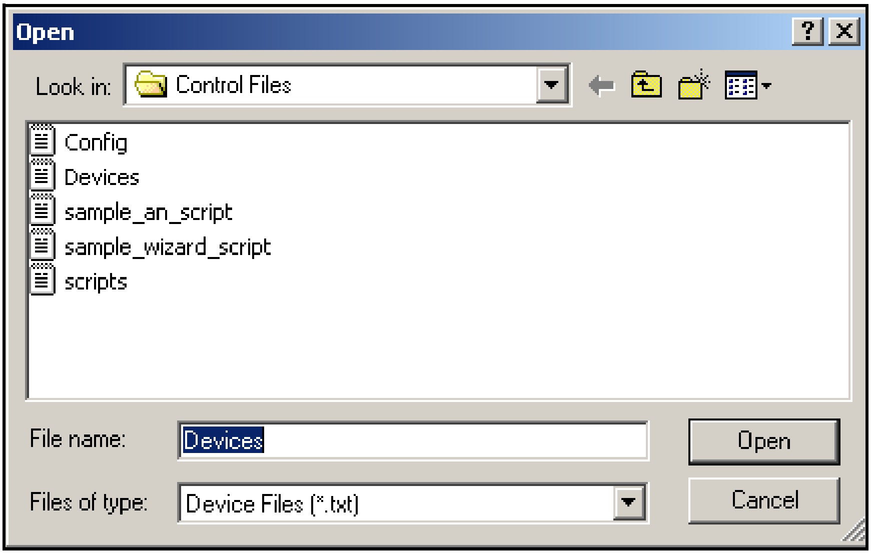
1 In the **OTM Navigator** window select **Utilities > Alarm Notification**. The **OTM Alarm Notification** dialog box appears.

2 Select **Configuration > Run Options**. The "Alarm Notification Run Options" dialog box appears.

3 Click the **Control Files** tab.

4 Click **Devices > Browse**. The "Open" dialog box appears. See Figure 65 on page 368.

Figure 65
“Open” dialog box



Look in: Control Files

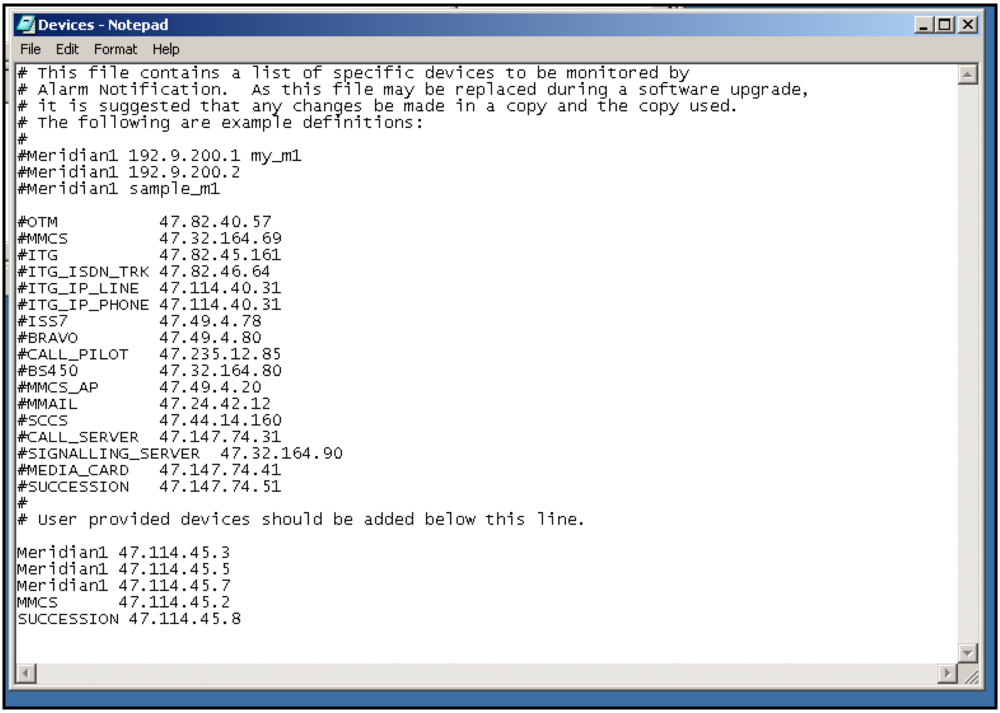
Config
Devices
sample_an_script
sample_wizard_script
scripts

File name: Devices

Files of type: Device Files (*.txt)

5 Select the Devices file from the Control Files folder and click **Open**. The Devices.txt file opens. See Figure 66 on page 369.

Figure 66
Devices.txt file:



```
# This file contains a list of specific devices to be monitored by
# Alarm Notification.  As this file may be replaced during a software upgrade,
# it is suggested that any changes be made in a copy and the copy used.
# The following are example definitions:
#
#Meridian1 192.9.200.1 my_m1
#Meridian1 192.9.200.2
#Meridian1 sample_m1

#OTM           47.82.40.57
#MMCS          47.32.164.69
#ITG           47.82.45.161
#ITG_ISDN_TRK 47.82.46.64
#ITG_IP_LINE  47.114.40.31
#ITG_IP_PHONE 47.114.40.31
#ISS7          47.49.4.78
#BRAVO         47.49.4.80
#CALL_PILOT   47.235.12.85
#BS450         47.32.164.80
#MMCS_AP      47.49.4.20
#MMAIL         47.24.42.12
#SCCS          47.44.14.160
#CALL_SERVER  47.147.74.31
#SIGNALLING_SERVER  47.32.164.90
#MEDIA_CARD   47.147.74.41
#SUCCESSION   47.147.74.51
#
# User provided devices should be added below this line.

Meridian1 47.114.45.3
Meridian1 47.114.45.5
Meridian1 47.114.45.7
MMCS      47.114.45.2
SUCCESSION 47.114.45.8
```

6 For each IP trunk card in each monitored IP Trunk 3.01 (and later) node, add a line consisting of three fields separated by spaces. See Table 49. Enter the first line beginning underneath the last line that begins with a "#". Lines beginning with "#" are comments and not processed. Do not begin any of the lines defining IP Trunk 3.01 (and later) devices with "#".

Table 49
Format of Devices.txt file

Device Type	IP Address	Device Name
ITG	xxx.xxx.xxx.xxx	Site_Leader_0
ITG	xxx.xxx.xxx.xxx	Site_Leader_1
ITG	xxx.xxx.xxx.xxx	Site_Follower_2
Note: The Device Name cannot contain any spaces. Use a descriptive name for the system site where the IP Trunk 3.01 (and later) node is located.		

7 Click **File** > **Save**.

8 In the **Alarm Notification Run Options** window, click **OK**.

OTM Alarm Notification must be restarted whenever Control Files are changed.

9 If OTM Alarm Notification is running (a red traffic light is showing on the tool bar), stop it by clicking on the red traffic light on the tool bar. Restart it by clicking on the green traffic light.

10 If OTM Alarm Notification is not running (a green traffic light is showing on the tool bar), start it by clicking on the green traffic light to change it to red.

11 Enter the **trap_gen** command from the ITG shell. A series of SNMP traps is emitted by the IP trunk card and appears in the **OTM Alarm Notification browser** window. Verify the device name identifies the correct IP trunk card.

End of Procedure

Make test calls to the remote nodes (ITG Trunk or IP Trunk)

Make test calls to ensure the following:

- The IP Trunk 3.01 (and later) system can process calls from each node to a remote node.
- The IP trunk cards are enabled.
- QoS, as defined within the Dialing Plan window, is acceptable.

Check the IP Trunk 3.01 (and later) operational report. If fallback to PSTN occurs, examine the IP data network for problems. Also, check the IP trunk cards' dialing plan table and verify that the remote ITG Trunk 2.x or IP Trunk 3.01 (and later) node is powered up, configured, and enabled.

Provisioning IP Trunk 3.01 (and later) in OTM 2.1 (and later)

Contents

This section contains information on the following topics:

Overview

This chapter describes the provisioning in OTM 2.1 (and later) required to operate the IP Trunk 3.01 (and later) application.

For detailed information on configuring a system in OTM 2.1 (and later), see *Optivity Telephony Manager: System Administration* (553-3001-330).

Add a site and system

Before the IP Trunk 3.01 (and later) application can be used, a site, a system, and at least one node must be configured.

> **Important**
>
> When OTM 2.1 (and later) is launched, it launches its own FTP service. Other FTP services, such as those found in Windows NT4 and Windows 2000 (which are launched by default) must be turned off, or OTM 2.1 (and later) will not work properly.

Add a site

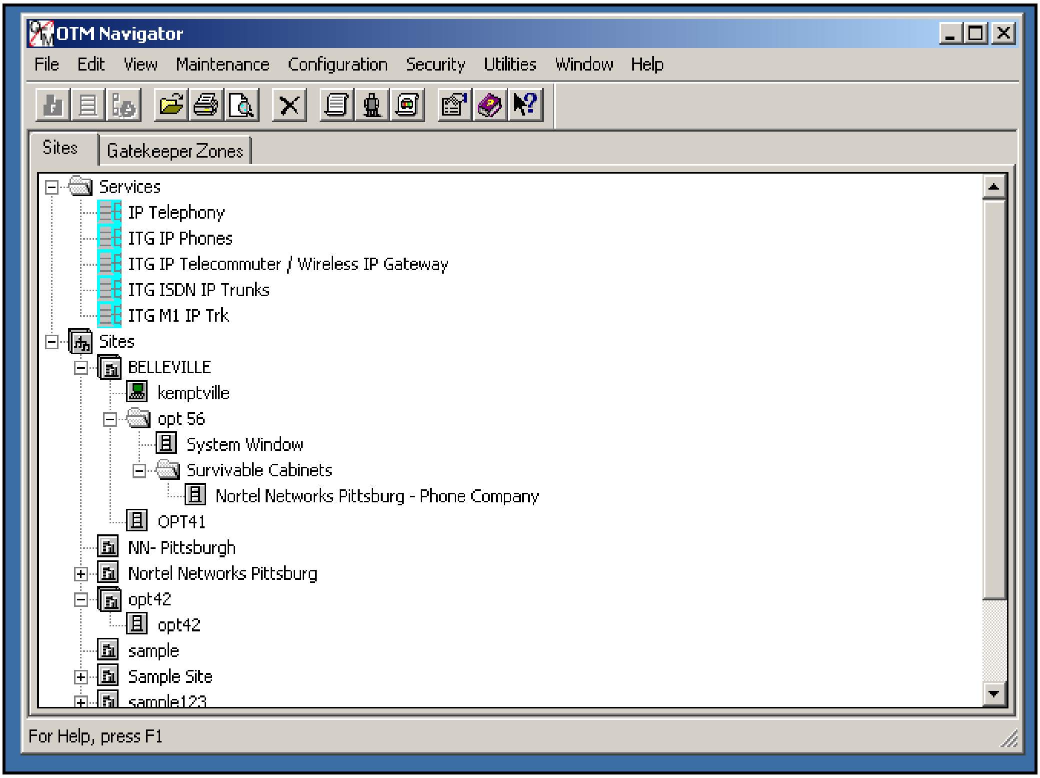
The first step is to add a site (or end-point).

Procedure 39
Adding a site

1 Log in to the OTM Navigator.

The window displays two sections – Services and Sites. See Figure 67 on page 375.

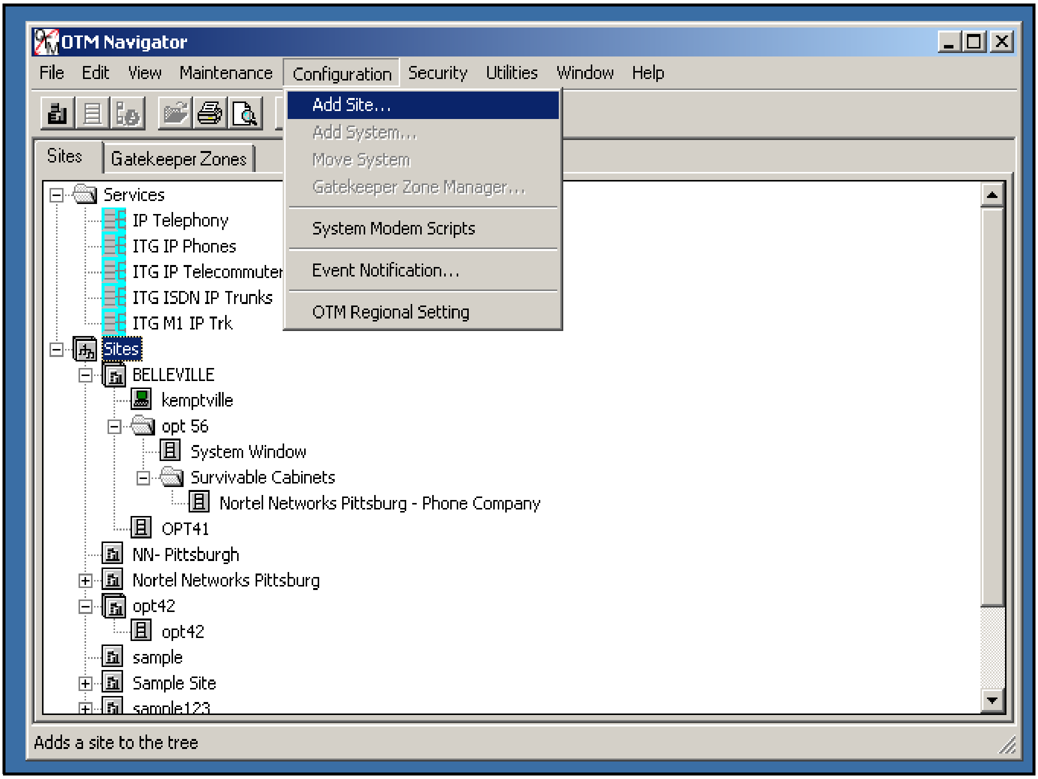
Figure 67
OTM Navigator



2 Click **Sites** to highlight it.

3 On the menu bar, click **Configuration > Add Site**. See Figure 68 on page 376.

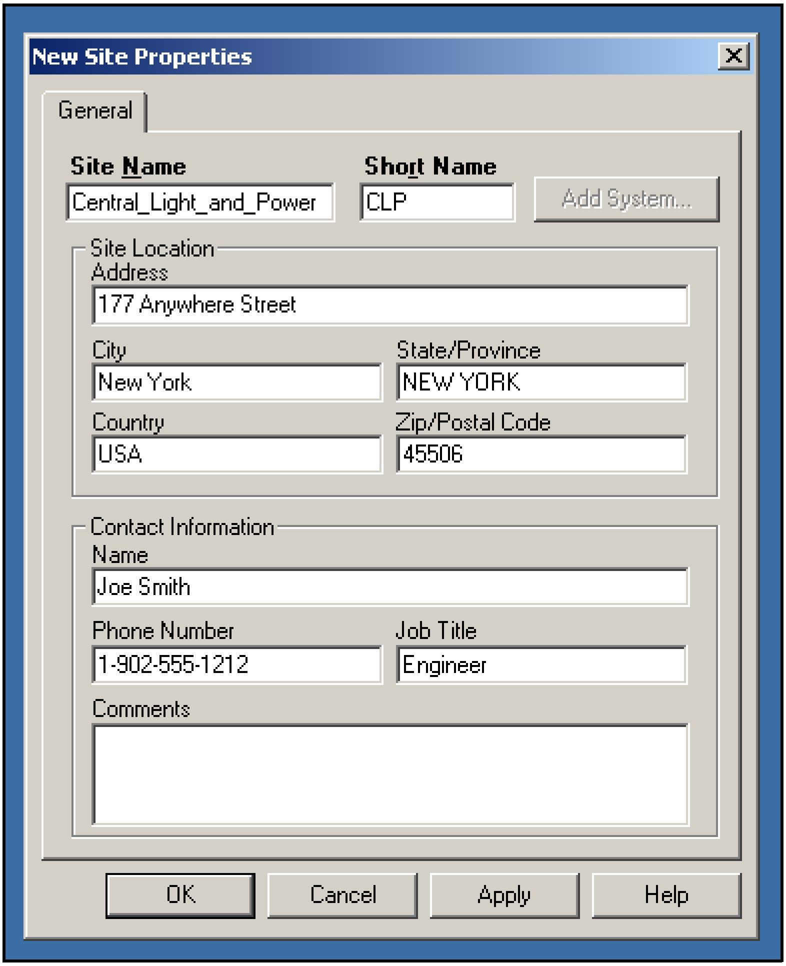
Figure 68
Add a Site



An empty **New Site Properties** window opens.

4 The site is a single entity, usually in one location. Enter as much information as is required for proper site maintenance. This information typically includes all the information entered into the example shown in Figure 69 on page 377.

Figure 69
New Site Properties – Provisioning a new site



Site Name: Central_Light_and_Power
Short Name: CLP

Site Location
Address: 177 Anywhere Street
City: New York
State/Province: NEW YORK
Country: USA
Zip/Postal Code: 45506

Contact Information
Name: Joe Smith
Phone Number: 1-902-555-1212
Job Title: Engineer
Comments:

5 Click **OK** to save the site information.

The **OTM Navigator** window opens again, with the new site added.

End of Procedure

For more information on how to add a site, see *Optivity Telephony Manager: System Administration* (553-3001-330).

Change an existing site

Follow the steps in Procedure 40 to make changes to an existing site.

Procedure 40
Changing an existing site

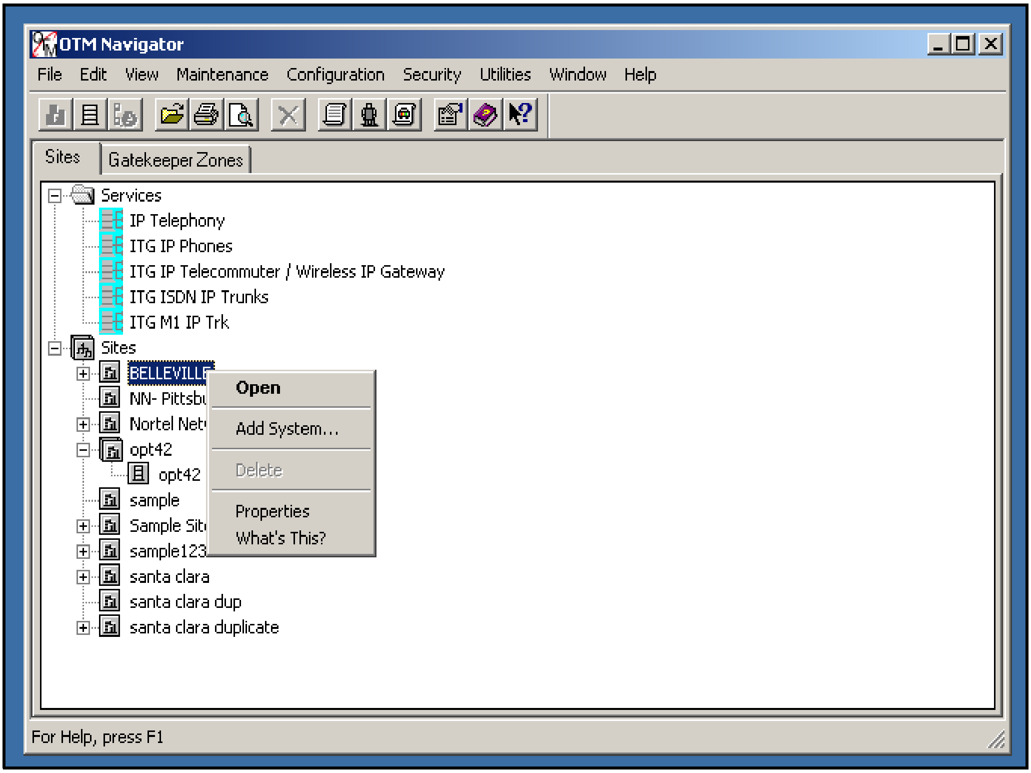
1 Log in to the OTM Navigator.

The window displays two sections: Services and Sites. See Figure 67 on page 375.

2 In the Sites section, click the site to be changed.

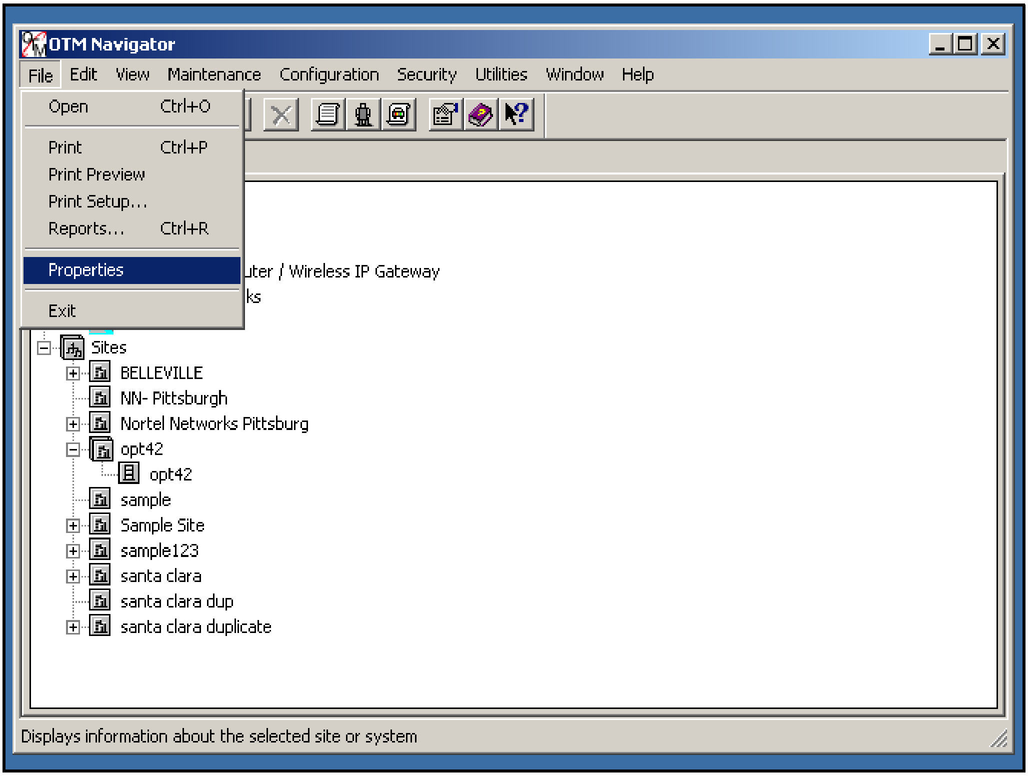
3 Right-click the site and from the drop-down list, select **Properties**. See Figure 70 on page 379.

Figure 70
Change System Properties



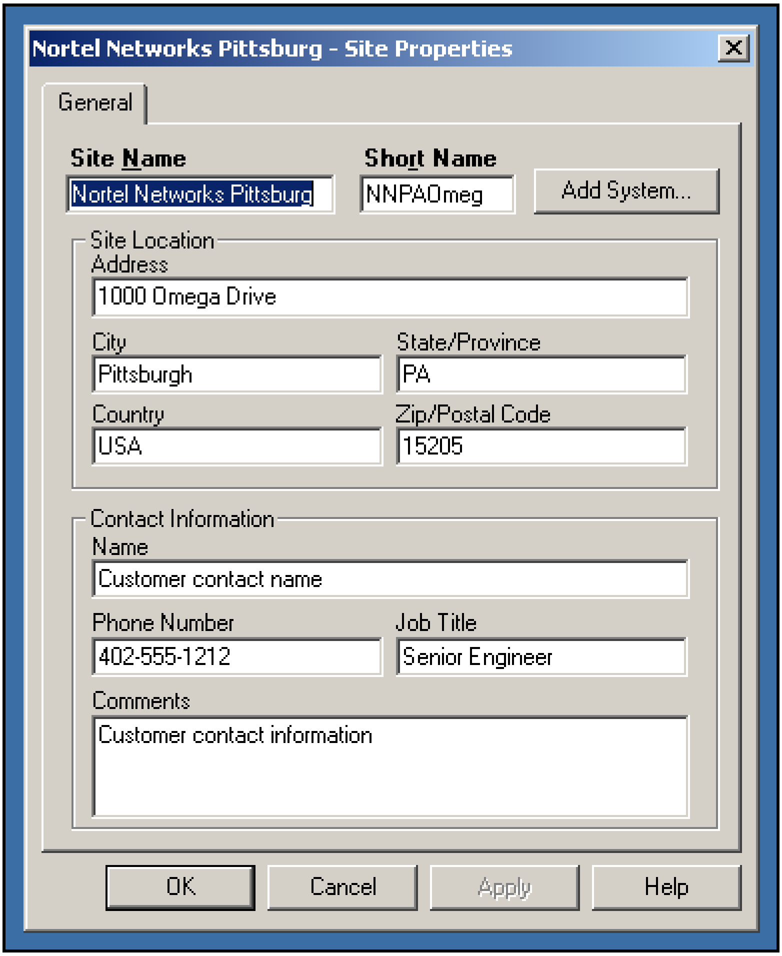
Alternatively, from the upper menu, click **File > Properties**. See Figure 71 on page 380.

Figure 71
Alternate way to change System Properties



The **Site Properties** window opens. See Figure 72 on page 381.

Figure 72
OTM Site Properties ready to change



Nortel Networks Pittsburg - Site Properties

General

Site Name: Nortel Networks Pittsburg

Short Name: NNPAOmeg

Add System...

Site Location

Address: 1000 Omega Drive

City: Pittsburgh

State/Province: PA

Country: USA

Zip/Postal Code: 15205

Contact Information

Name: Customer contact name

Phone Number: 402-555-1212

Job Title: Senior Engineer

Comments: Customer contact information

OK | Cancel | Apply | Help

4 Enter the information that is being changed.

5 Click **OK** to save the site information.

End of Procedure

Delete a site

Follow the steps in Procedure 41 to delete a site.

Procedure 41
Deleting a site

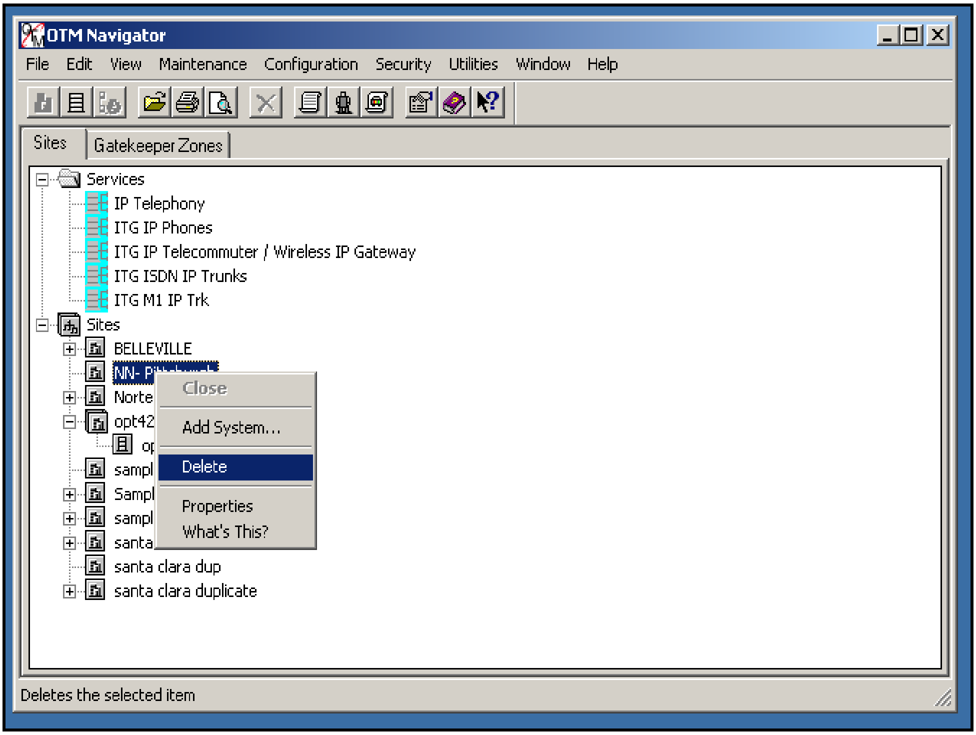
1 Log in to the OTM Navigator.

The window displays two sections – Services and Sites. See Figure 67 on page 375.

2 In the Sites section, click the site to be deleted.

3 Right-click the site and from the drop-down list, select **Delete**. See Figure 73.

Figure 73
Deleting a site



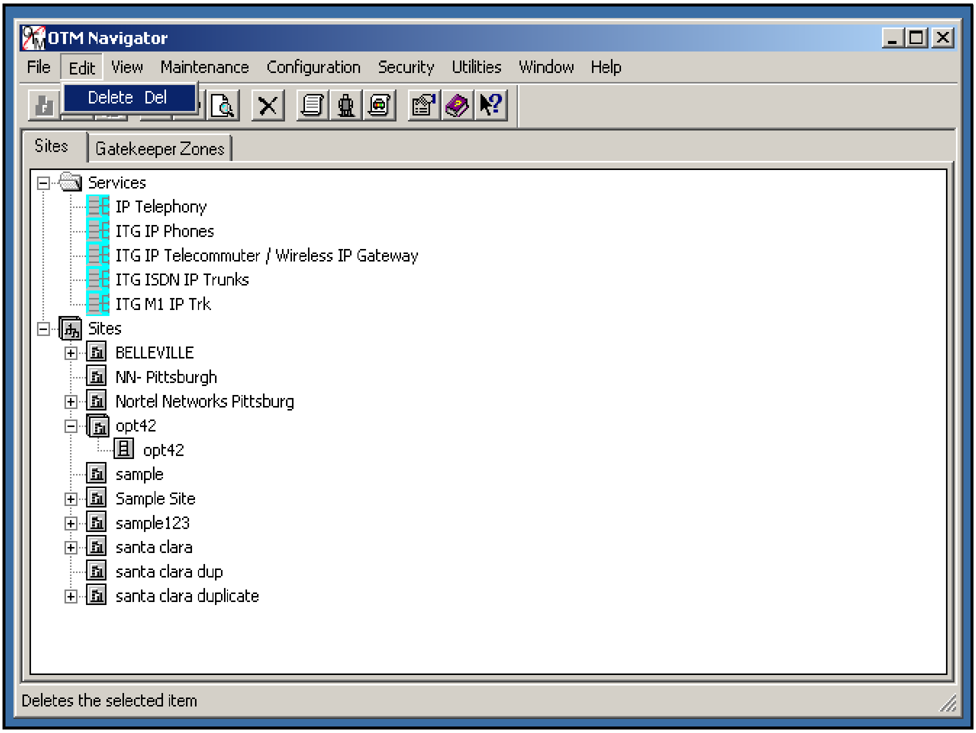
Alternatively, from the upper menu, click **Edit** > **Delete**.

WARNING

Deleting a site also deletes all of its systems.

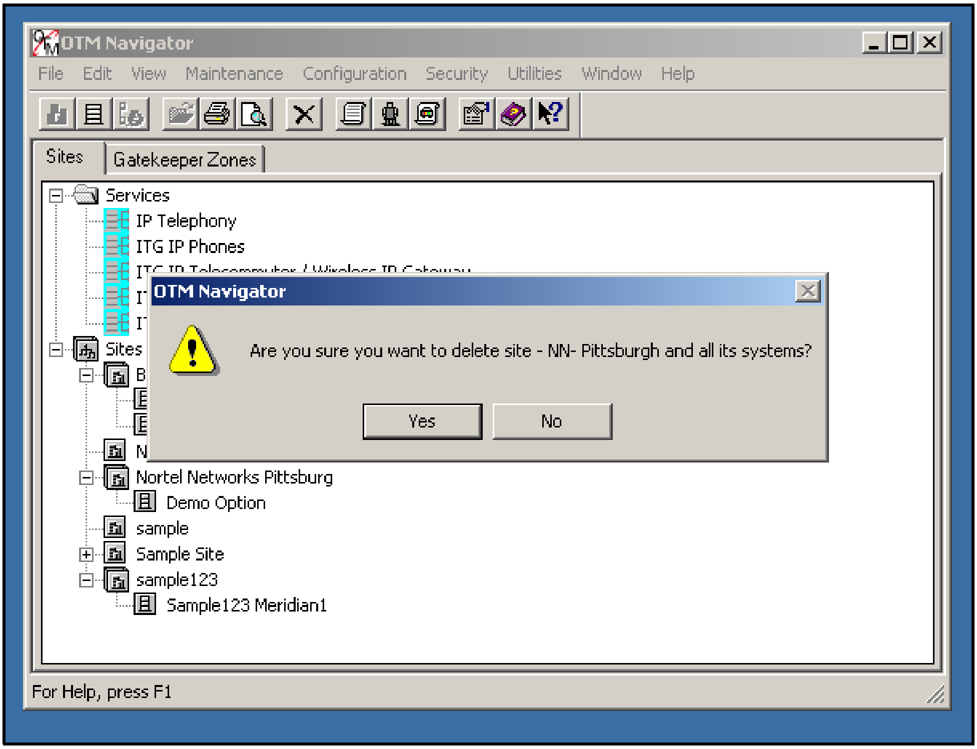
See Figure 74.

Figure 74
Alternative method of deleting a site



4 In the warning box that opens, click **Yes** to confirm the deletion. See Figure 75 on page 384.

Figure 75
Confirm deletion



Are you sure you want to delete site - NN- Pittsburgh and all its systems?

End of Procedure

Add a system

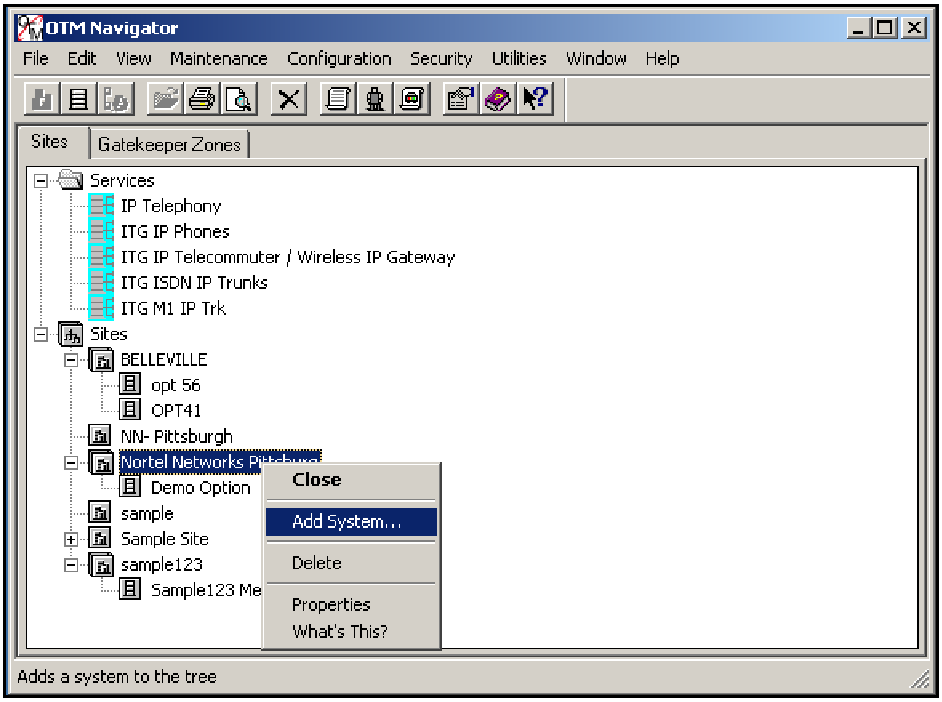
Though the site has been added, no switches or nodes have been defined. A PBX, also called a system, must be added. For IP Trunk 3.01 (and later), the system usually corresponds to a single PBX.

Procedure 42
Adding a system

1 There are two ways to add a new system in the **OTM Navigator** window, as follows:

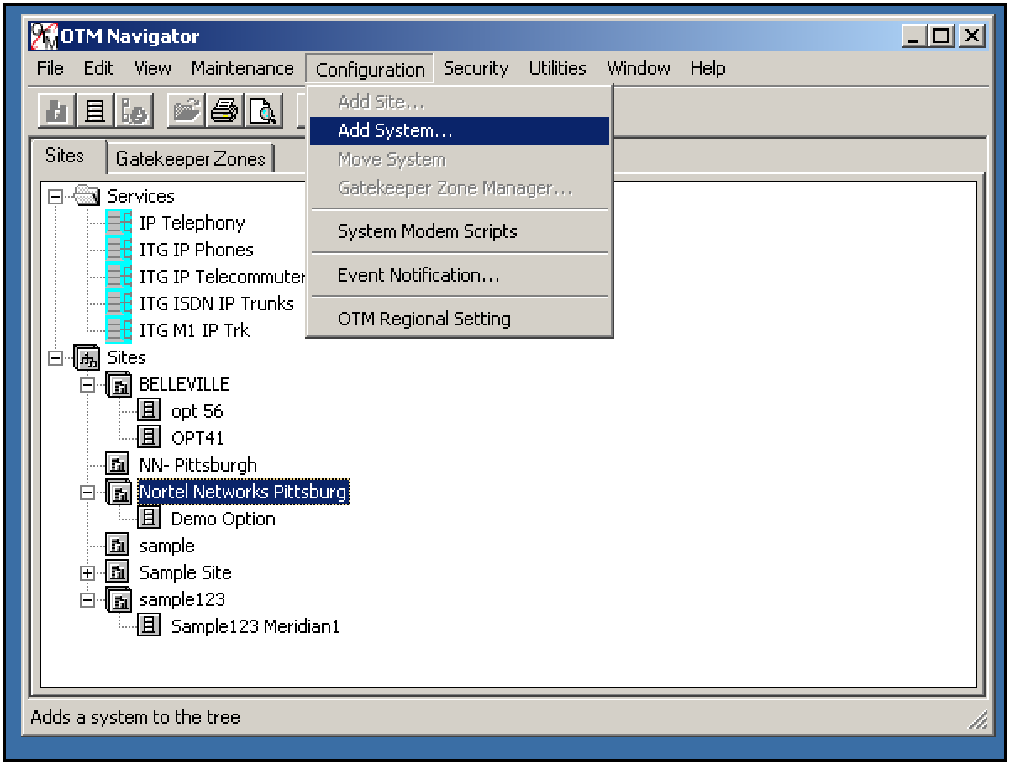
- Right-click the new site. A menu appears, as shown in Figure 76. Click **Add System.** The **Add System** window opens. See Figure 78 on page 387.

Figure 76
New system – add a system by right-clicking



- Alternatively, select the new site. From the menu bar, click **Configuration > Add System**. See Figure 77 on page 386. The **Add System** window opens. See Figure 78 on page 387.

Figure 77
New system – menu bar



2 The system selections that apply to IP Trunk 3.01 (and later) are:

- Meridian 1

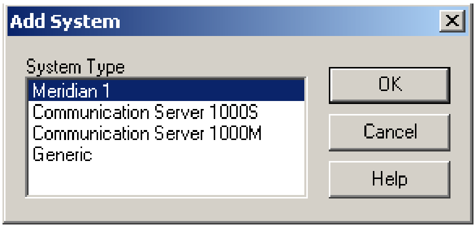
  The IP trunk cards are provisioned as part of the Meridian 1 system, as they are the trunk cards that provide access to the VoIP network and allow interworking with the IP Peer H.323 gateway.

- Communication Server 1000S
- Communication Server 1000M
- Generic

  CS 1000S and CS 1000M use IP Peer Networking to inter-operate with the IP Trunk 3.01 (and later) nodes. CS 1000S/CS 1000M must also be provisioned in OTM 2.1 (and later). The CS 1000S/1000M Gatekeeper enables interworking between IP Peer and IP Trunk 3.01 (and later). By provisioning the CS 1000S/1000M system on the same OTM 2.1 (and later) PC, the Gatekeeper information is stored in OTM 2.1 (and later), making it easier to provision IP Trunk 3.01 (and later) to use the Gatekeeper. The Gatekeeper IP address is already stored as part of a Gatekeeper zone.

For IP Trunk 3.01 (and later), select Meridian 1 in the **Add System** window. Click **OK**. See Figure 78.

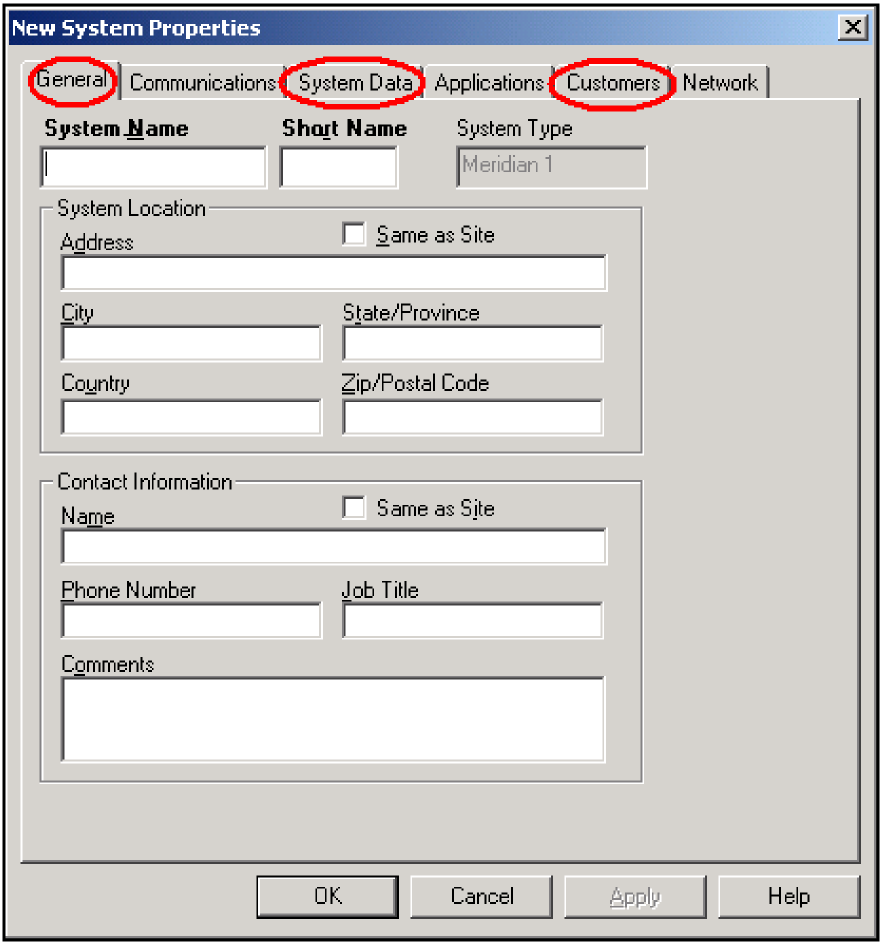
Figure 78
Select a system type



The **New System Properties** window opens. This window enables system-wide values to be provisioned.

3 Click the **General** tab. An empty **New System Properties** window opens. See Figure 79 on page 388.

Figure 79
Empty New System Properties window



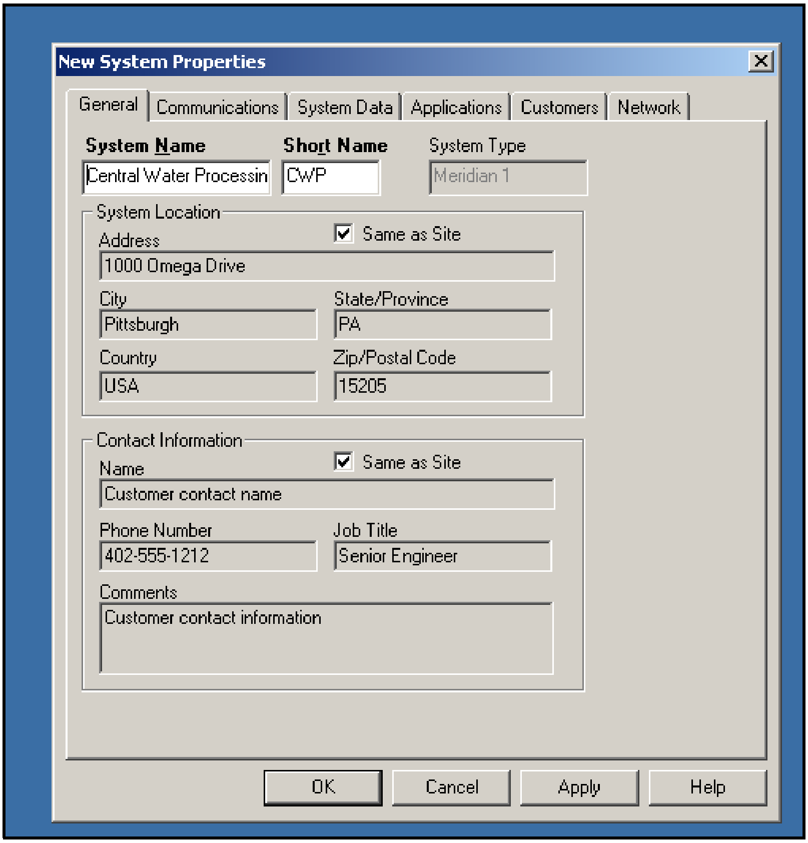
System Type: Meridian 1

The General properties must be provisioned before any other site properties, as the information on the General tab pertains to the entire system and all IP Trunk nodes on the system.

4 Give the system its own unique name. If the system is co-located with the site, as in this example, select the **Same as Site** check box. The rest of the information is obtained from the site information and is entered automatically. See Figure 80 on page 389.

5 If the system and site are not in the same location, enter the system location and service personnel contact information.

Figure 80
New system properties – General tab



New System Properties

System Name: Central Water Processin
Short Name: CWP
System Type: Meridian 1

System Location
☑ Same as Site
Address: 1000 Omega Drive
City: Pittsburgh
State/Province: PA
Country: USA
Zip/Postal Code: 15205

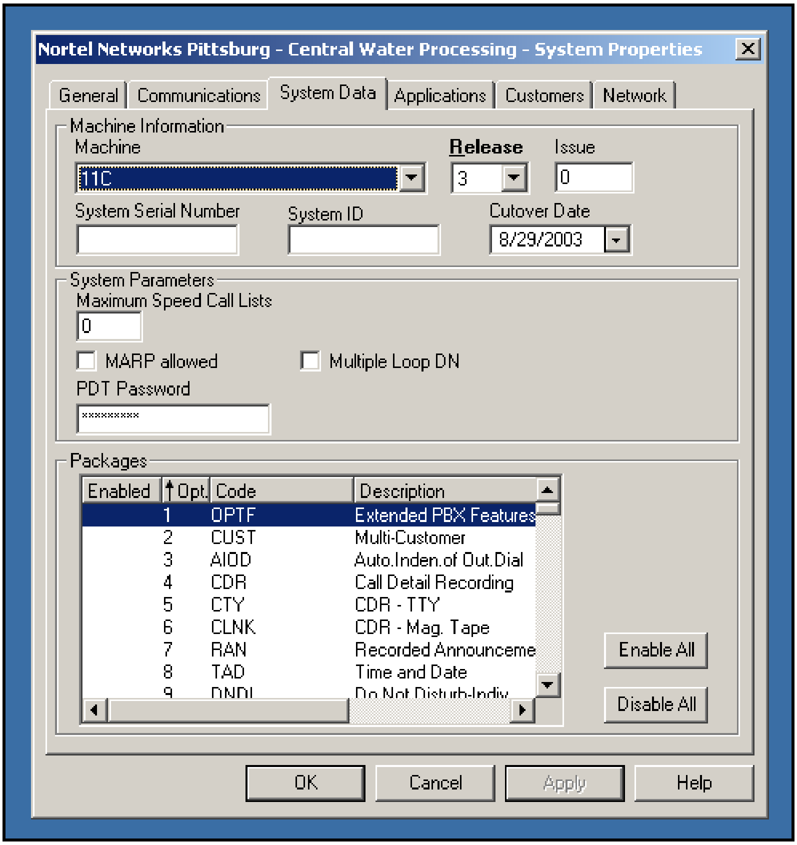
Contact Information
☑ Same as Site
Name: Customer contact name
Phone Number: 402-555-1212
Job Title: Senior Engineer
Comments: Customer contact information

Enter system data

6 Click the **System Data** tab. Enter the correct machine type, software release, and system parameters. Ensure the correct packages are provisioned. See Figure 81 on page 391.

Note: If OTM 2.1 (and later) can communicate with the Meridian 1/ CS 1000M and the **Communications** tab in the **System Properties** window is filled in correctly, the system data can be retrieved. See *Optivity Telephony Manager: System Administration* (553-3001-330) for more information.

Figure 81
System Data tab



Machine: 11C

Release: 3

Issue: 0

System Serial Number:

System ID:

Cutover Date: 8/29/2003

Maximum Speed Call Lists: 0

□ MARP allowed

□ Multiple Loop DN

PDT Password: *********

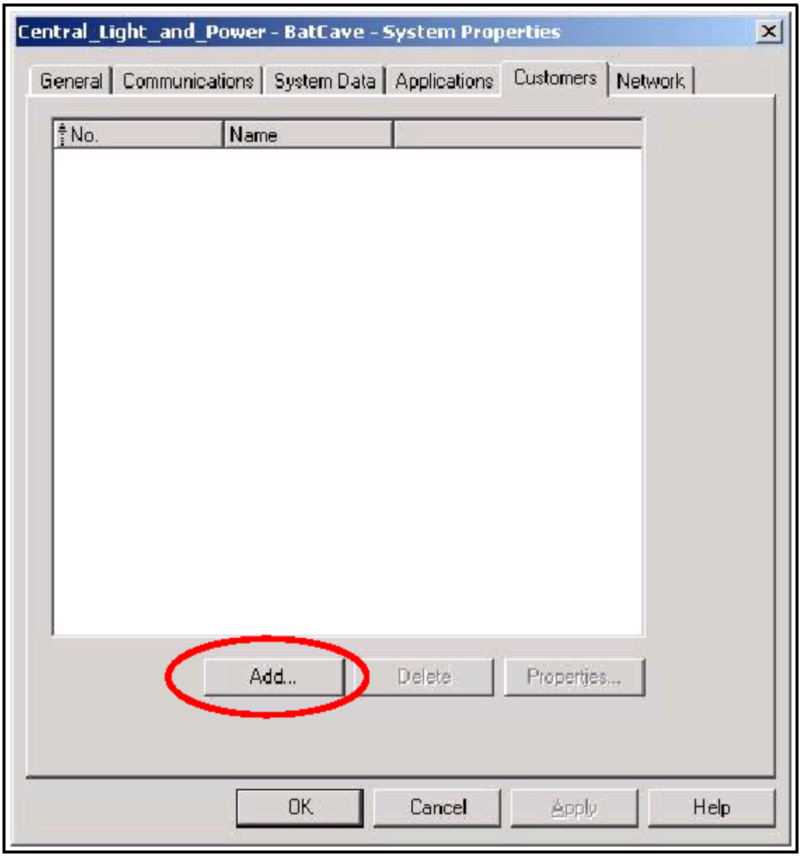
Enabled	Opt.	Code	Description
	1	OPTF	Extended PBX Features
	2	CUST	Multi-Customer
	3	AIOD	Auto.Inden.of Out.Dial
	4	CDR	Call Detail Recording
	5	CTY	CDR - TTY
	6	CLNK	CDR - Mag. Tape
	7	RAN	Recorded Announceme
	8	TAD	Time and Date
	9	DNDI	Do Not Disturb-Indiv

Provision the system customer information

7 Click the **Customers** tab. An empty **Customers** window appears. See Figure 82 on page 392.

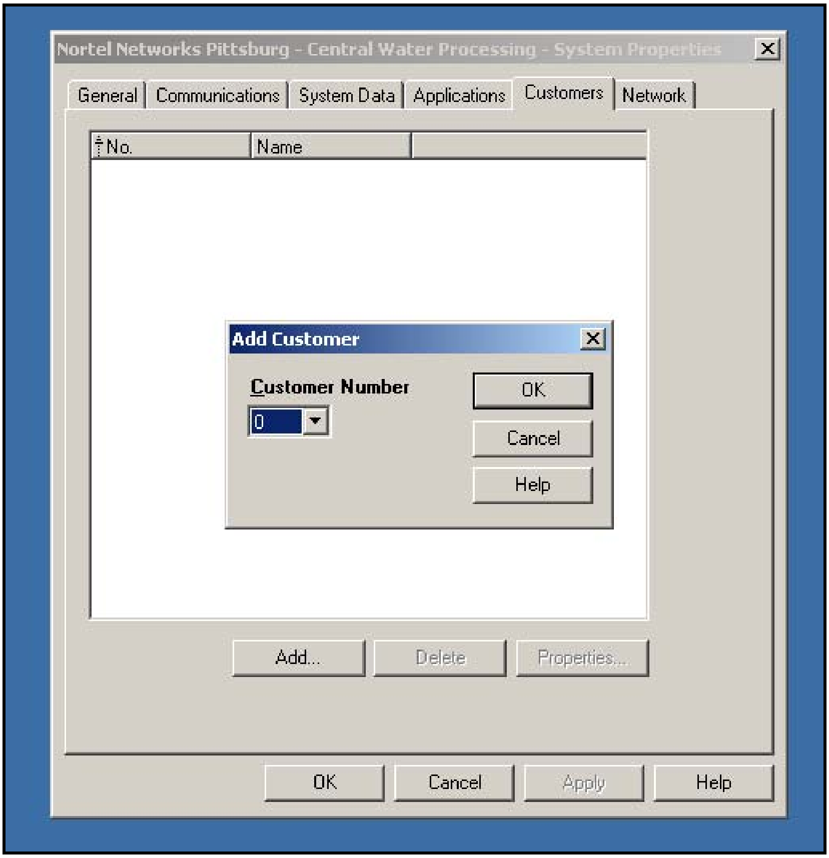
An IP trunk card cannot be provisioned unless it belongs to a system customer. Unless the system is to be administered through this interface, enter only the most basic customer number information.

Figure 82
Empty Customers window



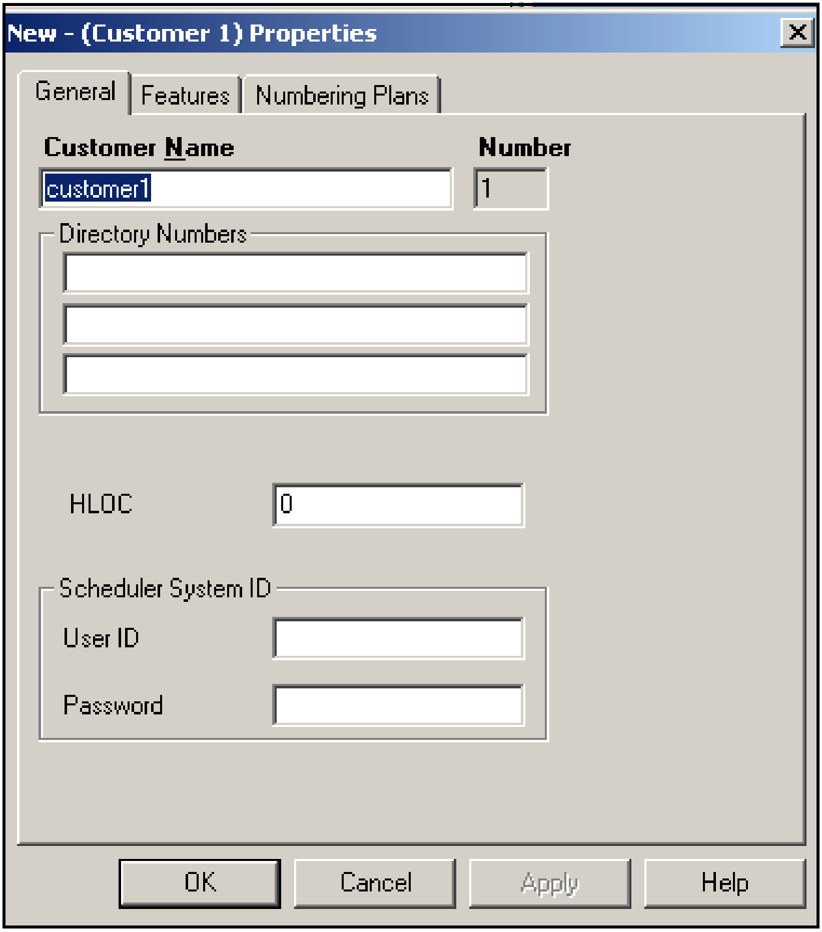
8 Click the **Add** button to add a customer. The **Add Customer** window opens. See Figure 83 on page 393.

Figure 83
Add Customer window



9 Use the **Customer Number** drop-down (pull-down) list to select the customer number. Click **OK**.
The **New – (Customer x) Properties** window opens. See Figure 84 on page 394.

Figure 84
New – (Customer x) Properties – General tab



New - (Customer 1) Properties

Customer Name: customer1

Number: 1

HLOC: 0

10 Enter the Directory Numbers and HLOC obtained from the system provisioning.

Note: The **Features** tab and the **Numbering Plans** tab are related to system provisioning. They are not used for IP Trunk 3.01 (and later).

11 Click **OK**.
The **New – (Customer x) Properties** window closes.

12 Click **OK** in the **System Properties** window.
The window closes and the **OTM Navigator** window is displayed.

End of Procedure

Change an existing system

Follow the steps in Procedure 43 to make changes to an existing system.

Procedure 43
Changing an existing system

1 Log in to the OTM Navigator.

The window displays two sections – Services and Sites. See Figure 67 on page 375.

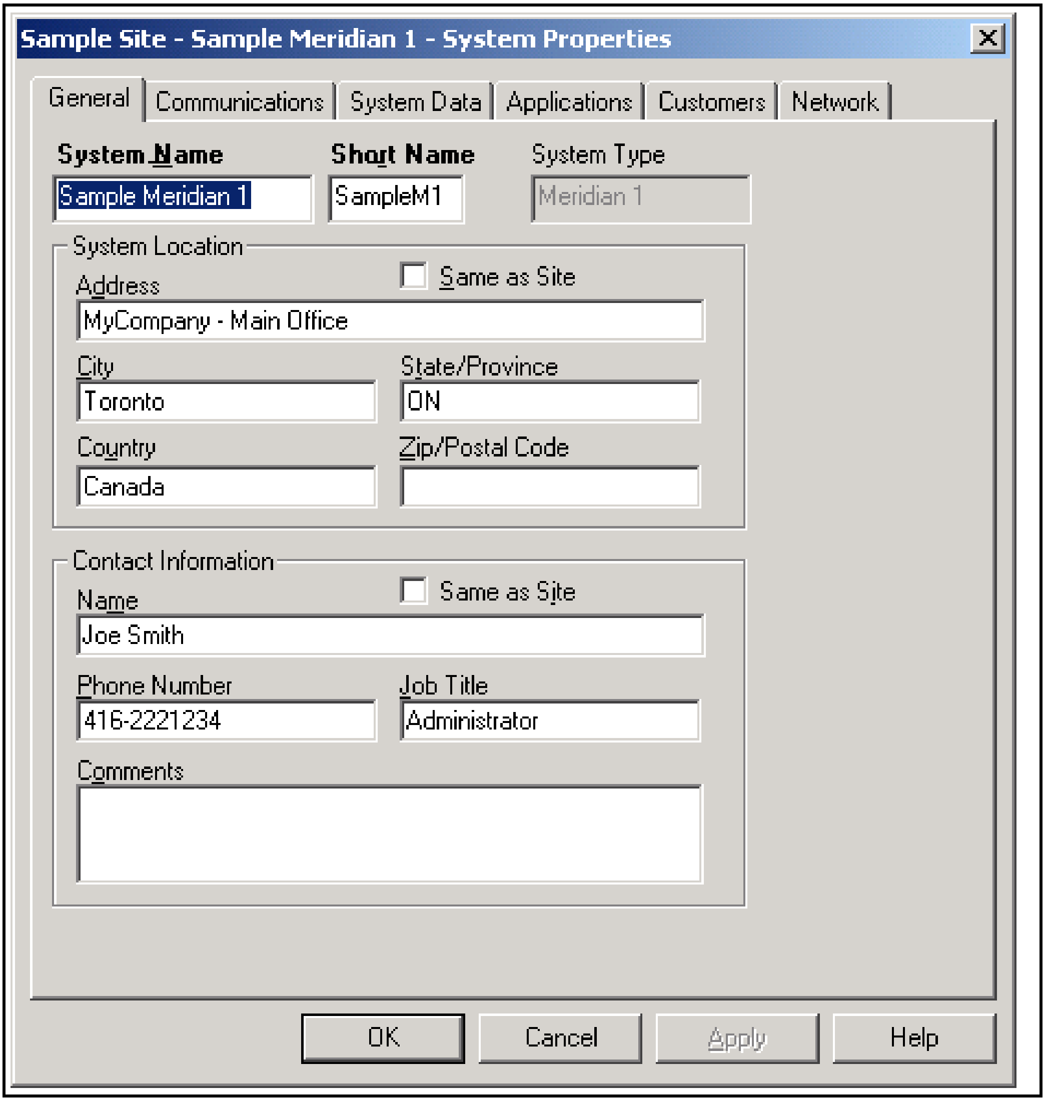
2 In the Site where the system is located, click the system to be changed.

3 Right-click the system and from the drop-down list, select **Properties**.

Alternatively, from the upper menu, click **File > Properties**.

The **System Properties** window opens. See Figure 85 on page 396.

Figure 85
System Properties window



System Name: Sample Meridian 1
Short Name: SampleM1
System Type: Meridian 1

System Location
□ Same as Site
Address: MyCompany - Main Office
City: Toronto
State/Province: ON
Country: Canada
Zip/Postal Code:

Contact Information
□ Same as Site
Name: Joe Smith
Phone Number: 416-2221234
Job Title: Administrator
Comments:

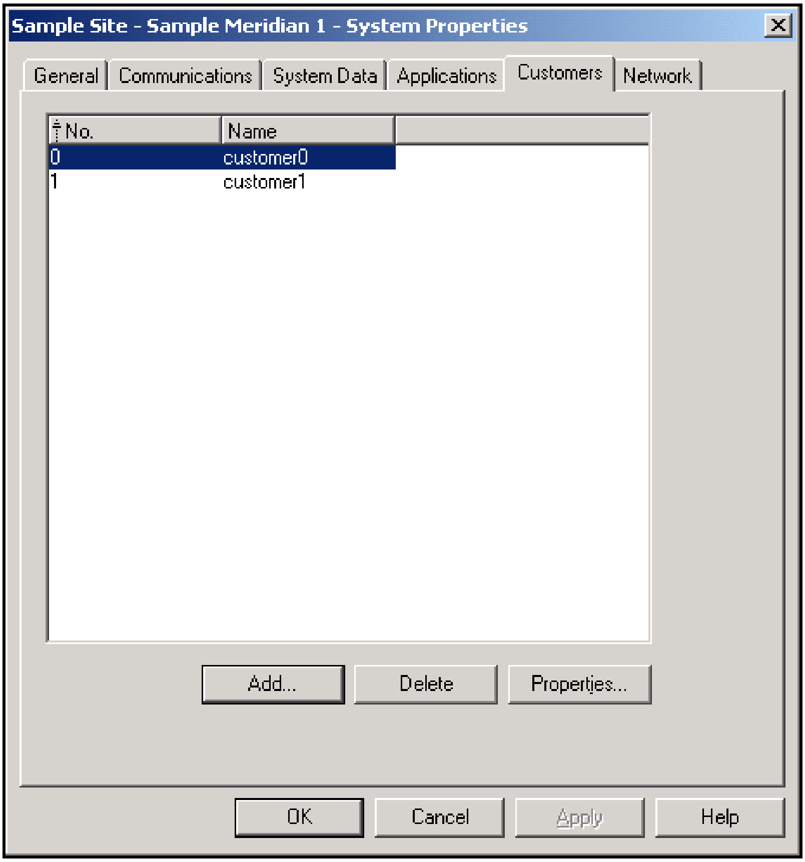
4 Enter the information that is being changed.

Change customer properties

5 To change a customer’s properties, click the **Customers** tab of the **System Properties** window, as seen in Figure 85.

6 Select the customer. See Figure 86.

Figure 86
System Properties – Customers tab

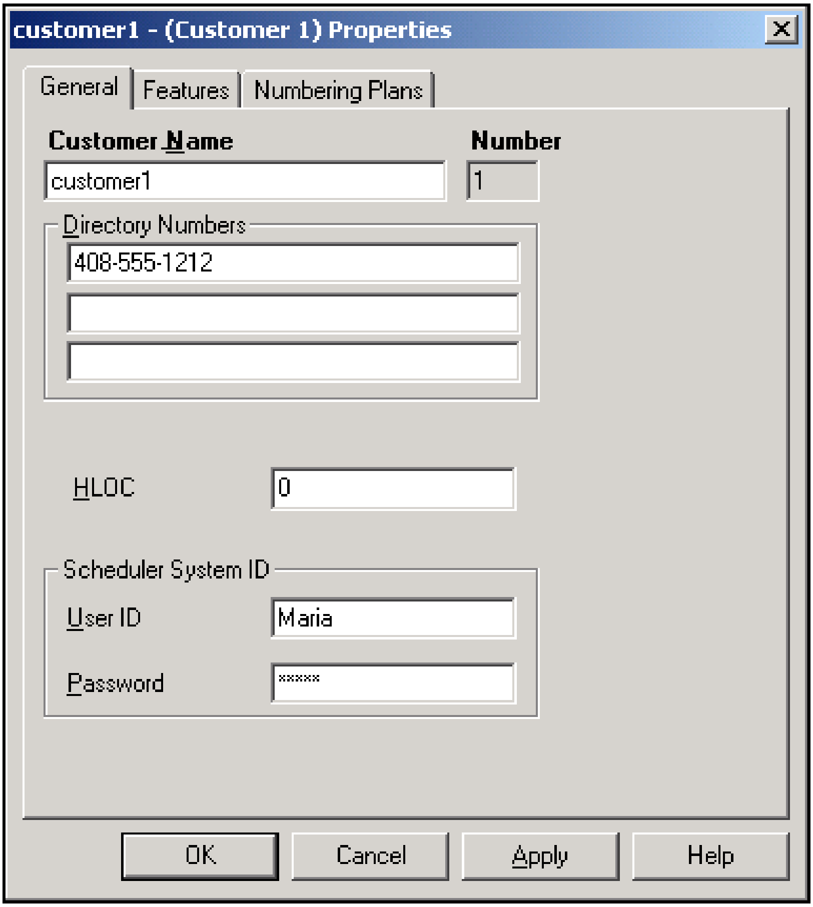


No.	Name
0	customer0
1	customer1

7 Click **Properties.**

Edit the customer's information in the **Customer Properties** window – General, Features, and Numbering Plans tabs. See Figure 87.

Figure 87
Customer Properties window



customer1 - (Customer 1) Properties

Customer Name: customer1
Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

Scheduler System ID
User ID: Maria
Password: *****

8 Click **OK** to save the customer information.

9 Click **OK** to save the system information.

End of Procedure

Delete a system

Follow the steps in Procedure 44 to delete a system.

Procedure 44
Deleting a system

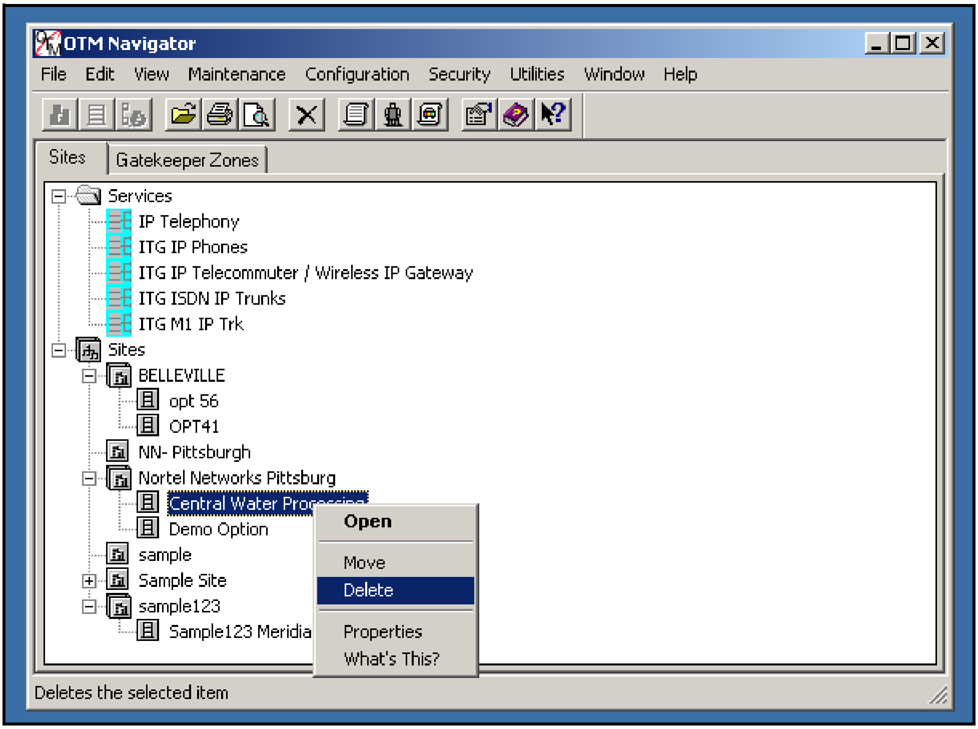
1 Log in to the OTM Navigator.

The window displays two sections – Services and Sites. See Figure 67 on page 375.

2 In the Sites section, locate and click the system to be deleted.

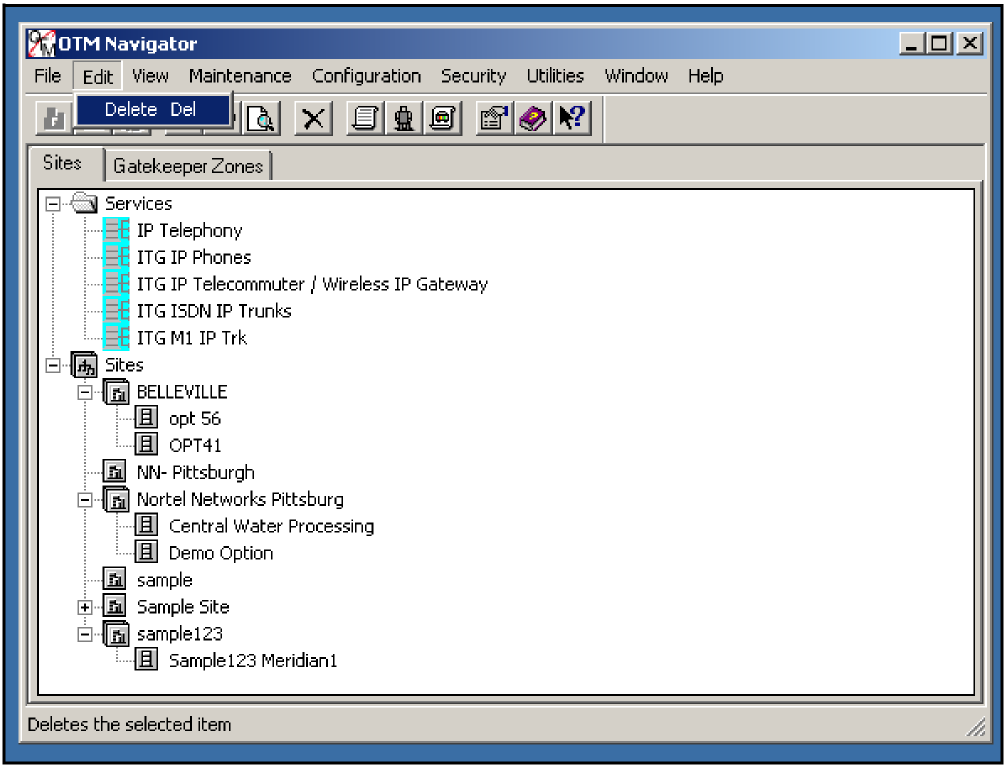
3 Right-click the system and from the drop-down list, select **Delete**. See Figure 88.

Figure 88
Delete a system



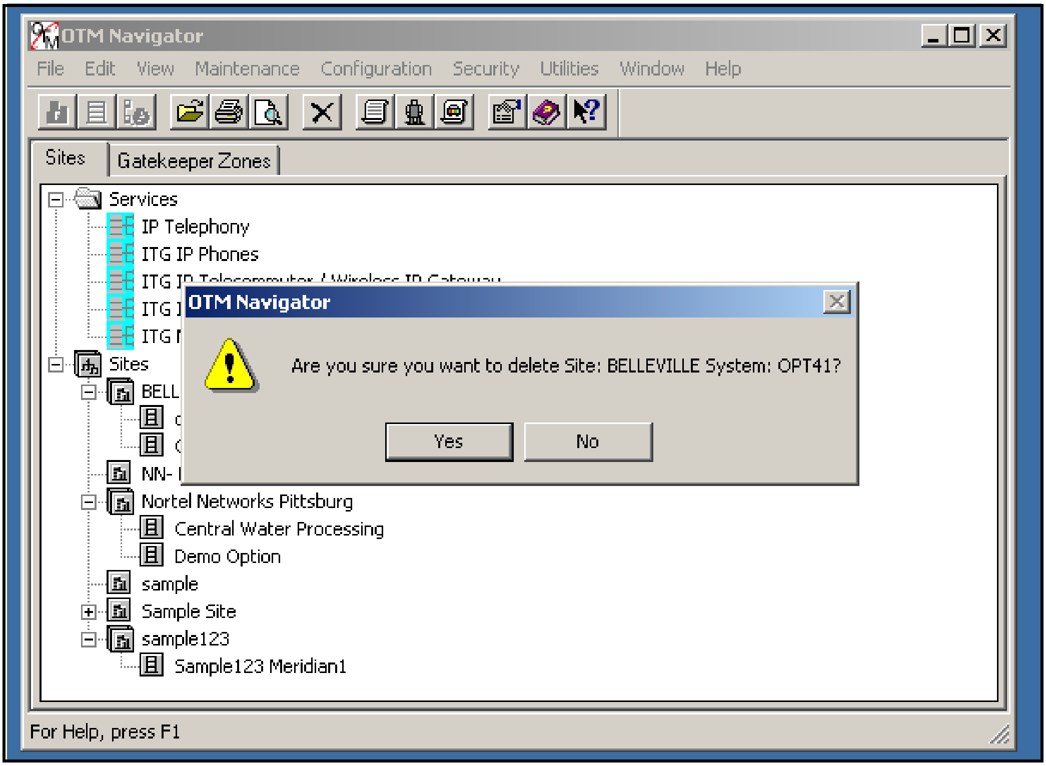
Alternatively, from the upper menu, click **Edit** > **Delete.** See Figure 89.

Figure 89
Alternative method of deleting a system



4 In the warning box that opens, click **Yes** to confirm the deletion. See Figure 90 on page 401.

Figure 90
Confirming the deletion



OTM Navigator

Are you sure you want to delete Site: BELLEVILLE System: OPT41?

Yes No

End of Procedure

Add an IP Trunk 3.01 (and later) node

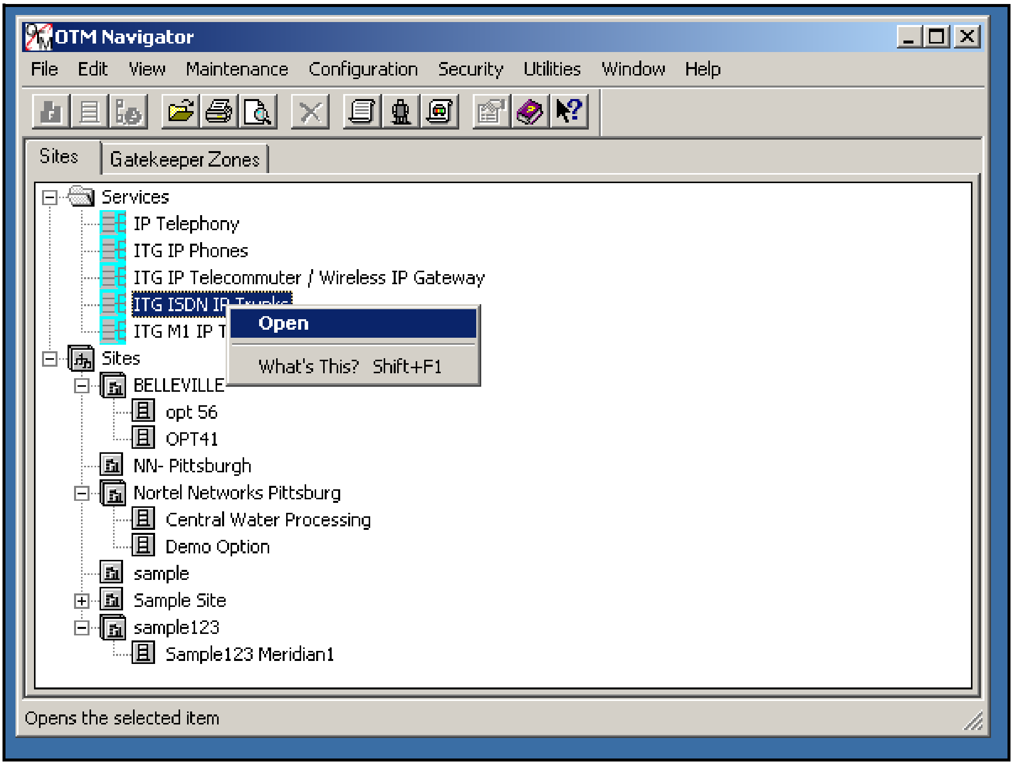
Follow the steps in Procedure 45 to add an IP Trunk 3.01 (and later) node.

Procedure 45
Adding an IP Trunk 3.01 (and later) node

1 In the **OTM Navigator** window, under Services, right-click **ITG ISDN IP Trunks.** A drop-down list appears.

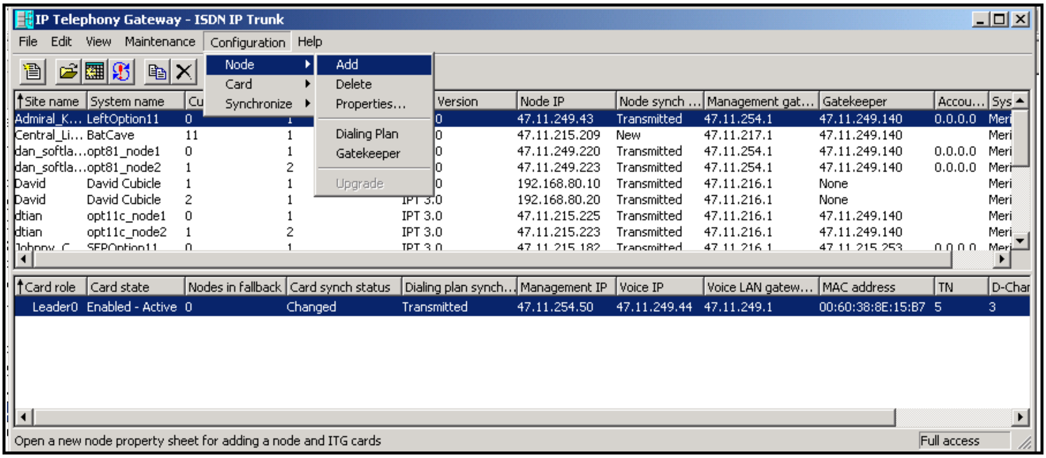
2 Click **Open**. See Figure 91 on page 402.

Figure 91
OTM Navigator – ITG ISDN IP Trunks service



The **IP Telephony Gateway – ISDN IP Trunk** window opens, as seen in Figure 92 on page 403. The smaller upper window lists the systems. The larger lower window lists all the cards in the selected system’s node.

Figure 92
ITG – ISDN IP Trunk window



Site name	System name	Cu		Version	Node IP	Node synch ...	Management gat...	Gatekeeper	Accou...	Sys
Admiral_K...	LeftOption11	0	1	0	47.11.249.43	Transmitted	47.11.254.1	47.11.249.140	0.0.0.0	Meri
Central_Li...	BatCave	11	1	0	47.11.215.209	New	47.11.217.1	47.11.249.140		Meri
dan_softla...	opt81_node1	0	1	0	47.11.249.220	Transmitted	47.11.254.1	47.11.249.140	0.0.0.0	Meri
dan_softla...	opt81_node2	1	2	0	47.11.249.223	Transmitted	47.11.254.1	47.11.249.140	0.0.0.0	Meri
David	David Cubicle	1	1	0	192.168.80.10	Transmitted	47.11.216.1	None		Meri
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None		Meri
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249.140		Meri
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249.140		Meri
Johnny_C	SFPOption11	0	1	IPT 3.0	47.11.215.182	Transmitted	47.11.216.1	47.11.215.253	0.0.0.0	Meri

Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address	TN	D-Char
Leader0	Enabled - Active	0	Changed	Transmitted	47.11.254.50	47.11.249.44	47.11.249.1	00:60:38:8E:15:B7	5	3

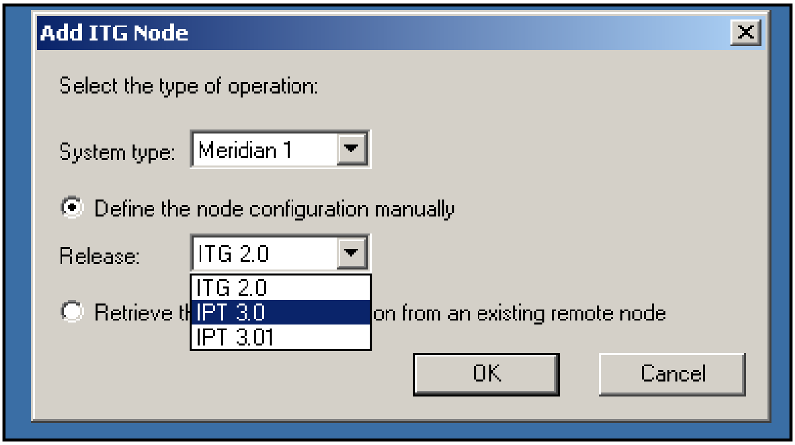
Open a new node property sheet for adding a node and ITG cards

Full access

3 From the **IP Telephony Gateway – ISDN IP Trunk** window menu bar, select **Configuration** > **Node** > **Add**.

The **Add ITG Node** dialog box shown in Figure 93 opens.

Figure 93
Add ITG Node dialog box



Select the type of operation:

System type: Meridian 1

● Define the node configuration manually

Release: ITG 2.0

ITG 2.0
IPT 3.0
IPT 3.01

○ Retrieve th… on from an existing remote node

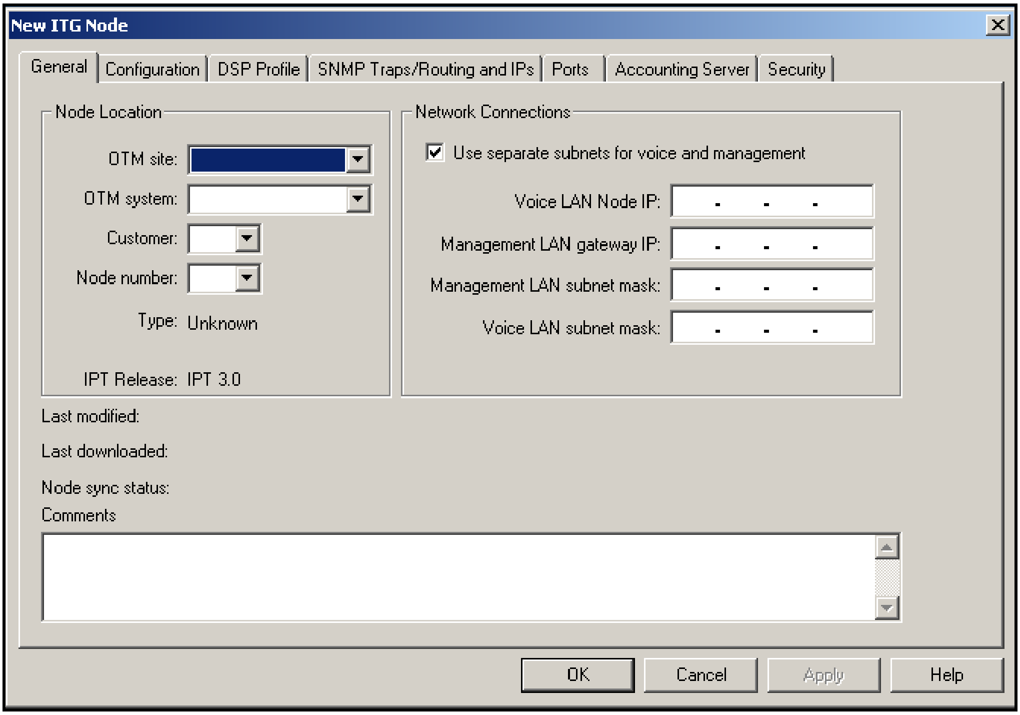
4 The **Add ITG Node** window indicates the system type. For IP Trunk 3.01 (and later), select Meridian 1 or MMCS.

5 Click a radio button to indicate whether to retrieve the information from an existing remote node, or to define the node configuration manually. Nortel recommends selecting the “Define the node configuration manually” radio button, as OTM generates comprehensive provisioning files, including the BOOTP.1 file, the CONFIG1.INI file, and all address resolution information.

6 Select the application release of the node to be defined from the drop-down list. Click **OK**.

The **New ITG Node** window opens. See Figure 94.

Figure 94
New ITG node – General tab



New ITG Node

☑ Use separate subnets for voice and management

Type: Unknown

IPT Release: IPT 3.0

7 On the **General** tab, on the left side of the window, define the following from the drop-down lists:

- The OTM site – the name that was assigned when the site was created. See “Add a site and system” on page 374.
- The OTM system name – the name of the system associated with this site. See “Add a system” on page 384.
- The Customer number.
- The Node number – there might be several nodes; this differentiates between them.

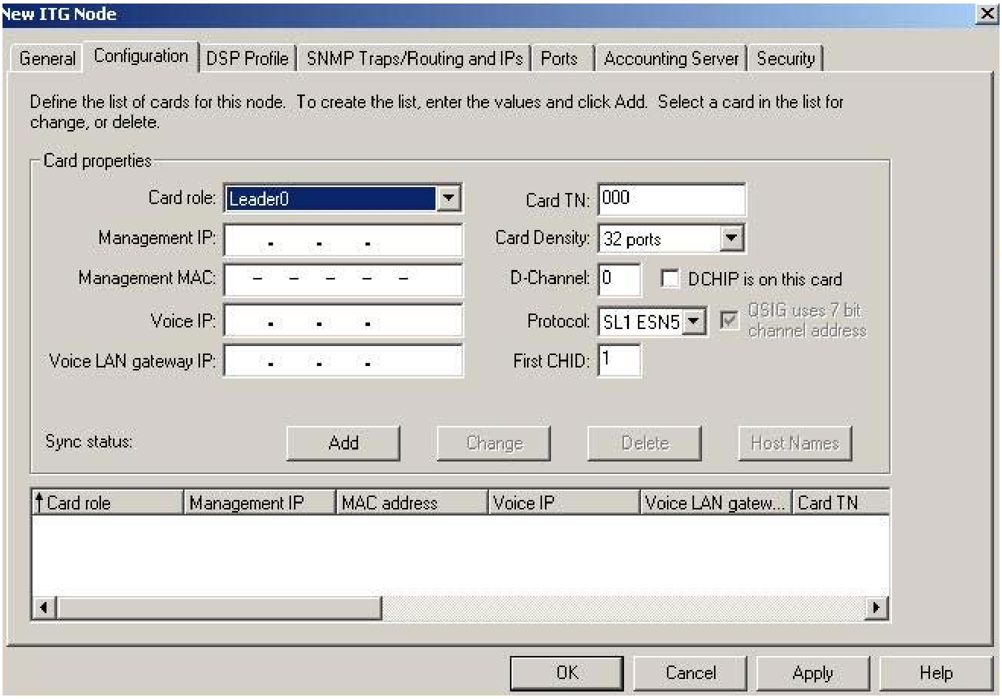
8 On the right side of the window, enter the following information:

- Voice LAN Node IP – the Leader IP address for call processing
- Management LAN gateway IP – the lowest valid IP address on the LAN segment of the Management Server
- Management LAN subnet mask – the ELAN subnet mask
- Voice LAN subnet mask – the TLAN subnet mask

Provision the IP trunk cards

9 Click the **Configuration** tab. This is where the IP trunk cards are provisioned. See Figure 95.

Figure 95
New ITG Node - Configuration tab



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card role: Leader0

Management IP: . . .

Management MAC: - - - - -

Voice IP: . . .

Voice LAN gateway IP: . . .

Card TN: 000

Card Density: 32 ports

D-Channel: 0 ☐ DCHIP is on this card

Protocol: SL1 ESN5 ☑ QSIG uses 7 bit channel address

First CHID: 1

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN

A minimum of one IP trunk card, Leader 0, must be defined. This card acts as the leader card on startup and remains as leader until it suffers some sort of failure that would require changeover to the Backup Leader card.

Note: OTM 2.1 (and later) requires that the second card that is provisioned be configured as Leader 1 (Backup Leader). Leader 1 must be configured before any Follower cards are provisioned.

10 Enter the appropriate data in the following fields:

- Card role – the default is Leader 0, indicating that this is the primary leader. Other options include Leader 1 (Backup) and Follower.
- Management IP – the IP trunk card ELAN network interface IP address

Note: The MAC address entered must match the IP trunk card's MAC address, or the card cannot be used. The MAC address is unique to every card and if the address is entered is incorrect, the OTM server cannot send any information to the IP trunk card.

- Management MAC – the IP trunk card ELAN MAC address
- Voice IP – the IP trunk card's TLAN network interface IP address for RTP and H.323 messaging
- Voice LAN gateway IP – the lowest IP address on the TLAN subnet
- Card TN – the first three numbers (loop/shelf/card). The exception is the Meridian 1 Option 11C Cabinet and CS 1000M Cabinet which is only "card".
- Card density – 24- or 32-port IP trunk card
- D-channel – the D-channel on the system. If the D-channel card resides on this IP trunk card, check the DCHIP box.
- Protocol – the local protocol. For IP Trunk 3.01 (and later) to interwork with CS 1000S/1000M, the protocol must be SL1 or SL1 with ESN, as H.323-compatible gateways do not understand QSIG.

The **QSIG** checkbox enables IP Trunk 3.01 to be configured with a QSIG channel address length of 7 bits for Primary Rate D-Channels or 8 bits for an ISL D-Channel used in prior releases of IP Trunk software. The **QSIG** checkbox is checked or unchecked by default, depending on the software release running on the system. The checkbox is enabled only when the selected protocol is QSIG (ESGF or ISGF) and the node version is IP Trunk 3.01.

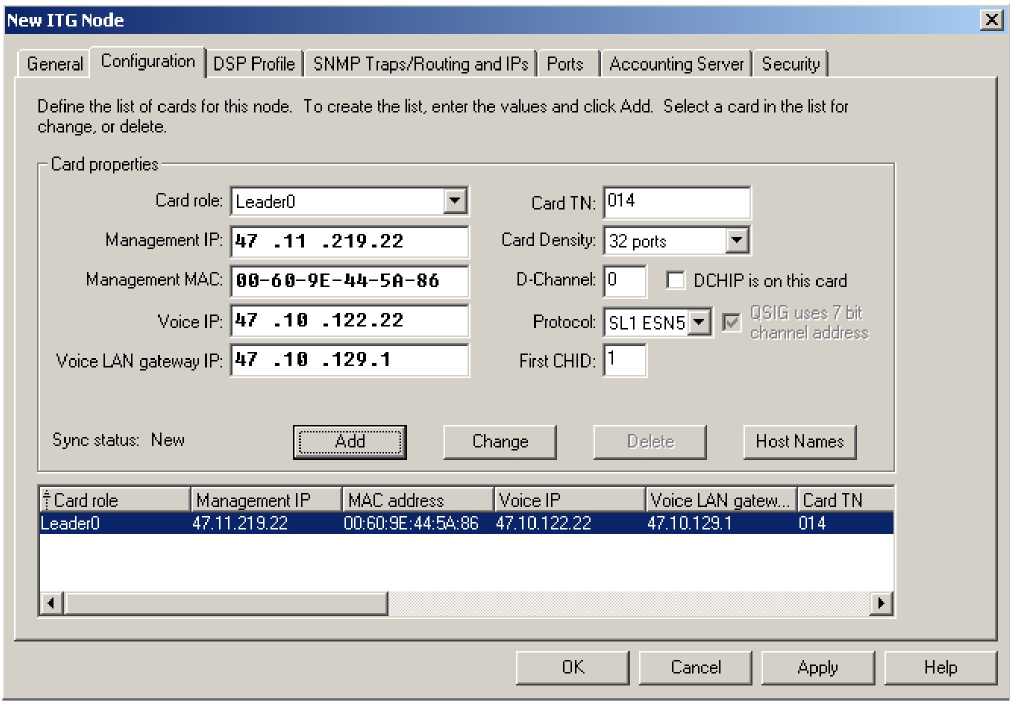
- First CHID 0 – the first channel number. All other channels autonumber in increasing order.

11 Click **Add** to define the card.

Note: Clicking **Add** does not add the D-channel or card to the system; it only adds the IP trunk card information. The system must still be provisioned separately.

When **Add** is clicked, the lower card information window displays the saved card information. See Figure 96.

Figure 96
New ITG Node – Configuration tab window with Leader 0 provisioned



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

Card role: Leader0
Management IP: 47 .11 .219.22
Management MAC: 00-60-9E-44-5A-86
Voice IP: 47 .10 .122.22
Voice LAN gateway IP: 47 .10 .129.1
Card TN: 014
Card Density: 32 ports
D-Channel: 0 □ DCHIP is on this card
Protocol: SL1 ESN5 ☑ QSIG uses 7 bit channel address
First CHID: 1

Sync status: New

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.219.22	00:60:9E:44:5A:86	47.10.122.22	47.10.129.1	014

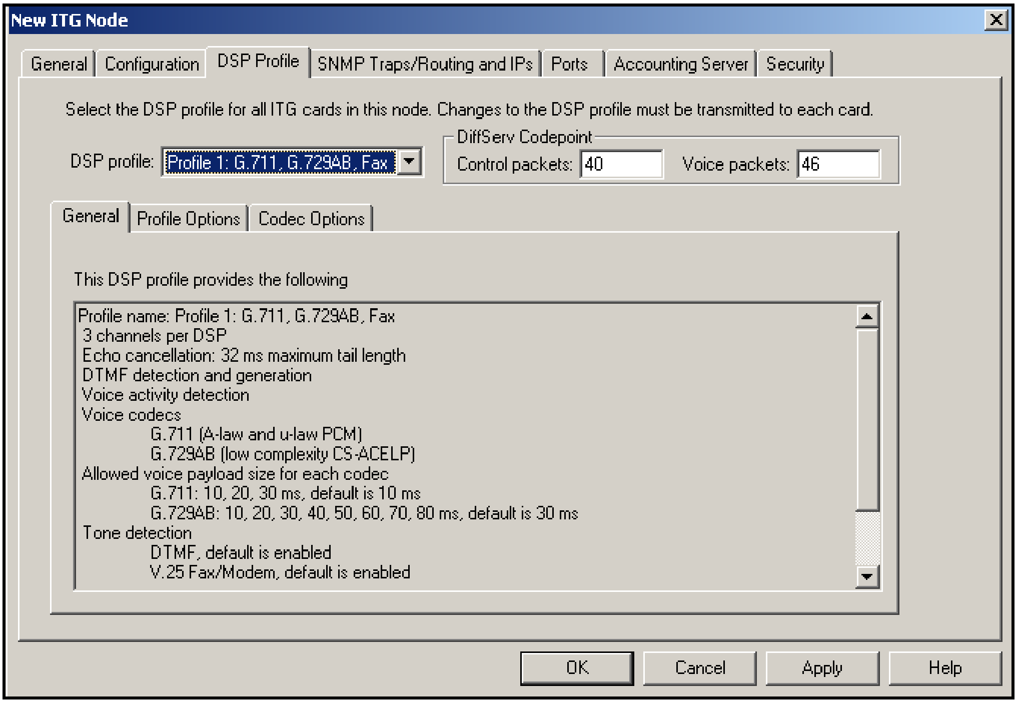
In the window, where the saved card data is displayed, the column width can be increased or decreased to see more or less information. Use the scroll bar slider to see more information hidden from view. If more than one card is listed in the window, selecting a card enables OTM to display that card's configuration in the applicable fields in the data entry section.

Provision the DSP data

12 Click the **DSP Profile** tab of the **New ITG Node** window to provision the DSP data. See Figure 97 on page 409.

The Control packets and Voice packets can be assigned a different DIFFSERV/TOS value to assist in QoS in the IP network. Only change these values if it is found to be necessary and ensure that all network routers have been updated with the new TOS value. For more information see "IP Trunk 3.01 (and later) DiffServ support for IP QoS" on page 177.

Figure 97
New ITG Node – DSP Profile tab - General sub-tab - Profile 1



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40
Voice packets: 46

This DSP profile provides the following

Profile name: Profile 1: G.711, G.729AB, Fax
3 channels per DSP
Echo cancellation: 32 ms maximum tail length
DTMF detection and generation
Voice activity detection
Voice codecs
G.711 (A-law and u-law PCM)
G.729AB (low complexity CS-ACELP)
Allowed voice payload size for each codec
G.711: 10, 20, 30 ms, default is 10 ms
G.729AB: 10, 20, 30, 40, 50, 60, 70, 80 ms, default is 30 ms
Tone detection
DTMF, default is enabled
V.25 Fax/Modem, default is enabled

13 Select the applicable DSP Profile information. There are three choices in the **DSP Profile** drop-down list, as seen in Figure 97. Click **Apply.**

CAUTION — Service Interruption

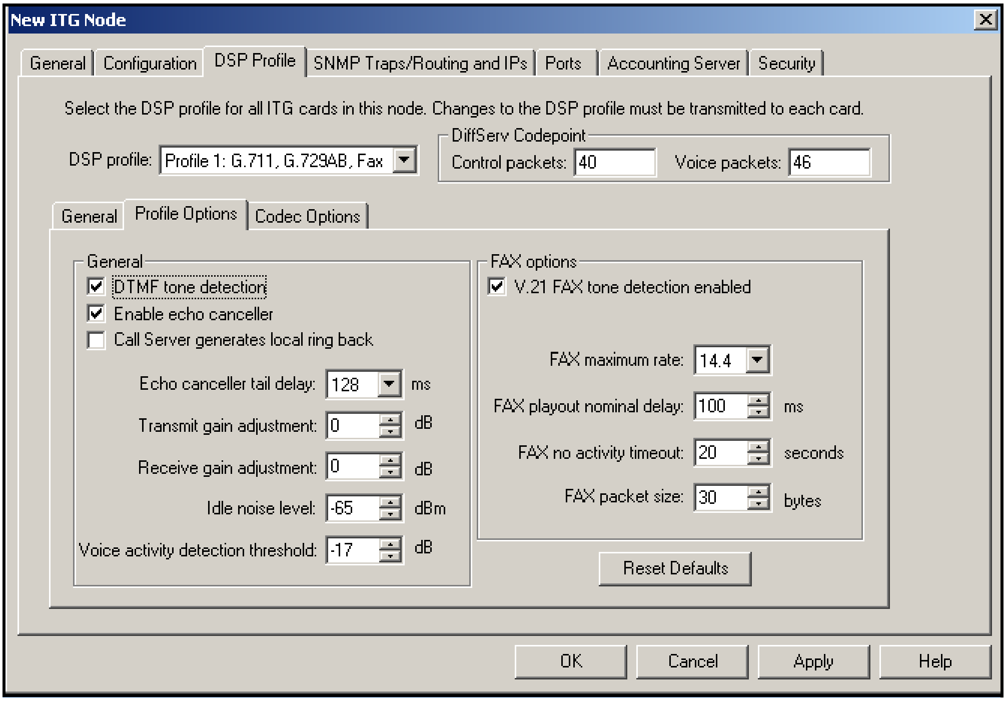
The Media Card 32-port trunk card does not support Profile 3. If Profile 3 is provisioned, the card is unable to make or receive calls.

The DSP Profile values appear. See Figure 98.

Some of the values that can be changed are:

- DTMF tone detection – for voice mail access and IVR, for example. Allows DTMF tones to be reliably transmitted across the network. See “DTMF Through Dial” on page 103.
- Enable echo canceller – enables echo in calls, on by default
- Echo canceller tail delay – by default, the value is 128 ms
- V.21 fax tone detection – allows fax calls to be transmitted as data and not as voice packets. When the fax call is transmitted as data (T.30), the call has a much greater chance of success.

Figure 98
DSP Profile sub-tabs – Profile 1 Options sub-tab



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40
Voice packets: 46

General
☑ DTMF tone detection
☑ Enable echo canceller
☐ Call Server generates local ring back

Echo canceller tail delay: 128 ms
Transmit gain adjustment: 0 dB
Receive gain adjustment: 0 dB
Idle noise level: -65 dBm
Voice activity detection threshold: -17 dB

FAX options
☑ V.21 FAX tone detection enabled

FAX maximum rate: 14.4
FAX playout nominal delay: 100 ms
FAX no activity timeout: 20 seconds
FAX packet size: 30 bytes

Note: OTM 2.1 (and later) does not permit “V.25 Fax/Modem tone detection enabled” for IP Trunk 3.01 (and later) and ITG Trunk 2.x. This is because the IP trunk cards do not have a mechanism for properly handling modem calls. IP Trunk 3.01 (and later) does not officially support modem calls. The only way modem calls can be made is if G.711 is the first choice for both endpoints. Even then, modem calls might still be lost due to latency and packet loss, which is inherent with IP networks.

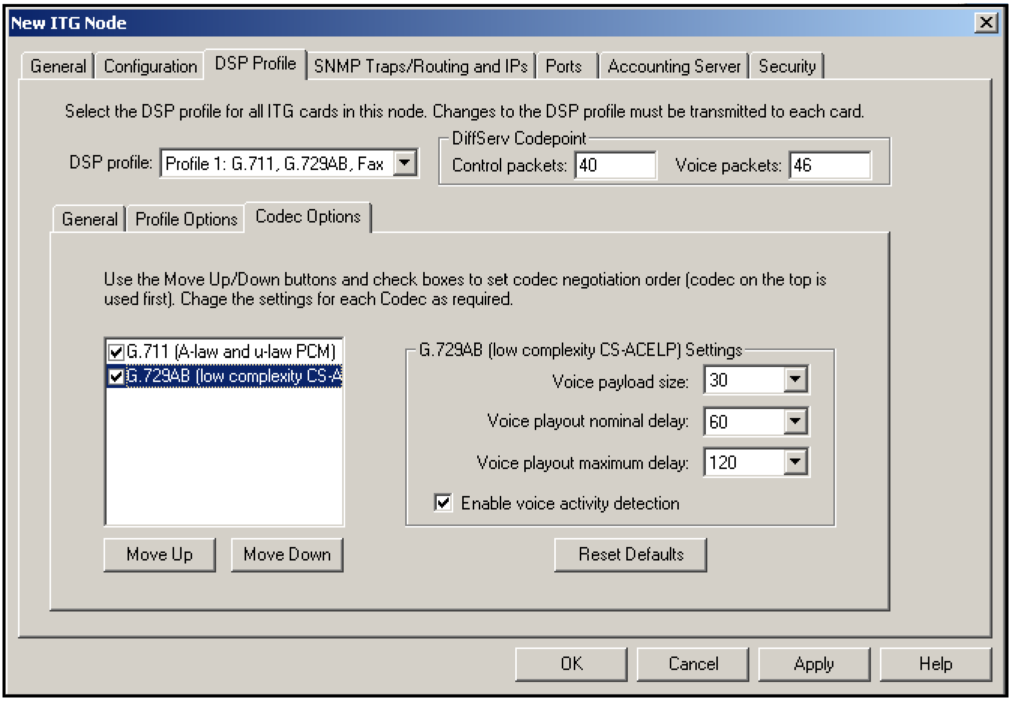
Fax calls using the “V.21 Fax tone detection” (14.4 baud and below) are supported.

Codec options

14 Place the codecs in the preferred sequence (most desirable to least desirable). Configure the payload size and delay settings.

15 Click the check box to enable or disable Voice Activity Detection (VAD). See Figure 99 on page 412.

Figure 99
New ITG Node – DSP Profile tab - Codec sub-tab



Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40
Voice packets: 46

Use the Move Up/Down buttons and check boxes to set codec negotiation order (codec on the top is used first). Chage the settings for each Codec as required.

☑ G.711 (A-law and u-law PCM)
☑ G.729AB (low complexity CS-A

G.729AB (low complexity CS-ACELP) Settings
Voice payload size: 30
Voice playout nominal delay: 60
Voice playout maximum delay: 120
☑ Enable voice activity detection

WARNING

Do not turn off G.711, unless there is no other alternative. Some IP devices use G.723 and G.711, some devices use G.729 and G.711, and some devices support all three codecs. If this node were configured with only G.723, for example, and a device configured with G.729 and G.711 attempted to place a call to this node, the call would fail, because no matching codec exists.

Always include G.711, even if it is listed as the last choice, unless it is impossible to use G.711 due to bandwidth restrictions.

VAD

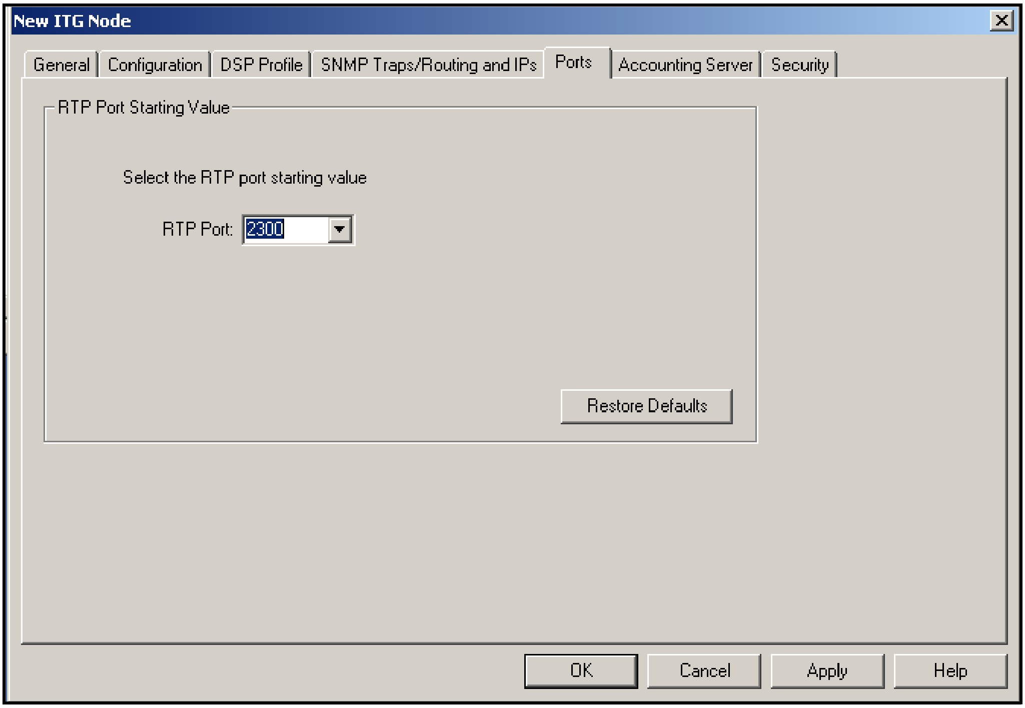
Figure 99 on page 412 shows a DSP Profile with VAD enabled for the G.711. This is the default setting for OTM 2.1 (and later).

16 When G.711 is selected as the codec option and the only remote device on the network is an ITG 2.x trunk or an IP 3.0 trunk, then the VAD setting can be left enabled. If the IP Trunk 3.01 (and later) node will interwork with CS 1000S and CS 1000M, disable VAD. Only devices at the remote end of a small number of gateways can perform VAD and understand the pertinent signaling.

Select an RTP port

17 Click the **Ports** tab. See Figure 100.

Figure 100
New ITG Node – Ports tab



RTP Port Starting Value

Select the RTP port starting value

RTP Port: 2300

18 This tab is only present for IP Trunk 3.01 (and later) nodes. Use the drop-down list to select the RTP port starting value. There are two options, as follows:

- 2300 – default value
- 17300 – used for Cisco RTP header compression

Alternatively, enter any even-numbered port starting value between 1024 and 65534.

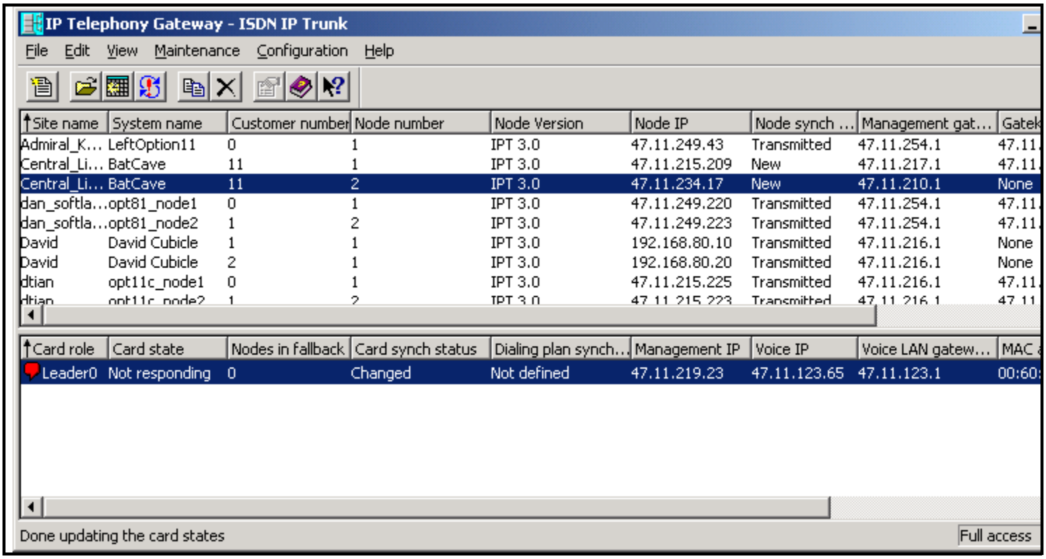
> **WARNING**
>
> Entering a starting port value other than 2300 or 17300 does not block calls, but can result in unexpected behavior, as certain port ranges are reserved by the IETF.
>
> Cisco header compression can be used only if a starting port value is entered that is equal to or greater than 17300.

Click the **Restore Default** button to restore the default port start value.

Add the node

19 Click **OK** to complete the node provisioning. The **ITG Node Properties** window closes. The node data is now displayed in the **ITG – ISDN IP Trunk** window. See Figure 101 on page 415.

Figure 101
ITG – ISDN IP Trunk window with new node displayed



Site name	System name	Customer number	Node number	Node Version	Node IP	Node synch ...	Management gat...	Gatek
Admiral_K...	LeftOption11	0	1	IPT 3.0	47.11.249.43	Transmitted	47.11.254.1	47.11.
Central_Li...	BatCave	11	1	IPT 3.0	47.11.215.209	New	47.11.217.1	47.11.
Central_Li...	BatCave	11	2	IPT 3.0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1	0	1	IPT 3.0	47.11.249.220	Transmitted	47.11.254.1	47.11.
dan_softla...	opt81_node2	1	2	IPT 3.0	47.11.249.223	Transmitted	47.11.254.1	47.11.
David	David Cubicle	1	1	IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11

Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC a
Leader0	Not responding	0	Changed	Not defined	47.11.219.23	47.11.123.65	47.11.123.1	00:60:

Done updating the card states

Full access

End of Procedure

Edit a node

Follow the steps in Procedure 46 to edit a node’s information.

Procedure 46
Editing a node

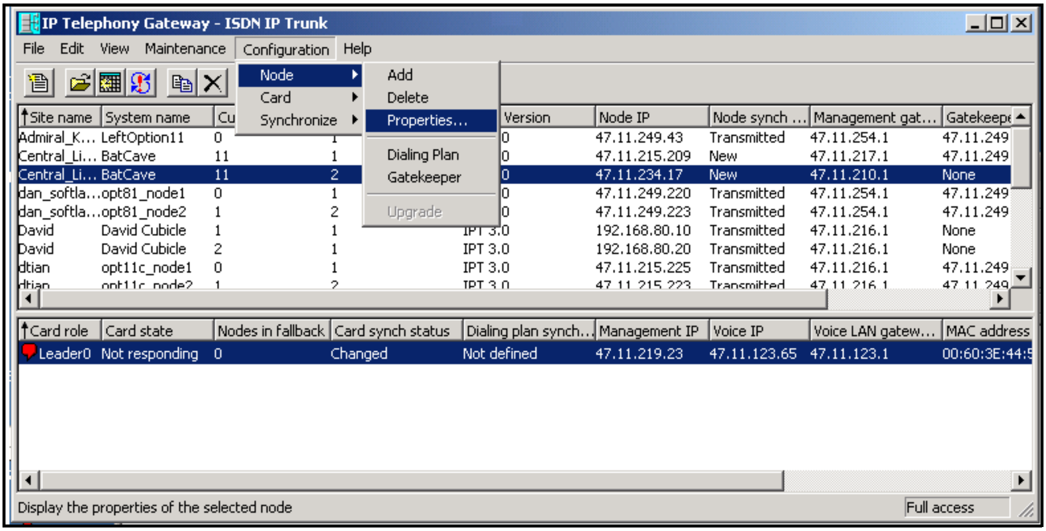
1 In the **OTM Navigator** window, under Services, right-click **ITG ISDN IP Trunks.** A drop-down list appears.

2 Click **Open.** See Figure 91 on page 402.

The **IP Telephony Gateway – ISDN IP Trunk** window opens, as seen in Figure 92 on page 403. The smaller upper window lists the systems. The larger lower window lists all the cards in the selected system’s node.

3 In the window, select the node to be edited from the list.
From the upper menu, click **Configuration > Properties**. See Figure 102 on page 416.

Figure 102
Change node properties



Site name	System name	Cu		Version	Node IP	Node synch ...	Management gat...	Gatekeepe
Admiral_K...	LeftOption11	0	1	0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave	11	1	0	47.11.215.209	New	47.11.217.1	47.11.249
Central_Li...	BatCave	11	2	0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1	0	1	0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_node2	1	2	0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cubicle	1	1	IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249

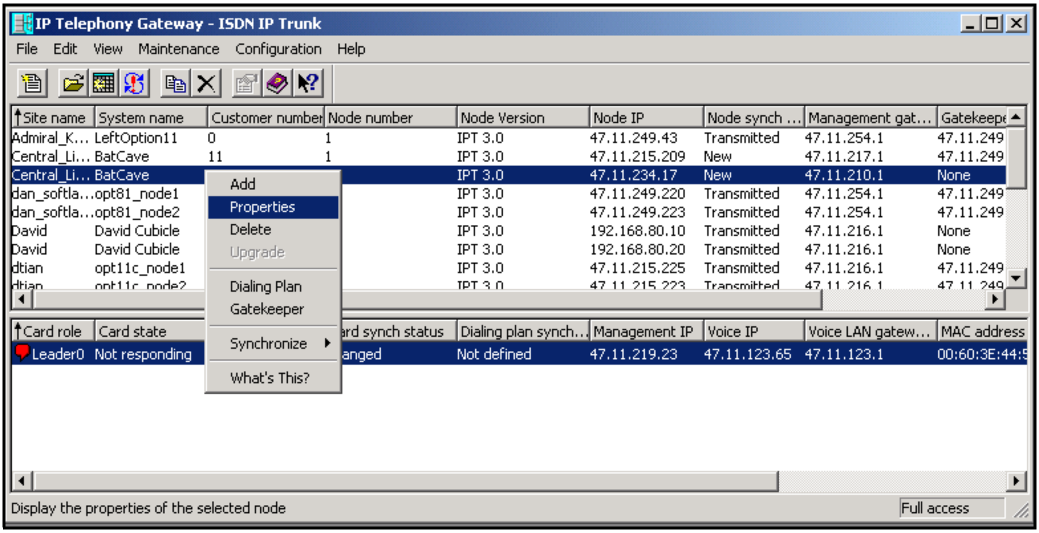
Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Leader0	Not responding	0	Changed	Not defined	47.11.219.23	47.11.123.65	47.11.123.1	00:60:3E:44:5

Display the properties of the selected node

Full access

4 Alternatively, right-click the node to be edited, the select **Properties** from the pop-up menu. See Figure 103 on page 417.

Figure 103
Alternative method of selecting node to be edited



Site name	System name	Customer number	Node number	Node Version	Node IP	Node synch ...	Management gat...	Gatekeepe
Admiral_K...	LeftOption11	0	1	IPT 3.0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave	11	1	IPT 3.0	47.11.215.209	New	47.11.217.1	47.11.249
Central_Li...	BatCave			IPT 3.0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1			IPT 3.0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_node2			IPT 3.0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cubicle			IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle			IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1			IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_node2			IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249

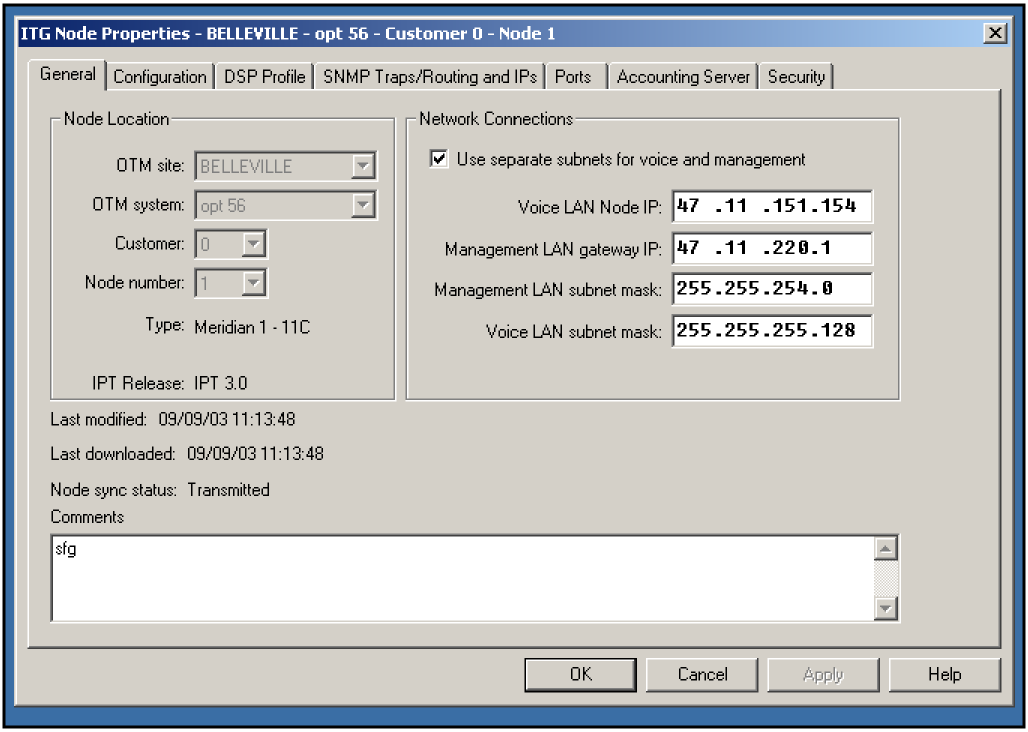
Card role	Card state		rd synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Leader0	Not responding		anged	Not defined	47.11.219.23	47.11.123.65	47.11.123.1	00:60:3E:44:5

Display the properties of the selected node

Full access

5 The **Node Properties** window opens. The **Node Properties** window has six tabs. Select the applicable tab to change the data associated with that section of the node. See Figure 104 on page 418.

Figure 104
ITG Node Properties – General tab



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Node Location

OTM site: BELLEVILLE

OTM system: opt 56

Customer: 0

Node number: 1

Type: Meridian 1 - 11C

IPT Release: IPT 3.0

Network Connections

☑ Use separate subnets for voice and management

Voice LAN Node IP: 47 .11 .151.154

Management LAN gateway IP: 47 .11 .220.1

Management LAN subnet mask: 255.255.254.0

Voice LAN subnet mask: 255.255.255.128

Last modified: 09/09/03 11:13:48

Last downloaded: 09/09/03 11:13:48

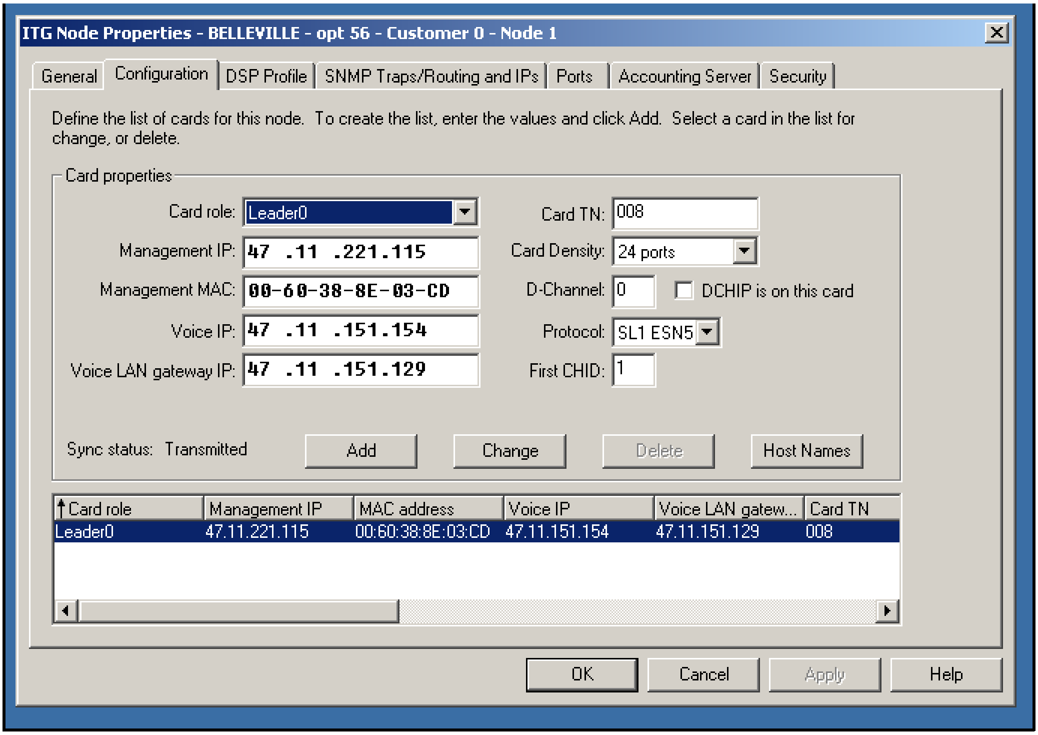
Node sync status: Transmitted

Comments

sfg

6 To add a new IP trunk card, select the **Configuration** tab. Select the correct card role for the new IP trunk card. Leader 1 (Backup Leader) must be selected before Follower cards. See Figure 105 on page 419.

Figure 105
ITG Node Properties – Configuration tab



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

Card role: Leader0
Management IP: 47 .11 .221.115
Management MAC: 00-60-38-8E-03-CD
Voice IP: 47 .11 .151.154
Voice LAN gateway IP: 47 .11 .151.129
Card TN: 008
Card Density: 24 ports
D-Channel: 0
□ DCHIP is on this card
Protocol: SL1 ESN5
First CHID: 1

Sync status: Transmitted

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008

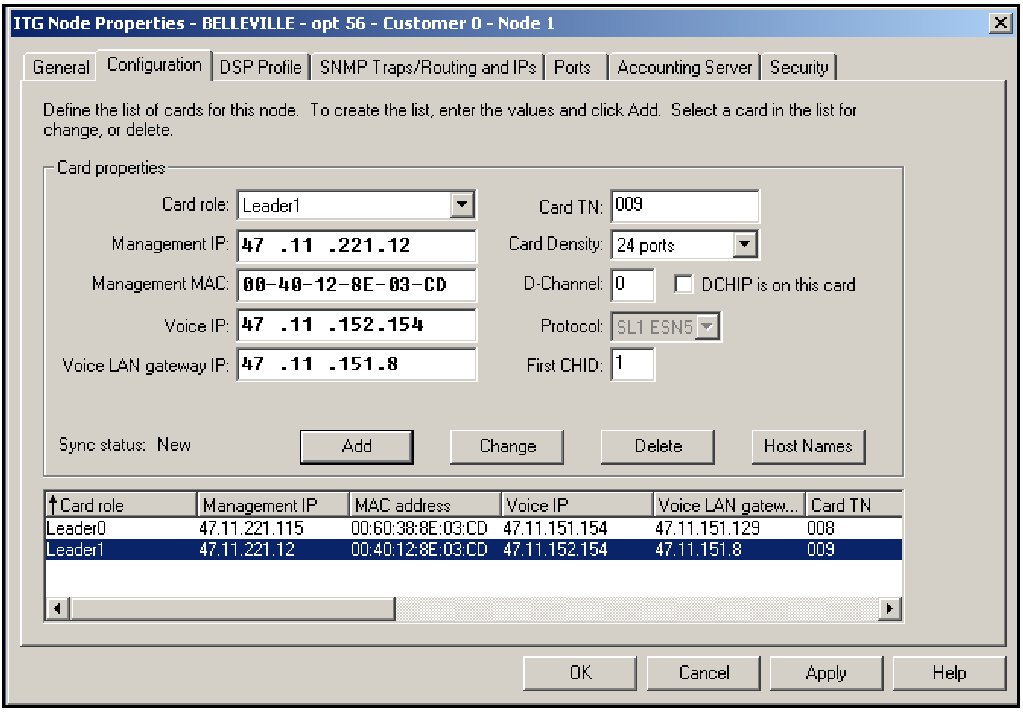
7 Enter the required data. Note that, compared to the Leader 0 configuration

- the Management (ELAN network interface) IP address, the Voice (TLAN network interface) IP address, and the Management (ELAN network interface) MAC address have changed
- the TN is different (4-0-10)
- the first channel ID has changed (1 to 33)

See Figure 106 on page 420.

Click **Add.**

Figure 106
Leader 1 (Backup Leader) sample configuration



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card role: Leader1
Management IP: 47 .11 .221.12
Management MAC: 00-40-12-8E-03-CD
Voice IP: 47 .11 .152.154
Voice LAN gateway IP: 47 .11 .151.8
Card TN: 009
Card Density: 24 ports
D-Channel: 0
□ DCHIP is on this card
Protocol: SL1 ESN5
First CHID: 1

Sync status: New

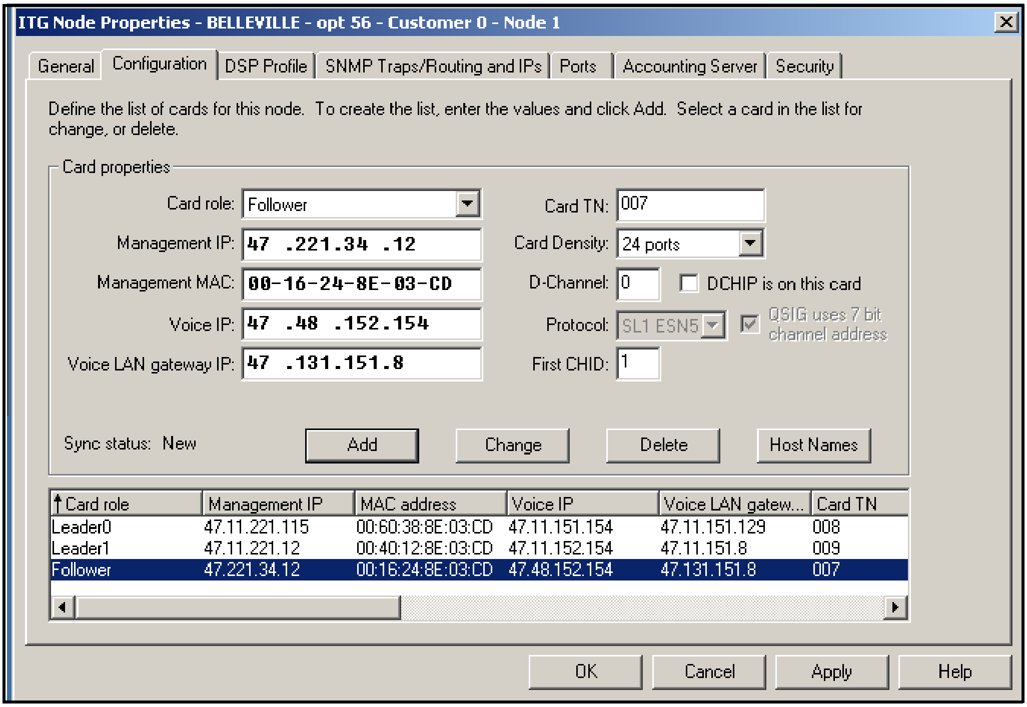
Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008
Leader1	47.11.221.12	00:40:12:8E:03:CD	47.11.152.154	47.11.151.8	009

8 To edit an IP trunk card, select the **Configuration** tab. Select the desired IP trunk card in the lower window.

In the example shown in Figure 107 on page 421, the Follower card is edited to change the D-channel. A second D-channel, D-channel 8, is on this card; the original D-channel was “7”.

Click **Change** (above the lower window) to accept the change.

Figure 107
Editing an IP trunk card in a node



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

Card role: Follower

Management IP: 47 .221.34 .12

Management MAC: 00-16-24-8E-03-CD

Voice IP: 47 .48 .152.154

Voice LAN gateway IP: 47 .131.151.8

Card TN: 007

Card Density: 24 ports

D-Channel: 0 □ DCHIP is on this card

Protocol: SL1 ESN5 ☑ QSIG uses 7 bit channel address

First CHID: 1

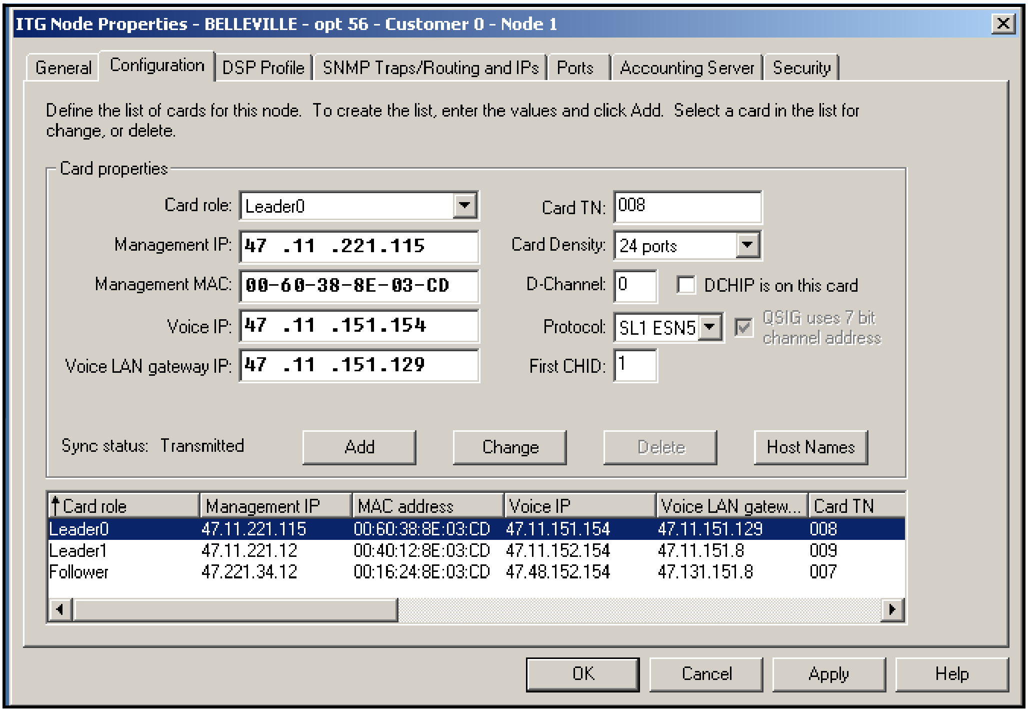
Sync status: New

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008
Leader1	47.11.221.12	00:40:12:8E:03:CD	47.11.152.154	47.11.151.8	009
Follower	47.221.34.12	00:16:24:8E:03:CD	47.48.152.154	47.131.151.8	007

9 To delete an IP trunk card from the node, select the desired card and click **Delete**.

The **Delete** button is greyed out if the card cannot be deleted; for example the Leader 0 card cannot be deleted from a node that still has other IP trunk cards in the node. See Figure 108 on page 422.

Figure 108
When an IP trunk card cannot be deleted



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

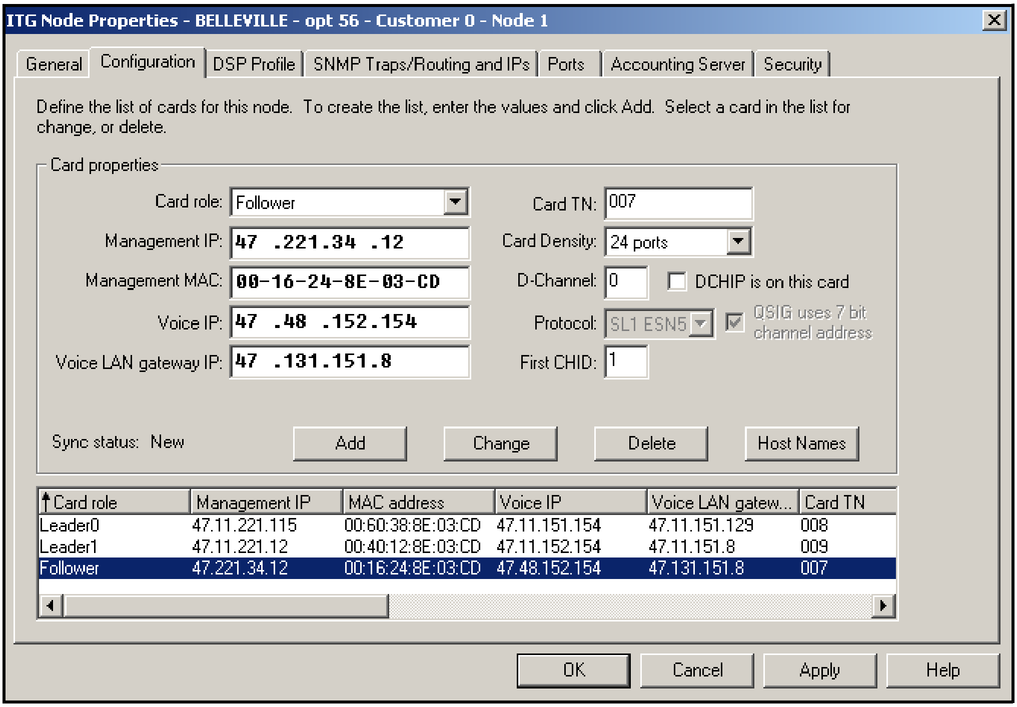
Card role:	Leader0	Card TN:	008
Management IP:	47 .11 .221.115	Card Density:	24 ports
Management MAC:	00-60-38-8E-03-CD	D-Channel:	0 ☐ DCHIP is on this card
Voice IP:	47 .11 .151.154	Protocol:	SL1 ESN5 ☑ QSIG uses 7 bit channel address
Voice LAN gateway IP:	47 .11 .151.129	First CHID:	1

Sync status: Transmitted

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008
Leader1	47.11.221.12	00:40:12:8E:03:CD	47.11.152.154	47.11.151.8	009
Follower	47.221.34.12	00:16:24:8E:03:CD	47.48.152.154	47.131.151.8	007

If the IP trunk card can be deleted, the print on the **Delete** button is in black. See Figure 109 on page 423.

Figure 109
Delete an IP trunk card from a node



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete.

Card properties

Card role: Follower
Management IP: 47 .221.34 .12
Management MAC: 00-16-24-8E-03-CD
Voice IP: 47 .48 .152.154
Voice LAN gateway IP: 47 .131.151.8
Card TN: 007
Card Density: 24 ports
D-Channel: 0
□ DCHIP is on this card
Protocol: SL1 ESN5
☑ QSIG uses 7 bit channel address
First CHID: 1

Sync status: New

Card role	Management IP	MAC address	Voice IP	Voice LAN gatew...	Card TN
Leader0	47.11.221.115	00:60:38:8E:03:CD	47.11.151.154	47.11.151.129	008
Leader1	47.11.221.12	00:40:12:8E:03:CD	47.11.152.154	47.11.151.8	009
Follower	47.221.34.12	00:16:24:8E:03:CD	47.48.152.154	47.131.151.8	007

Note: Leader 0 and Leader 1 cannot be deleted if there is still a Follower card in the node. Leader 0 cannot be deleted if there is still a Leader 1 card in the node.

End of Procedure

Delete a node

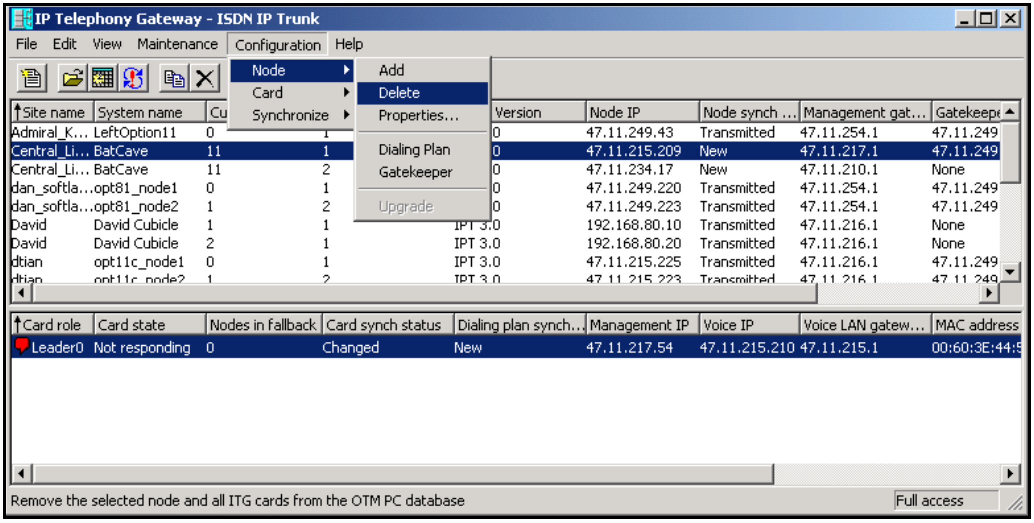
Follow the steps in Procedure 47 to delete a node.

Procedure 47
Deleting a node

1 In the **ITG -ISDN IP Trunk** window, select the node to be deleted.

From the upper menu, click **Configuration > Delete.** See Figure 110 on page 424.

Figure 110
Delete a node



Site name	System name	Cu		Version	Node IP	Node synch ...	Management gat...	Gatekeepe
Admiral_K...	LeftOption11	0	1	0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave	11	1	0	47.11.215.209	New	47.11.217.1	47.11.249
Central_Li...	BatCave	11	2	0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1	0	1	0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_node2	1	2	0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cubicle	1	1	IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249

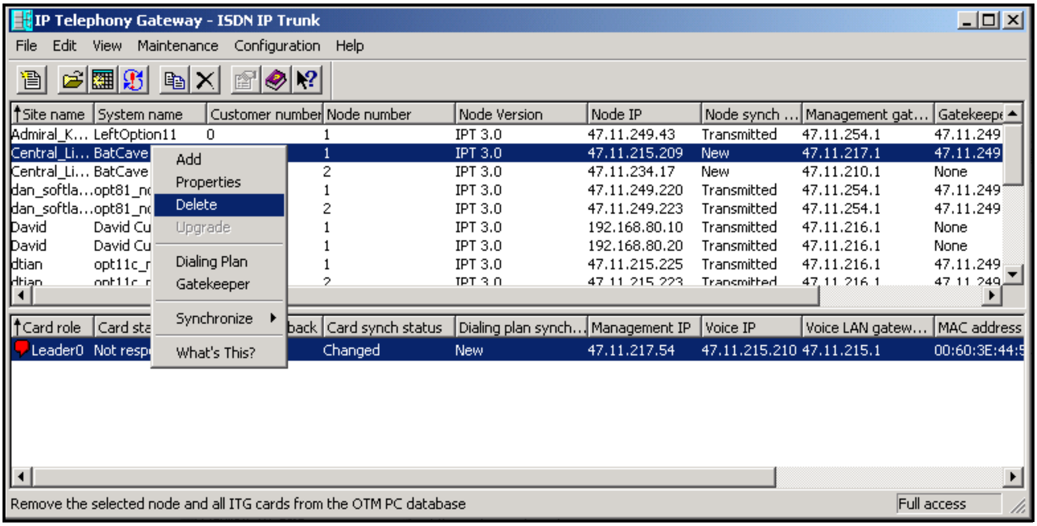
Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Leader0	Not responding	0	Changed	New	47.11.217.54	47.11.215.210	47.11.215.1	00:60:3E:44:5

Remove the selected node and all ITG cards from the OTM PC database

Full access

2 Alternatively, right-click the node to be deleted, and from the pop-up menu, click **Delete**. See Figure 111 on page 425.

Figure 111
Alternative method of deleting a node



Site name	System name	Customer number	Node number	Node Version	Node IP	Node synch ...	Management gat...	Gatekeepe
Admiral_K...	LeftOption11	0	1	IPT 3.0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave		1	IPT 3.0	47.11.215.209	New	47.11.217.1	47.11.249
Central_Li...	BatCave		2	IPT 3.0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_nc		1	IPT 3.0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_nc		2	IPT 3.0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cu		1	IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cu		1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_r		1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_r		2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249

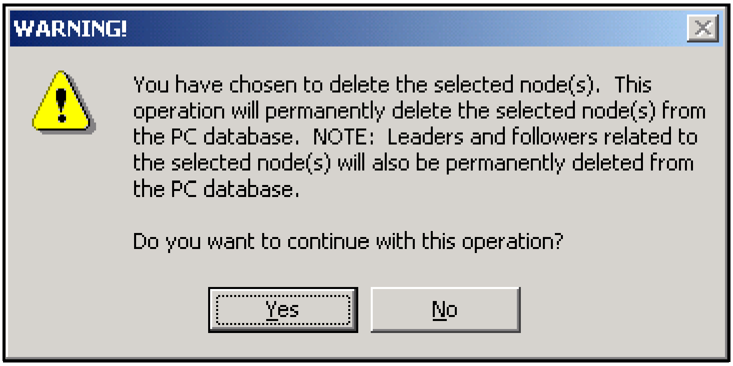
Card role	Card sta	back	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Leader0	Not resp		Changed	New	47.11.217.54	47.11.215.210	47.11.215.1	00:60:3E:44:5

Remove the selected node and all ITG cards from the OTM PC database

Full access

3 When prompted by the warning box to confirm the node deletion, click **Yes** to delete the node or click **No** to cancel the deletion. See Figure 112.

Figure 112
Confirm the node deletion

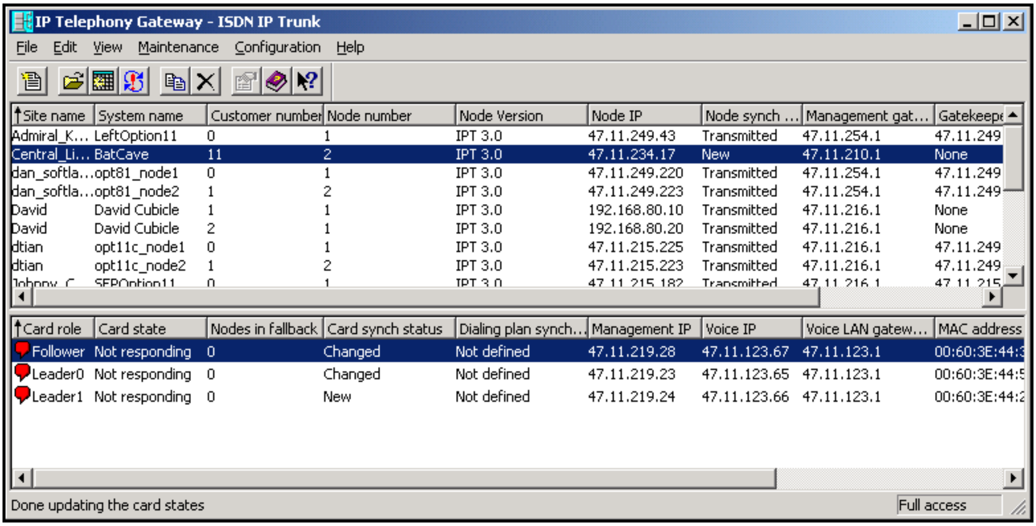


You have chosen to delete the selected node(s). This operation will permanently delete the selected node(s) from the PC database. NOTE: Leaders and followers related to the selected node(s) will also be permanently deleted from the PC database.

Do you want to continue with this operation?

If **Yes** is selected, the node is deleted. See Figure 113 on page 426.

Figure 113
The node is deleted



Site name	System name	Customer number	Node number	Node Version	Node IP	Node synch ...	Management gat...	Gatekeepe
Admiral_K...	LeftOption11	0	1	IPT 3.0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave	11	2	IPT 3.0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1	0	1	IPT 3.0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_node2	1	2	IPT 3.0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cubicle	1	1	IPT 3.0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249
Johnny_C	SEPOption11	0	1	IPT 3.0	47.11.215.182	Transmitted	47.11.216.1	47.11.215

Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Follower	Not responding	0	Changed	Not defined	47.11.219.28	47.11.123.67	47.11.123.1	00:60:3E:44:3
Leader0	Not responding	0	Changed	Not defined	47.11.219.23	47.11.123.65	47.11.123.1	00:60:3E:44:5
Leader1	Not responding	0	New	Not defined	47.11.219.24	47.11.123.66	47.11.123.1	00:60:3E:44:2

Done updating the card states

Full access

End of Procedure

Define the dialing plan information

IP Trunk 3.01 (and later) retains the ability of locally resolving an outgoing dialed number to an IP address of the remote node, using an internally-stored dialing plan table. IP Trunk 3.01 (and later) also adds the ability to send a request (ARQ) to a Gatekeeper, if one is provisioned, to resolve the Dialed Number (DN) to a destination IP address.

After the DN has been resolved to a destination IP address, a setup message is sent from the IP trunk card to the correct destination IP address.

It is necessary to first define the local dialing plan entries, then define the Gatekeeper information.

Follow the steps in Procedure 48 on page 431 to define the local dialing plan.

Non-Gatekeeper-resolved (local) dialing plan

The local dialing plan consists of a number of VoIP destination nodes, such as IP Trunk 3.01 (and later) and ITG Trunk 2.x nodes, and one or more dialing plan entries for each destination node.

If the destination node is also provisioned as a node in OTM 2.1 (and later), select the destination node and the protocol is provided. If the destination node is not provisioned in OTM 2.1 (and later), manually enter the destination node and select the node capability. For each destination node, select whether QoS monitoring is enabled and the level of QoS required. Qos monitoring is only available on IP Trunk 3.01 (and later) and ITG Trunk 2.x nodes. Enter the destination nodes for all destination nodes in the VoIP network.

The following sections provide information on the node protocol to use, the QoS values to enter, and the dialing plan type to enter.

Destination node protocol

The dialing plan information in OTM 2.1 (and later) must correspond with what is provisioned on the far end. The node capability must match what is provisioned in OTM 2.1 (and later) and on the Meridian 1/CS 1000M. For example, the ESN5 feature works optimally if all endpoints contacting an ESN5 node have SL1ESN5 provisioned as the node protocol. Foe more information, see “ESN5 network signaling” on page 308.

If the far end is using IP Trunk 3.01 (and later) or ITG Trunk 2.x software, and is a Small System, the possible protocols are SL1 and SL1ESN5. If the far end is using IP Trunk 3.01 (and later) or ITG Trunk 2.x software, and is a Large System, the possible protocols are SL1, SL1ESN5, and QSIG.

In IP Trunk 3.01 (and later), the capability of “CS 1000S” has been added as a destination node protocol. The CS 1000S destination protocol can be used for making calls to IP Trunk 3.01 (and later) and CS 1000S endpoints, although this is strictly for initial setup. The intention is that an IP Trunk 3.01 (and later) node can have a local dialing plan provisioned with the IP address of a CS 1000S endpoint and the protocol of CS 1000S in order to make test calls. Once the test calls are made and it is confirmed that the endpoints can be reached, the endpoint should be removed from the local dialing plan. It is not a supported configuration to use the local dialing plan to store CS 1000S endpoints. This is because not all MCDN features work with this configuration. Only when a Gatekeeper is used for resolving a destination IP address do all MCDN features work for IP Trunk 3.01 (and later)–to–CS 1000S calls.

Quality of Service

Quality of Service monitoring allows new calls to fall back to alternate circuit-switched trunk routes such as PRI trunk when the IP network QoS level falls below the configured threshold. If the QoS is disabled, then the IP Trunk 3.01 (and later) node attempts to make new calls over the IP network, whether the IP network status is good or poor.

If the far end is an ITG 2.x Trunk node or an IP Trunk 3.01 (and later) node and all calls to that far end are going to be locally resolved using the provisioned dialing plan, then QoS can be used. If QoS is selected, then a level of Qos must also be selected. The level of QoS is based on a model developed by the ITU-T which is explained in the section “E-Model” on page 108. The default is value for QoS is 3 which is considered “Good”, according to the E-model.

The QoS feature only works if the far end is an IP Trunk 3.01 (and later) or an ITG Trunk 2.x node. Additionally, there must be a fallback route for the IP Trunk 3.01 (and later) node to use to reach the far end, such as a PRI trunk. Otherwise, if the QoS level between the two nodes falls below the threshold, calls can no longer be made. If the far end is an IP Peer endpoint and QoS is turned on, calls cannot be made to that node.

IP Peer Networking does not support the QoS messages sent from the IP Trunk 3.01 (and later) node. If QoS is turned on, the IP Trunk 3.01 (and later) node interprets this as a node that is unreachable.

Another concern when using QoS monitoring is the effect of the additional traffic generated by QoS messages being sent between nodes. If all nodes have QoS enabled, the effect of adding one additional node nearly doubles the number of QoS messages being sent.

For example:
A two-node network will generate 2 QoS messages.
A three-node network will generate 6 QoS messages.

A four-node network will generate 12 QoS messages.
A five-node network will generate 20 QoS messages.

The formula that can be used is:

Number of QoS messages sent = $x^2 - x$

where x = number of nodes using QoS

QoS monitoring might need to be turned off for IP Trunk 3.01 (and later) nodes using low bandwidth connection. For more information on how to properly engineer the network, refer “ITG engineering guidelines” on page 125.

Dialing plan types

There are six kinds of dialing plans supported with IP Trunk 3.01 (and later):

1 **NPA –** North American Area codes (the 613 in 1-613-555-1212). A maximum of 7 digits are supported; for example, 1-613-555.

2 **NXX** – North American Exchange, the first three numbers of a local number; for example, the 555 in 1-613-555-1212).

3 **LOC** – Location Code. A code for a particular location. Each LOC must be leftwise-unique. For example, 011 and 0112 are not unique, but 011 and 012 are unique. The maximum number of digits supported is 7 digits.

4 **SPN** – Special Cases. This is for routing international calls or special cases; for example, 011923xxxx or 911. The maximum number of digits supported is 19 digits.

5 **DSC** – Distance Steering Code, part of a Coordinated Dialing Plan (CDP) network. In a CDP network, all numbers must be leftwise-unique as all the systems in that network are viewed by the end user as part of one system.

   For example, Network ABC has half of the users on a Meridian 1 system and half on a CS 1000S system. The Meridian 1’s extensions start with 5; for example, 5xxxx. The Meridian 1 routes calls with Dialed Numbers that start with 7 (for example, 7xxxx) through the IP Trunk card to the CS 1000S system.

6 **TSC** – Trunk Steering Code, also part of a Coordinated Dialing Plan (CDP) network. See DSC for an explanation of a CDP network.

Note: Performing digit manipulation on outgoing numbers might adversely affect non-call-associated signaling for MCDN features. These features include: NRAG, NMS, NACD, and NAS.

The Type of Number (TON) and Numbering Plan Identification (NPI) fields in the Information Element (IE) of the ISDN message direct the call to the correct address translation table. Table 50 shows the mapping between the NPI/TON fields and the resulting IP Trunk 3.01 (and later) dialing plan tables which are searched.

Table 50
Mapping of dialing plan with TON and NPI (Part 1 of 2)

NPI	TON	Dialing plan
E.164	National	NPA
E.164	Subscriber	NXX
E.164	International	SPN
E.164	Unknown	SPN DSC TSC LOC
Private	UDP	LOC
Private	SPN	SPN
Private	CDP	DSC TSC

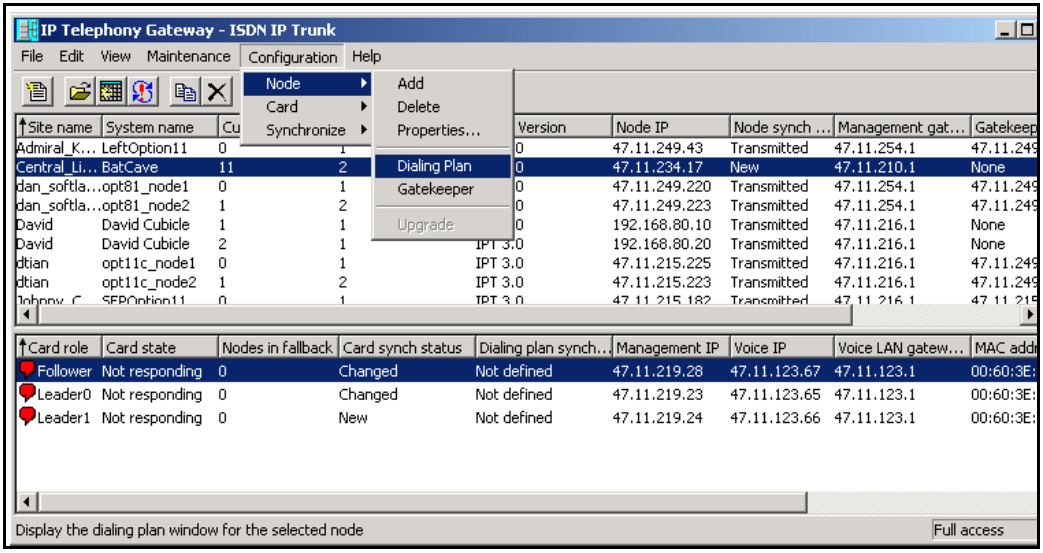
Table 50
Mapping of dialing plan with TON and NPI (Part 2 of 2)

NPI	TON	Dialing plan
Private	Unknown	SPN DSC TSC LOC
Unknown	Unknown	SPN DSC TSC LOC

Procedure 48
Defining the local Dialing plan

1 From the **IP Telephony Gateway – ISDN IP Trunk** window (see Figure 114), select a node. From the Menu, click **Configuration > Dialing Plan**.

Figure 114
Access the Dialing Plan window



Site name	System name	Cu		Version	Node IP	Node synch ...	Management gat...	Gatekeep
Admiral_K...	LeftOption11	0	1	0	47.11.249.43	Transmitted	47.11.254.1	47.11.249
Central_Li...	BatCave	11	2	0	47.11.234.17	New	47.11.210.1	None
dan_softla...	opt81_node1	0	1	0	47.11.249.220	Transmitted	47.11.254.1	47.11.249
dan_softla...	opt81_node2	1	2	0	47.11.249.223	Transmitted	47.11.254.1	47.11.249
David	David Cubicle	1	1	0	192.168.80.10	Transmitted	47.11.216.1	None
David	David Cubicle	2	1	IPT 3.0	192.168.80.20	Transmitted	47.11.216.1	None
dtian	opt11c_node1	0	1	IPT 3.0	47.11.215.225	Transmitted	47.11.216.1	47.11.249
dtian	opt11c_node2	1	2	IPT 3.0	47.11.215.223	Transmitted	47.11.216.1	47.11.249
Johnny_C	SFPOption11	0	1	IPT 3.0	47.11.215.182	Transmitted	47.11.216.1	47.11.215

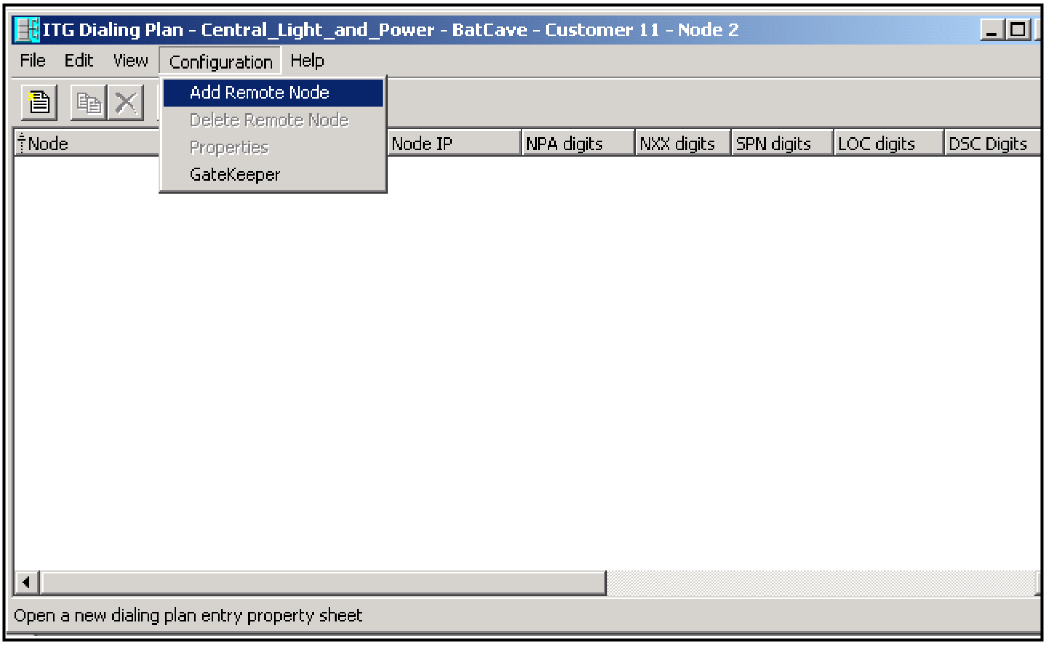
Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC addr
Follower	Not responding	0	Changed	Not defined	47.11.219.28	47.11.123.67	47.11.123.1	00:60:3E:
Leader0	Not responding	0	Changed	Not defined	47.11.219.23	47.11.123.65	47.11.123.1	00:60:3E:
Leader1	Not responding	0	New	Not defined	47.11.219.24	47.11.123.66	47.11.123.1	00:60:3E:

Display the dialing plan window for the selected node

Full access

The **ITG Dialing Plan** window opens. If it is a new node, the **Dialing Plan** window is blank. See Figure 115 on page 432.

Figure 115
ITG Dialing Plan window



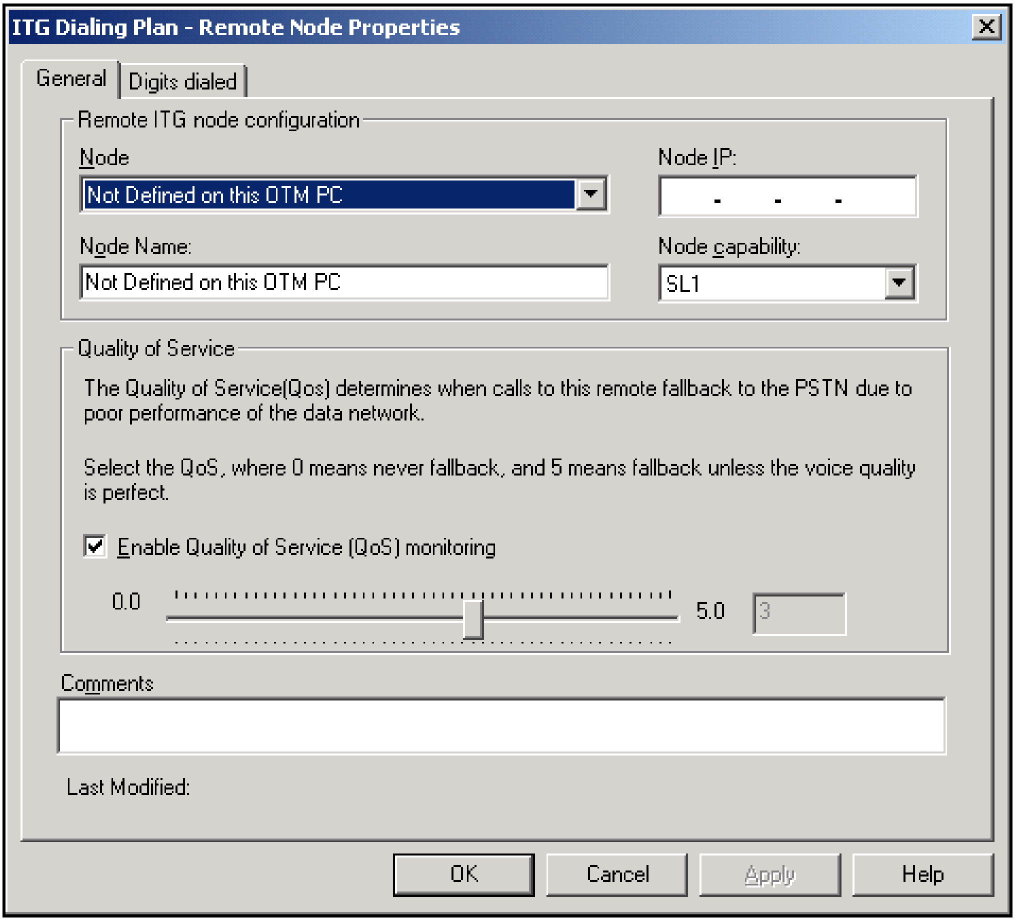
2 To add a new remote node, click **Configuration > Add Remote Node.** A remote node is an entry in the dialing plan table that represents a device to be reached by provisioning on the IP trunk card. See Figure 115 on page 432.

Note: In IP Trunk 3.01 (and later), an address that does not exist in this provisioning is routed to the Gatekeeper, which, at a minimum, resolves the destination.

Note: This enables interworking of legacy ITG Trunk applications with H.323 gateways.

The **ITG Dialing Plan – Remote Node Properties** window opens. See Figure 116 on page 433 and Figure 117 on page 434.

Figure 116
ITG Dialing Plan – Remote Node Properties window – General tab



ITG Dialing Plan - Remote Node Properties

Remote ITG node configuration

Node: Not Defined on this OTM PC

Node IP: . . .

Node Name: Not Defined on this OTM PC

Node capability: SL1

Quality of Service

The Quality of Service(Qos) determines when calls to this remote fallback to the PSTN due to poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

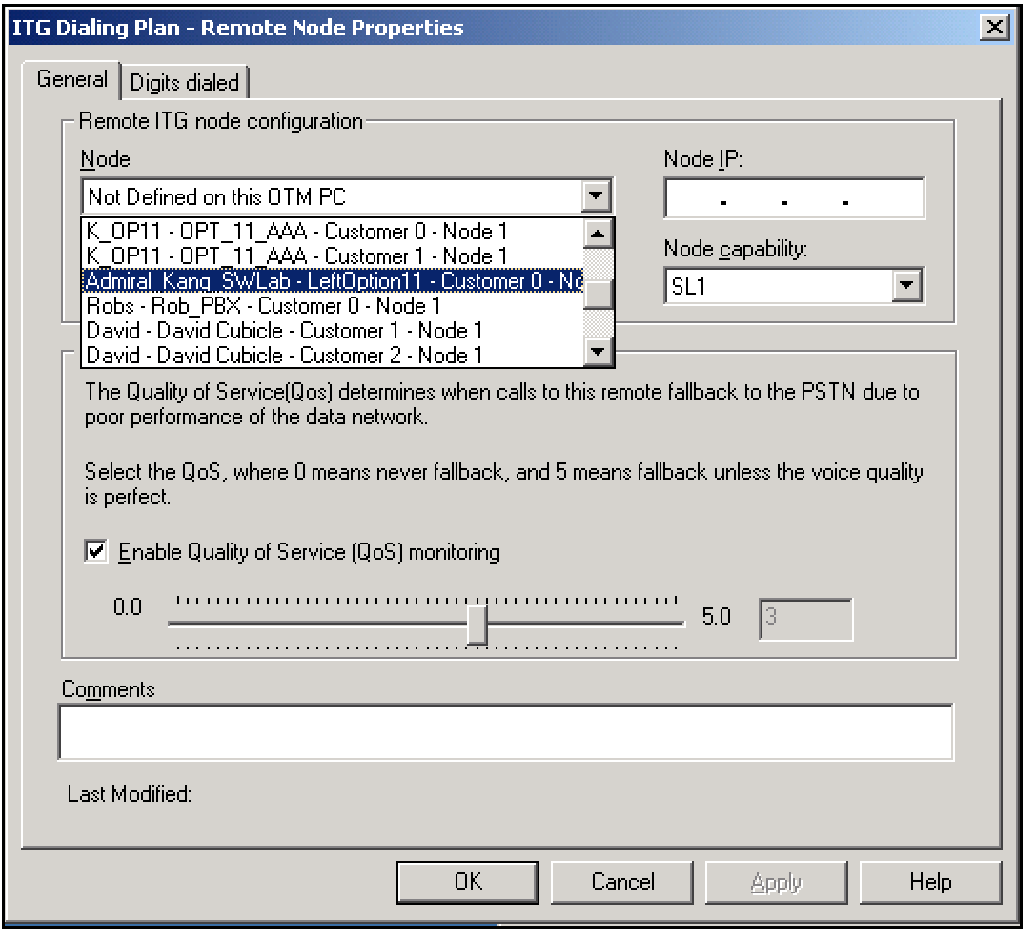
☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments

Last Modified:

Figure 117
ITG Dialing Plan – Remote Node Properties window – General tab with drop-down list open



ITG Dialing Plan - Remote Node Properties

General | Digits dialed

Remote ITG node configuration

Node: Not Defined on this OTM PC

- K_OP11 - OPT_11_AAA - Customer 0 - Node 1
- K_OP11 - OPT_11_AAA - Customer 1 - Node 1
- Admiral_Kang_SWLab - LeftOption11 - Customer 0 - No
- Robs - Rob_PBX - Customer 0 - Node 1
- David - David Cubicle - Customer 1 - Node 1
- David - David Cubicle - Customer 2 - Node 1

Node IP: . . .

Node capability: SL1

The Quality of Service(Qos) determines when calls to this remote fallback to the PSTN due to poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

☑ Enable Quality of Service (QoS) monitoring

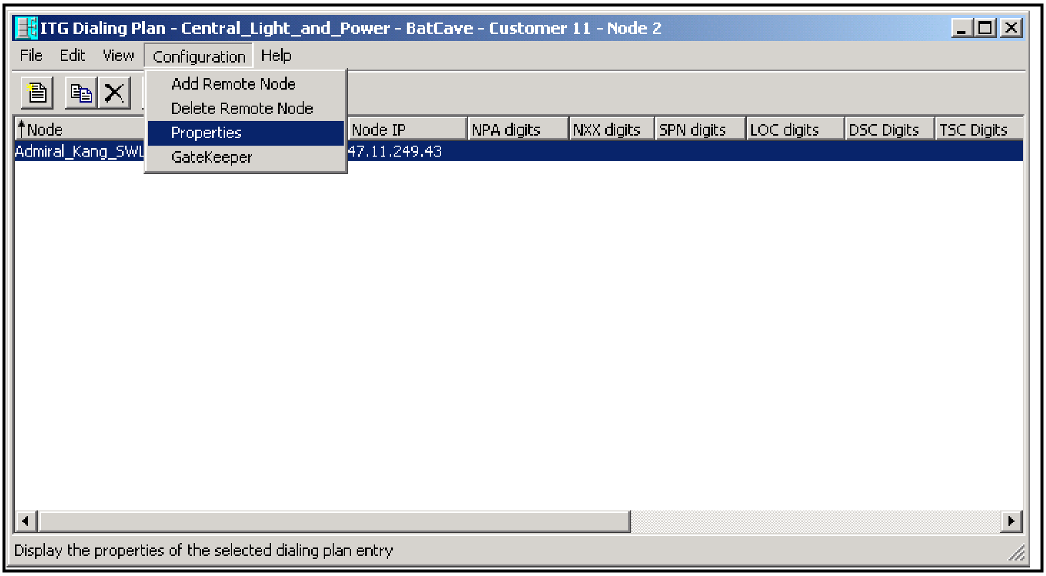
0.0 5.0 3

Comments:

Last Modified:

An existing destination node can also have its properties changed from the drop-down list. See Figure 118 on page 435. In that example, the properties are being changed for the Johnny Carson node.

Figure 118
Change properties on an existing destination node



3 Before entering data (for example, number plan, type of number, digits) for a specific address, the destination node must be selected. The destination node can be selected in one of the following ways:

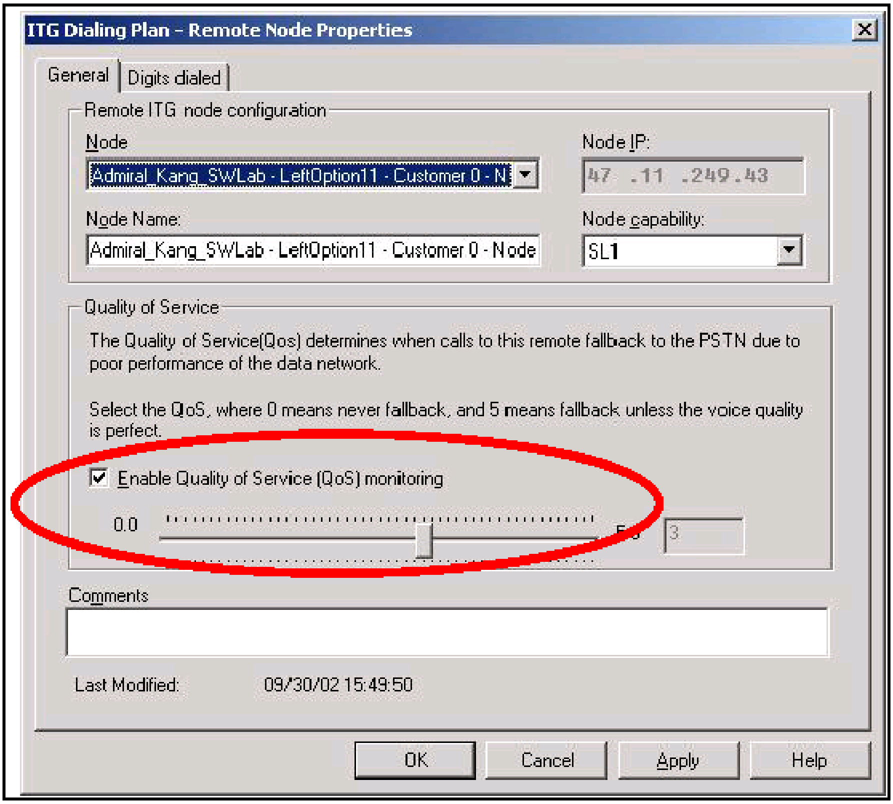
- If the destination is in the local OTM provisioning, select the node from the **Node** drop-down list (on the far left of the screen).
- If the destination is not in the local OTM provisioning, enter the information manually.

Destination node selection in local OTM provisioning

4 If the destination node is in the local OTM provisioning, select the node from the **Node** drop-down list (on the far left of the screen).

In this example, as seen in Figure 116 on page 433, the destination node is selected from the **Node** drop-down list from the local OTM provisioning. When a node is selected, the data specific to the selected remote node is displayed on the **General** tab. See Figure 119 on page 436.

Figure 119
Selected Remote Node



ITG Dialing Plan - Remote Node Properties

General | Digits dialed

Remote ITG node configuration

Node: Admiral_Kang_SWLab - LeftOption11 - Customer 0 - N

Node IP: 47 .11 .249.43

Node Name: Admiral_Kang_SWLab - LeftOption11 - Customer 0 - Node

Node capability: SL1

Quality of Service

The Quality of Service(Qos) determines when calls to this remote fallback to the PSTN due to poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments

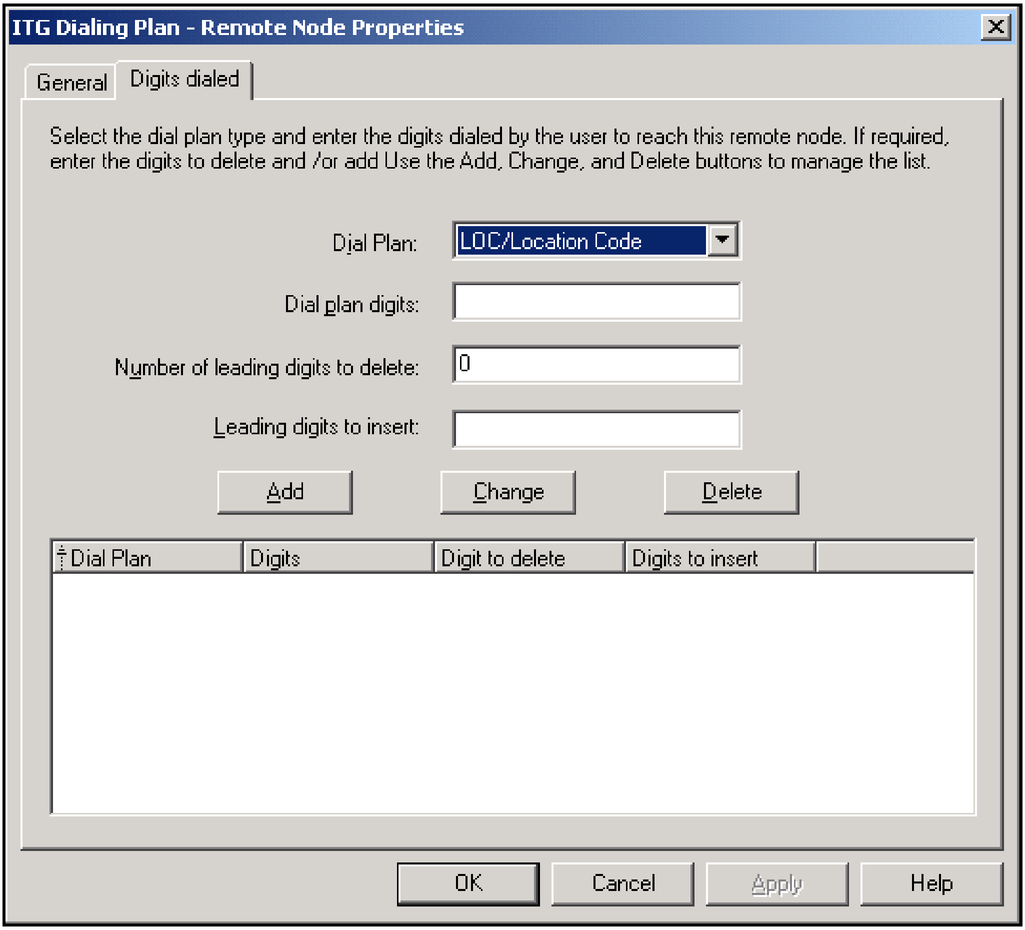
Last Modified: 09/30/02 15:49:50

5 Set the QoS parameter, if desired. Ensure that Fallback to the PBX is in place if QoS levels are not maintained.

> **WARNING**
>
> If a remote node has IP Peer H.323 Gateway capability, do not use QoS monitoring unless that node is also running IP Trunk 3.01 (and later). No other H.233 Gateways support IP Trunk 3.01 (and later)-formatted QoS.
>
> Unless both sides support IP Trunk 3.01 (and later) and have it enabled, calls cannot be made to that node if QoS monitoring is enabled.

6 Click the **Digits dialed** tab. The numbers that must reach this node are provisioned here. See Figure 120 on page 438, Figure 121 on page 439, and Figure 122 on page 440.

Figure 120
Remote Node Properties – Digits dialed tab with no entries



ITG Dialing Plan - Remote Node Properties

Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: LOC/Location Code

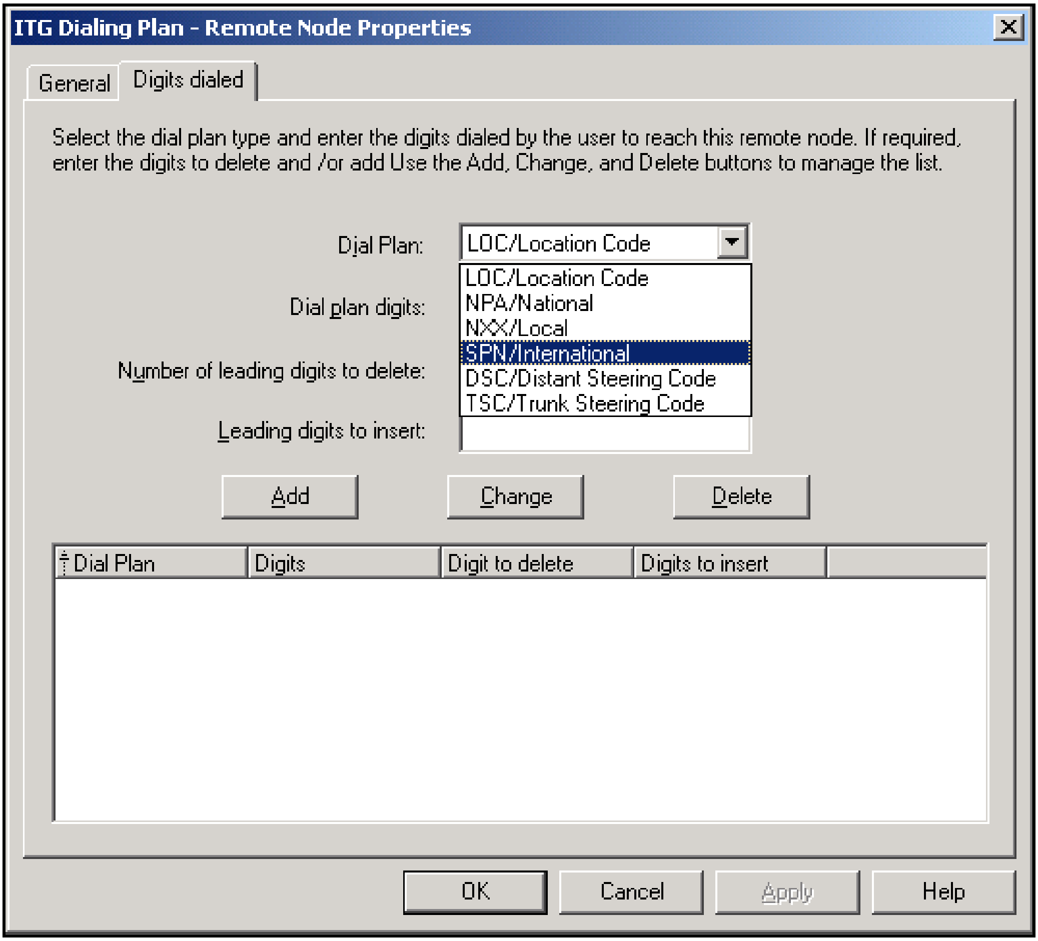
Dial plan digits:

Number of leading digits to delete: 0

Leading digits to insert:

Dial Plan	Digits	Digit to delete	Digits to insert

Figure 121
Select the destination node



ITG Dialing Plan - Remote Node Properties

Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: LOC/Location Code

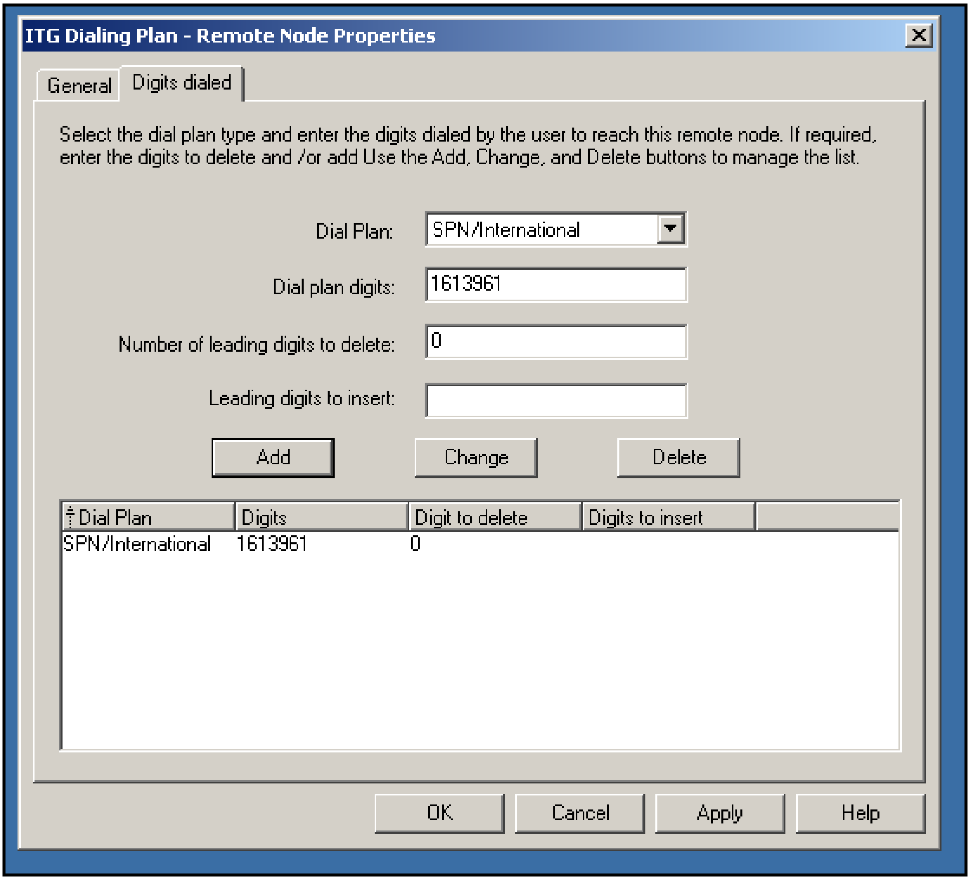
Dial plan digits:

Number of leading digits to delete:

Leading digits to insert:

Dial Plan	Digits	Digit to delete	Digits to insert	

Figure 122
Remote Node Properties – Digits dialed tab with a selected destination node



Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: SPN/International

Dial plan digits: 1613961

Number of leading digits to delete: 0

Leading digits to insert:

Dial Plan	Digits	Digit to delete	Digits to insert
SPN/International	1613961	0	

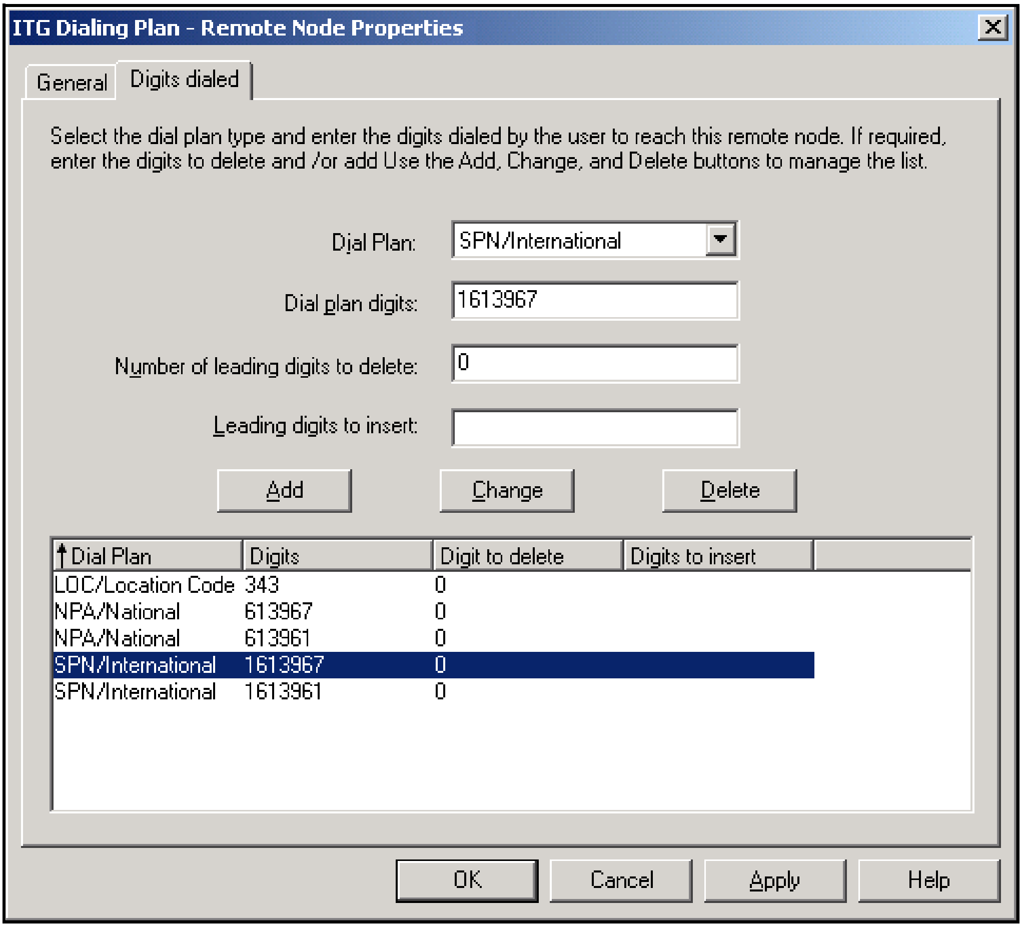
In the example seen in Figure 122, the dialing plan digits to be added are 613-961-xxxx.

7 Click the **ADD** button to add this dialing prefix to the list of previously-configured dialing plans displayed in the lower window.

8 To change the information for a destination node, select the desired destination node in the lower window, make the needed changes in the correct field above the lower window, and click **Change**. See Figure 123 on page 441.

To delete a destination node from the lower window, select the desired node and click **Delete**. Although there is no warning box to request confirmation of the deletion, the destination can immediately be re-added if deleted in error.

Figure 123
Changing the destination node information



ITG Dialing Plan - Remote Node Properties

Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: SPN/International

Dial plan digits: 1613967

Number of leading digits to delete: 0

Leading digits to insert:

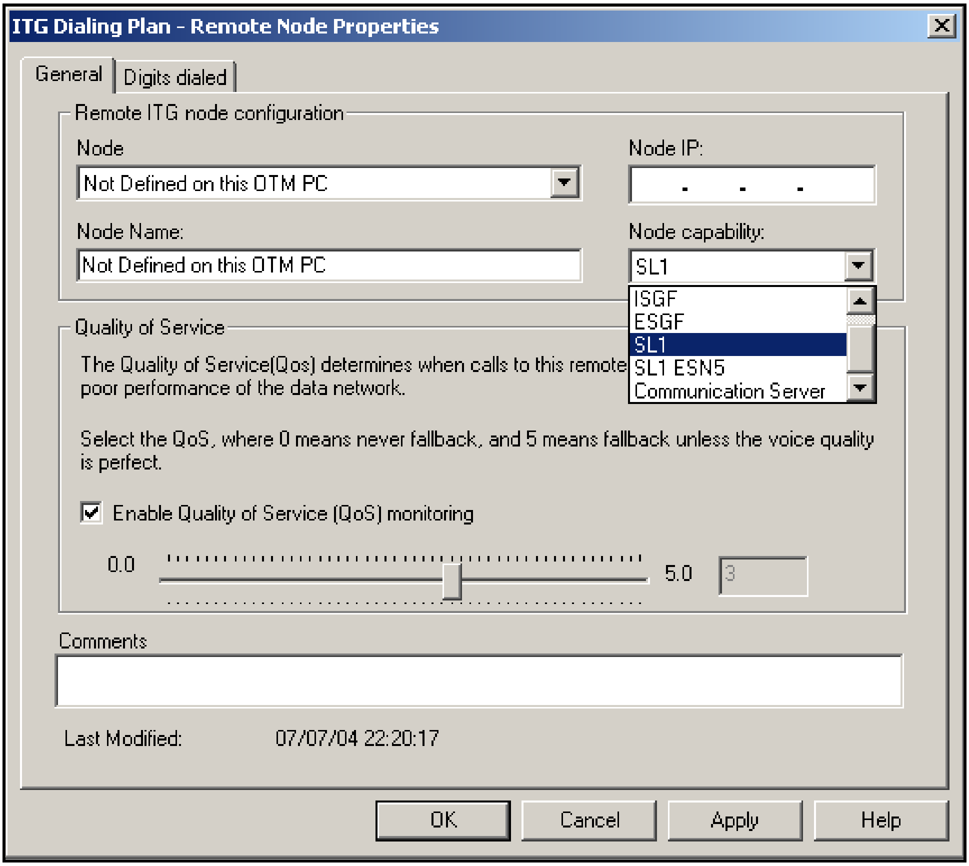
Dial Plan	Digits	Digit to delete	Digits to insert
LOC/Location Code	343	0	
NPA/National	613967	0	
NPA/National	613961	0	
SPN/International	1613967	0	
SPN/International	1613961	0	

Destination not in local OTM provisioning

9 Select **Not Defined on this PC** from the **Node** drop-down list on the ITG Dialing Plan – Remote Node Properties – General tab. See Figure 124.

Select **H.323 V2** from the **Node capability** drop-down list if selecting an IP Peer H.323 Gateway. See Figure 125 on page 443.

Figure 124
Destination not in local OTM provisioning



ITG Dialing Plan - Remote Node Properties

Remote ITG node configuration

Node: Not Defined on this OTM PC

Node IP: . . .

Node Name: Not Defined on this OTM PC

Node capability: SL1

Quality of Service

The Quality of Service(Qos) determines when calls to this remote poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

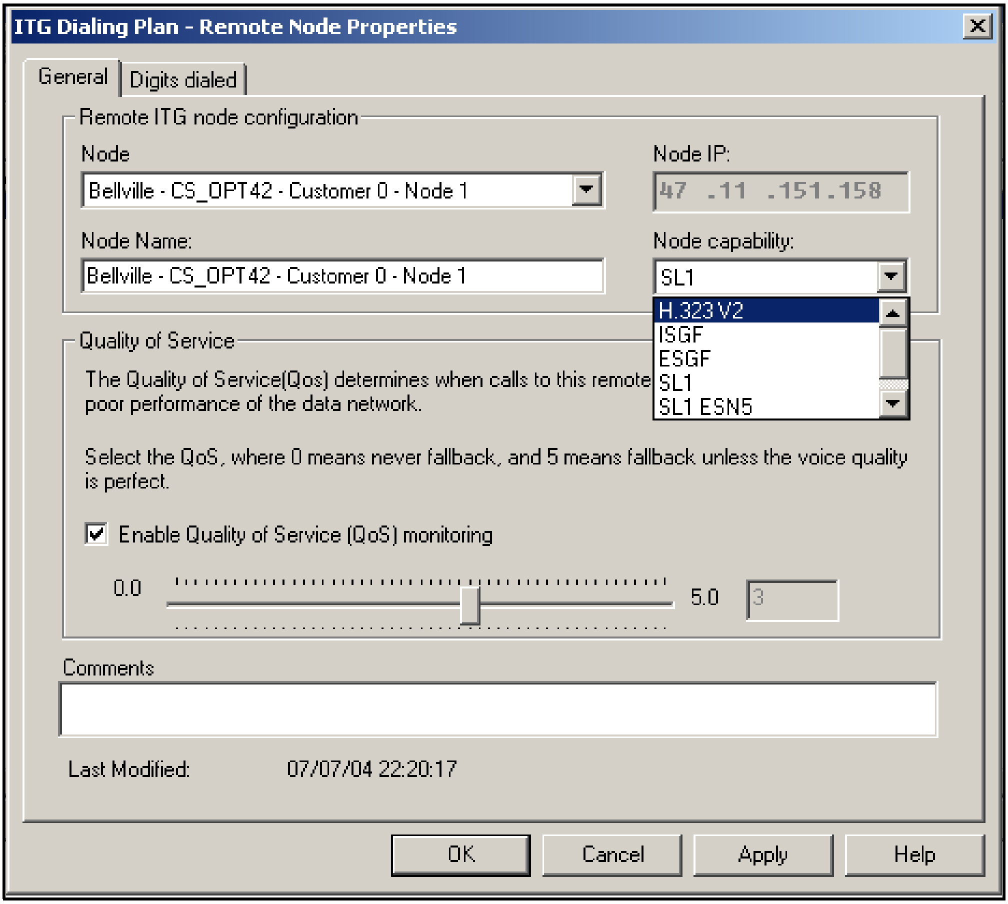
☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments

Last Modified: 07/07/04 22:20:17

Figure 125
Selecting an IP Peer H.323 Gateway



ITG Dialing Plan - Remote Node Properties

General | Digits dialed

Remote ITG node configuration

Node: Bellville - CS_OPT42 - Customer 0 - Node 1

Node IP: 47 .11 .151.158

Node Name: Bellville - CS_OPT42 - Customer 0 - Node 1

Node capability: SL1

Quality of Service

The Quality of Service(Qos) determines when calls to this remote poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments

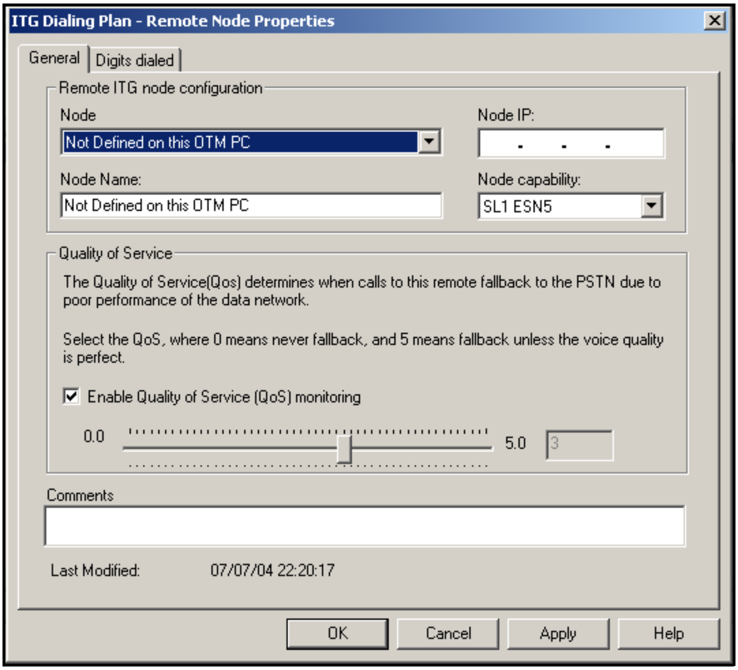
Last Modified: 07/07/04 22:20:17

10 Enter the node IP address, select the node capability from the drop-down list, enter a name for the node (optional), set the QoS monitoring option, and enter comments if desired.

> **WARNING**
>
> If a remote node has IP Peer H.323 Gateway capability, do not use QoS monitoring unless that node is also running IP Trunk 3.01 (and later). No other IP Peer H.323 Gateways support IP Trunk 3.01 (and later)-formatted QoS.
>
> Unless both sides support IP Trunk 3.01 (and later) and have it enabled, calls cannot be made to that node.

11 Click **Apply**. See Figure 126.

Figure 126
Remote Node Properties – General tab



ITG Dialing Plan - Remote Node Properties

General | Digits dialed

Remote ITG node configuration

Node: Not Defined on this OTM PC

Node IP: . . .

Node Name: Not Defined on this OTM PC

Node capability: SL1 ESN5

Quality of Service

The Quality of Service(Qos) determines when calls to this remote fallback to the PSTN due to poor performance of the data network.

Select the QoS, where 0 means never fallback, and 5 means fallback unless the voice quality is perfect.

☑ Enable Quality of Service (QoS) monitoring

0.0 5.0 3

Comments:

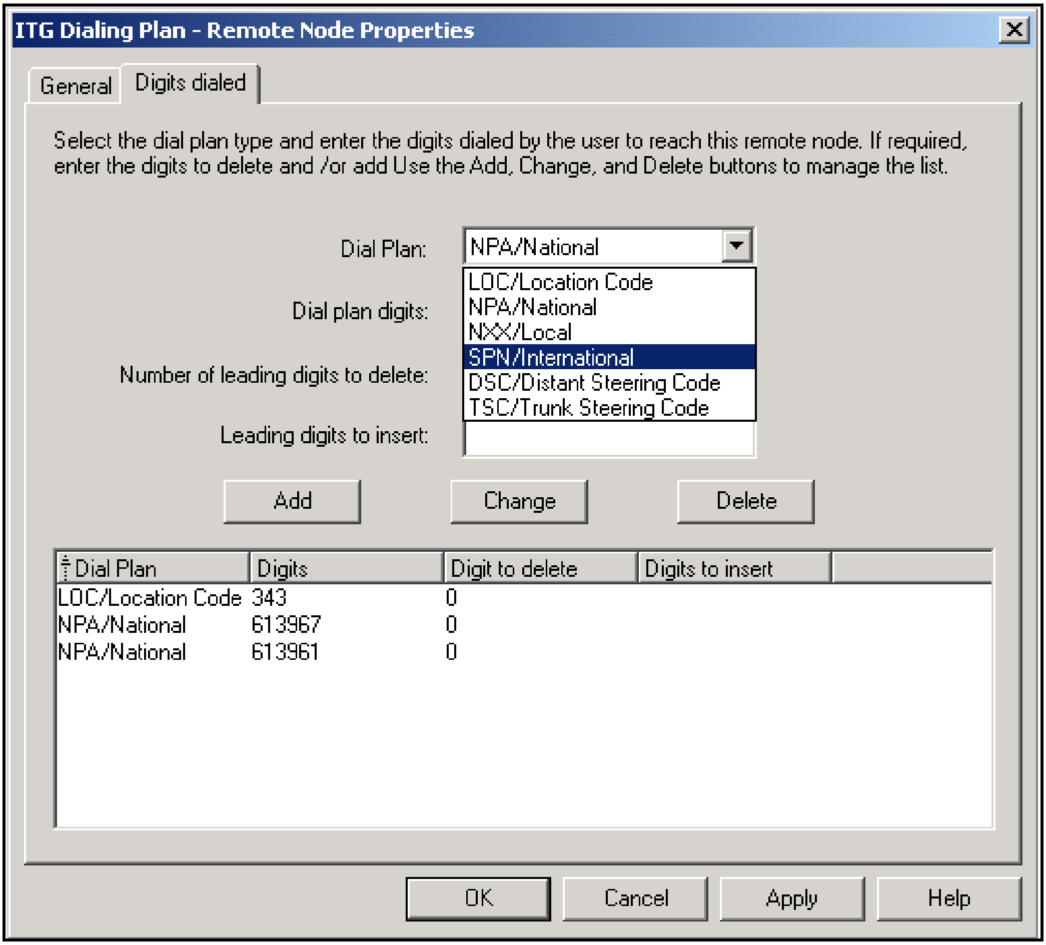
Last Modified: 07/07/04 22:20:17

12 Click the **Digits dialed** tab. The **Add** button is inactive until values are entered in the Dial plan digits field.

On the **Digits dialed** tab, enter the dial plan information for this node.

13 From the **Dial Plan** drop-down list, select the correct dial plan/type of number selection. See Figure 127 on page 445.

Figure 127
Select the Dial Plan



Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: NPA/National

Dial plan digits:

Number of leading digits to delete:

Leading digits to insert:

Dial Plan	Digits	Digit to delete	Digits to insert
LOC/Location Code	343	0	
NPA/National	613967	0	
NPA/National	613961	0	

14 Enter all of the numbers that must reach this node.

15 Enter all necessary data. The data includes the digits dialed, the number of digits to delete from the front, and the digit string to insert on the front.

16 Click **Add** to add the dialing plan to the list in the lower window.

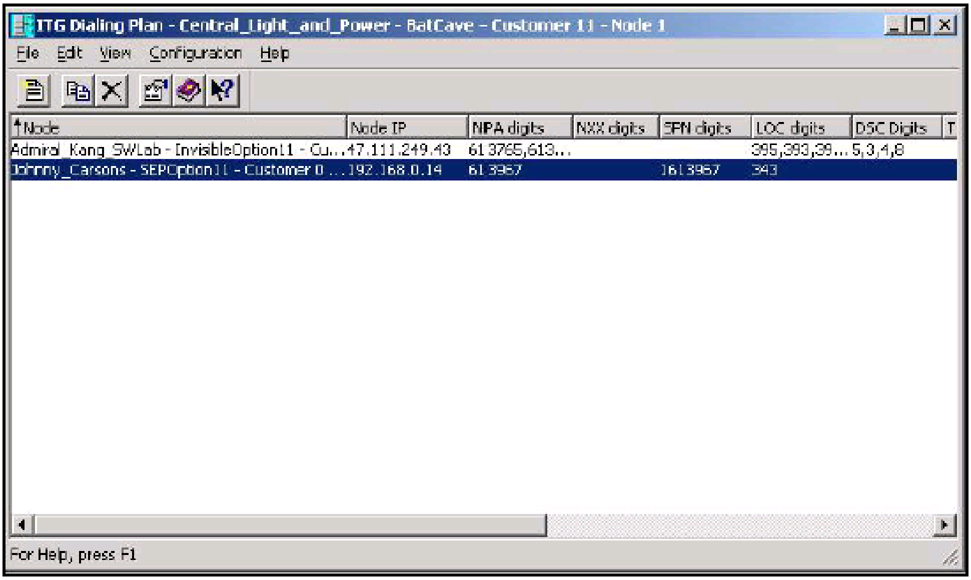
Note: All data from the last entry remains in the fields until it is overwritten. Use caution when adding a new entry to prevent incorrect information from being entered.

End of Procedure

A second number for the same dial plan can be added without having to re-enter all the dialing plan information. Just change the dial plan digit and if necessary, the digits to delete and the digit string to insert. Click **Add** to add the number to the Dial Plan displayed in the lower window.

Figure 128 shows a node with two remote sites provisioned.

Figure 128
Node with two remote sites

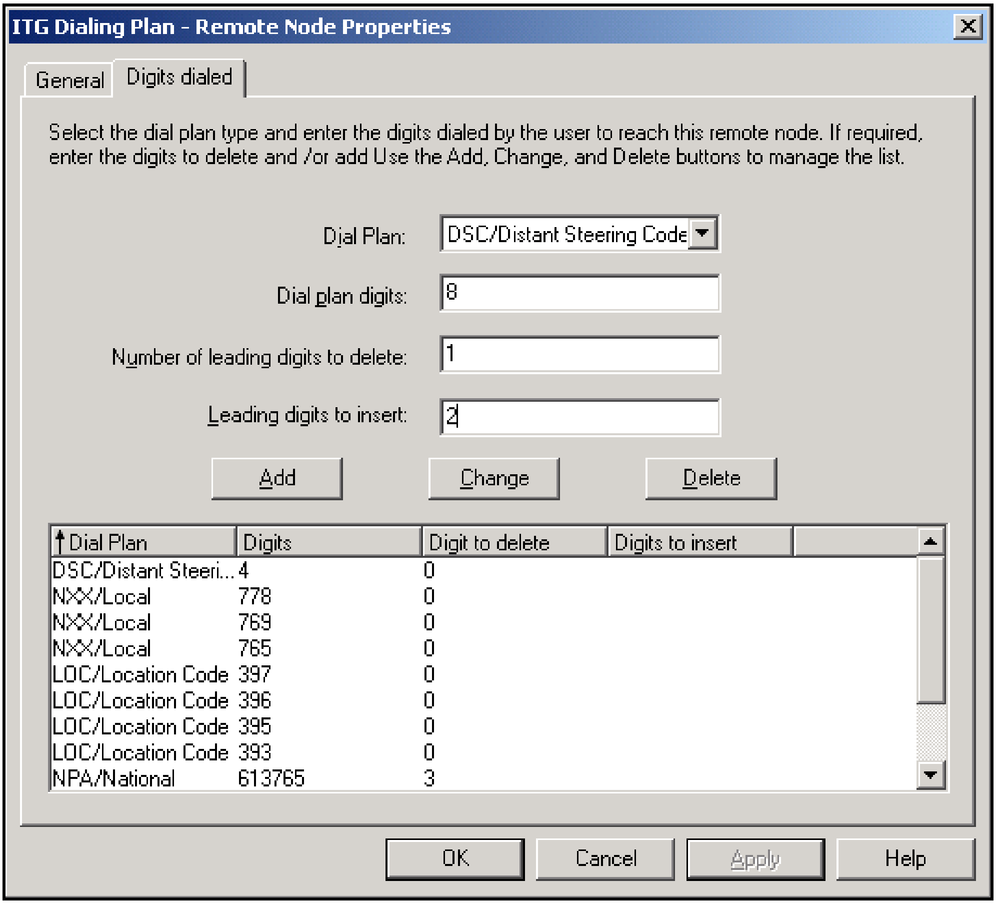

ITG Dialing Plan - Central_Light_and_Power - BatCave - Customer 11 - Node 1
File
Edit
View
Configuration
Help
For Help, press F1

Node	Node IP	NPA digits	NXX digits	SPN digits	LOC digits	DSC Digits	T
Admiral_Kang_SWLab - InvisibleOption11 - Cu...	47.111.249.43	613765,613...			395,393,39...	5,3,4,8	
Johnny_Carsons - SEPOption11 - Customer 0 ...	192.168.0.14	613967		1613967	343		

Complex dialing plans

There is no limit to the number of digit patterns that can terminate on a node. Some dialing plans can be very complex. Figure 129 shows a sample dial plan with a much more complex set of access numbers. This remote node can be reached through LOC (Location codes – ESN UDP dialing), NPA/NXX, and DSC dialing from the local node. In Figure 129, a DSC (Distant Steering Code) of 8 has been entered, but not yet added. Click **Add** to save this entry.

Figure 129
Example of a complex dialing plan



Select the dial plan type and enter the digits dialed by the user to reach this remote node. If required, enter the digits to delete and /or add Use the Add, Change, and Delete buttons to manage the list.

Dial Plan: DSC/Distant Steering Code

Dial plan digits: 8

Number of leading digits to delete: 1

Leading digits to insert: 2

Dial Plan	Digits	Digit to delete	Digits to insert
DSC/Distant Steeri...	4	0	
NXX/Local	778	0	
NXX/Local	769	0	
NXX/Local	765	0	
LOC/Location Code	397	0	
LOC/Location Code	396	0	
LOC/Location Code	395	0	
LOC/Location Code	393	0	
NPA/National	613765	3	

Gatekeeper-resolved endpoints

The IP Trunk 3.01 (and later) application has two methods of resolving addresses. The IP Trunk 3.01 (and later) node first checks the dialing plan information using the Address Translation Protocol Module (ATPM). If no match exists, the IP Trunk 3.01 (and later) node checks to see if a Gatekeeper has been provisioned. If a Gatekeeper has been provisioned, the IP Trunk 3.01 (and later) node forwards the applicable H.323 messaging to the Gatekeeper which attempts to complete the call. If a Dialed Number (DN) does not match what is stored in the local dialing plan, and if there is no Gatekeeper is provisioned or the Gatekeeper does not know the number, the call fails.

Zones

A network zone is a logical grouping of CS 1000S and CS 1000M systems with IP Peer H.323 Gateways, IP Line 3.0, IP Trunk 3.01 (and later), and/or third-party gateways or endpoints. Network zones can have geographical significance; for instance, a company could configure one network zone for its east coast offices and one network zone for its west coast offices.

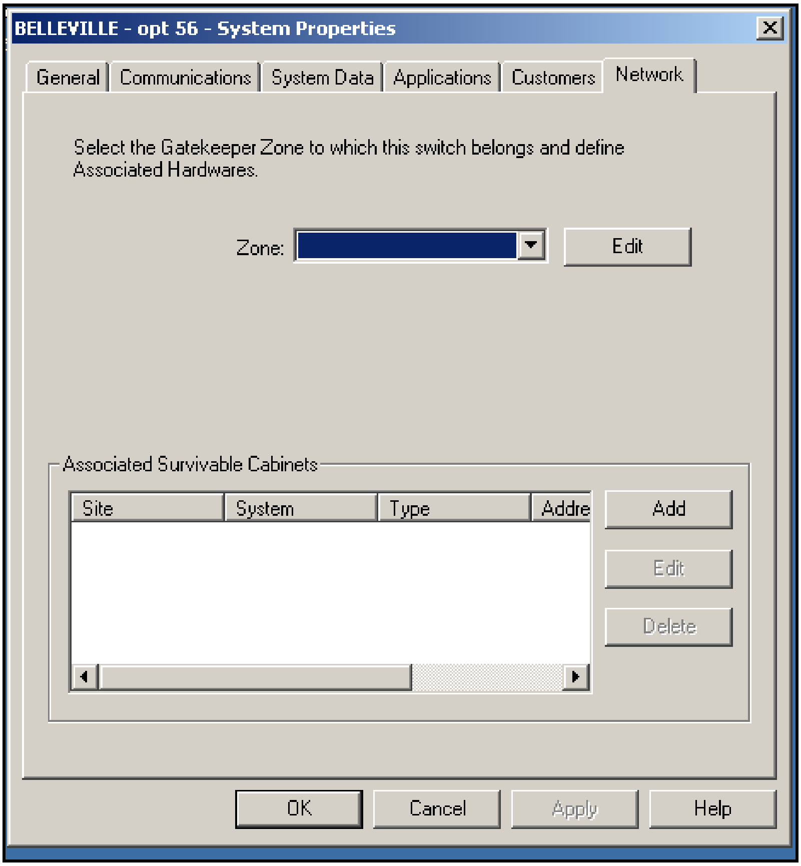
Recommendation

Though not mandatory, Nortel recommends that zones be used for IP Trunk 3.01 (and later).

In the OTM Navigator window, the Gatekeeper zone can be found by left-clicking on the CS 1000S or CS 1000M system, selecting **Properties**, and clicking on the Network tab. See Figure 130 on page 449.

When provisioning the applicable devices in OTM 2.1 (and later), use network zones to coordinate the Gatekeeper information. The Gatekeeper zones were defined on the CS 1000S/CS 1000M. For information on configuring zones on the CS 1000S and CS 1000M systems, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

Figure 130
Making a Gatekeeper zone



BELLEVILLE - opt 56 - System Properties

Select the Gatekeeper Zone to which this switch belongs and define Associated Hardwares.

All nodes within a network are configured with the IP addresses of the Primary and Alternate Gatekeepers in that network zone.

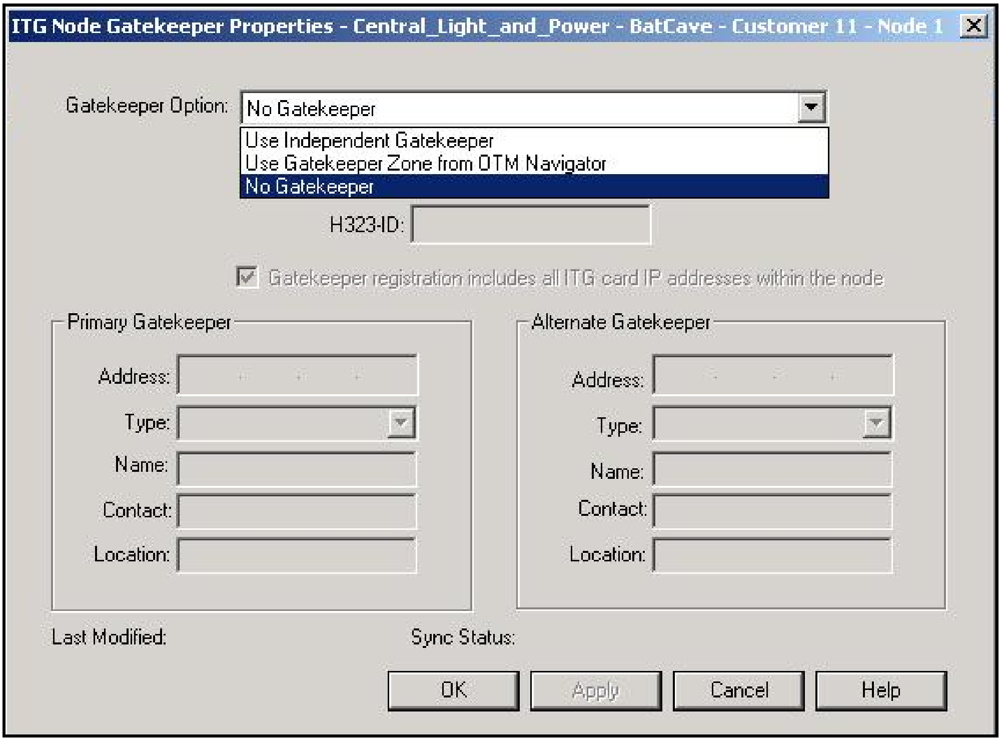
Follow the steps in Procedure 49 on page 450 to configure the correct network zone when provisioning an IP Trunk 3.01 (and later) node.

Procedure 49
Provisioning the IP Trunk 3.01 (and later) node to register with the Gatekeeper

1 Configure The IP Trunk 3.01 (and later) node to register with the IP Peer H.323 Gateway Gatekeeper. This can be done in either of two ways, as follows:

- In the **ITG – ISDN IP Trunk** window, as seen in Figure 92 on page 403, from the menu select **Configuration > Node > Gatekeeper**. The **ITG Node Gatekeeper properties** window opens. See Figure 131.

Figure 131
ITG Node Gatekeeper Properties window



Gatekeeper Option: No Gatekeeper

☑ Gatekeeper registration includes all ITG card IP addresses within the node

- Alternatively, from the ITG Dialing PLan window, click **Configuration > Gatekeeper**.

No matter which method was used, the **ITG Node Gatekeeper Properties** window opens.

2 Select the correct Gatekeeper option from the **Gatekeeper Option** drop-down list. The options are as follows:

- Use Gatekeeper Zone from OTM Navigator (see Procedure 50).
- Use Independent Gatekeeper (see Procedure 51 on page 453).
- No Gatekeeper. Select this option to remove the provisioning that tells the IP trunk card to use a Gatekeeper.

End of Procedure

Use Gatekeeper Zone from OTM Navigator option

If "Use Gatekeeper zone from OTM Navigator" was selected from the **Gatekeeper Option** drop-down list, follow the steps in Procedure 50.

Procedure 50
Using a Gatekeeper zone from OTM Navigator

1 Select the "Use Gatekeeper Zone from OTM Navigator" option if the applicable Gatekeeper or Gatekeepers exist in a zone administered by the OTM workstation.

2 It is only necessary to select the zone and enter the H.323 endpoint ID for the node. All other necessary details are automatically filled in.

WARNING

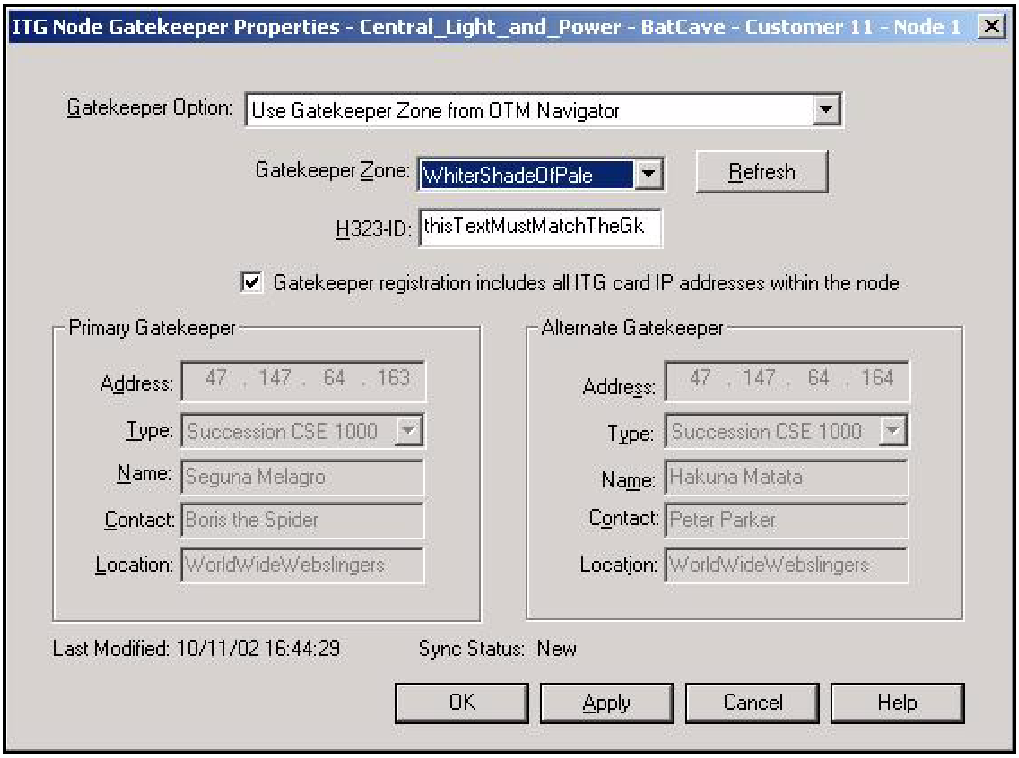
The H.323 endpoint ID is case-sensitive and alphanumeric-string content sensitive. The data entered in the H.323 ID field must be an exact match or calls to the Gatekeeper-controlled destinations fail.

WARNING

If the wrong zone is selected, calls fail because that zone's gatekeepers have not been provisioned to handle calls from this gateway.

See Figure 132.

Figure 132
Node Properties Gatekeeper from OTM



ITG Node Gatekeeper Properties - Central_Light_and_Power - BatCave - Customer 11 - Node 1

Gatekeeper Option: Use Gatekeeper Zone from OTM Navigator

Gatekeeper Zone: WhiterShadeOfPale

H323-ID: thisTextMustMatchTheGk

☑ Gatekeeper registration includes all ITG card IP addresses within the node

Primary Gatekeeper

Address: 47 . 147 . 64 . 163

Type: Succession CSE 1000

Name: Seguna Melagro

Contact: Boris the Spider

Location: WorldWideWebslingers

Alternate Gatekeeper

Address: 47 . 147 . 64 . 164

Type: Succession CSE 1000

Name: Hakuna Matata

Contact: Peter Parker

Location: WorldWideWebslingers

Last Modified: 10/11/02 16:44:29

Sync Status: New

3 Click **Apply**.

End of Procedure

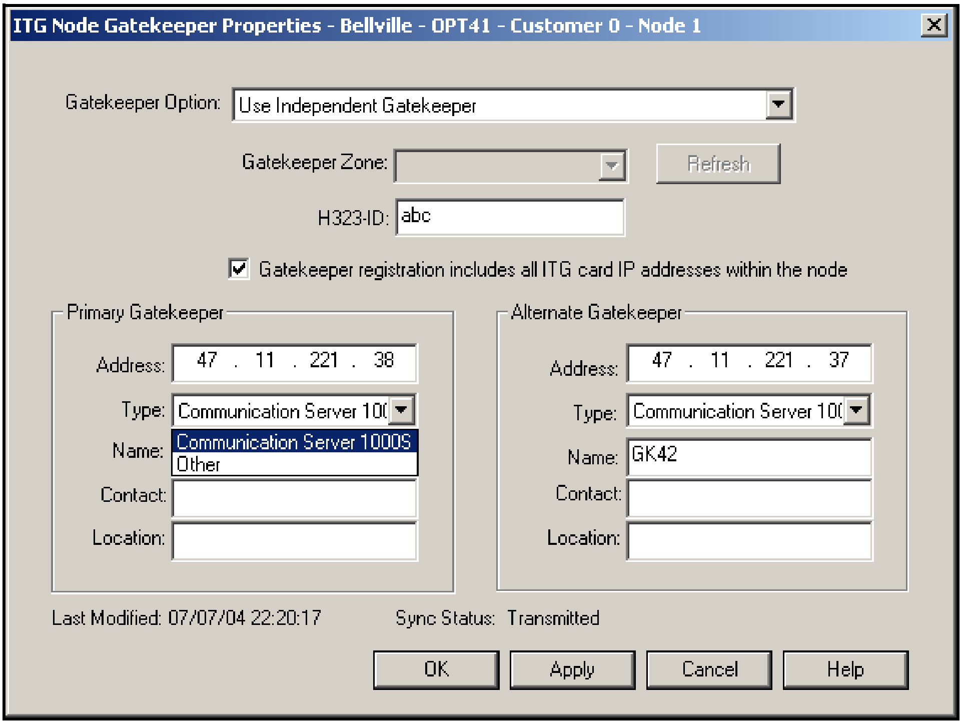
Use Independent Gatekeeper option

If “Use Independent Gatekeeper” was selected from the **Gatekeeper Option** drop-down list, follow the steps in Procedure 51. Provisioning an independent Gatekeeper requires full manual provisioning.

Procedure 51
Using the Independent Gatekeeper option

1 Select CS 1000S/CS 1000M as the remote Gatekeeper type. See Figure 133.

Figure 133
Gatekeeper Type drop-down list



ITG Node Gatekeeper Properties - Bellville - OPT41 - Customer 0 - Node 1

Gatekeeper Option: Use Independent Gatekeeper

Gatekeeper Zone:

H323-ID: abc

☑ Gatekeeper registration includes all ITG card IP addresses within the node

Primary Gatekeeper

Address: 47 . 11 . 221 . 38

Type: Communication Server 10(

Communication Server 1000S

Other

Name:

Contact:

Location:

Alternate Gatekeeper

Address: 47 . 11 . 221 . 37

Type: Communication Server 10(

Name: GK42

Contact:

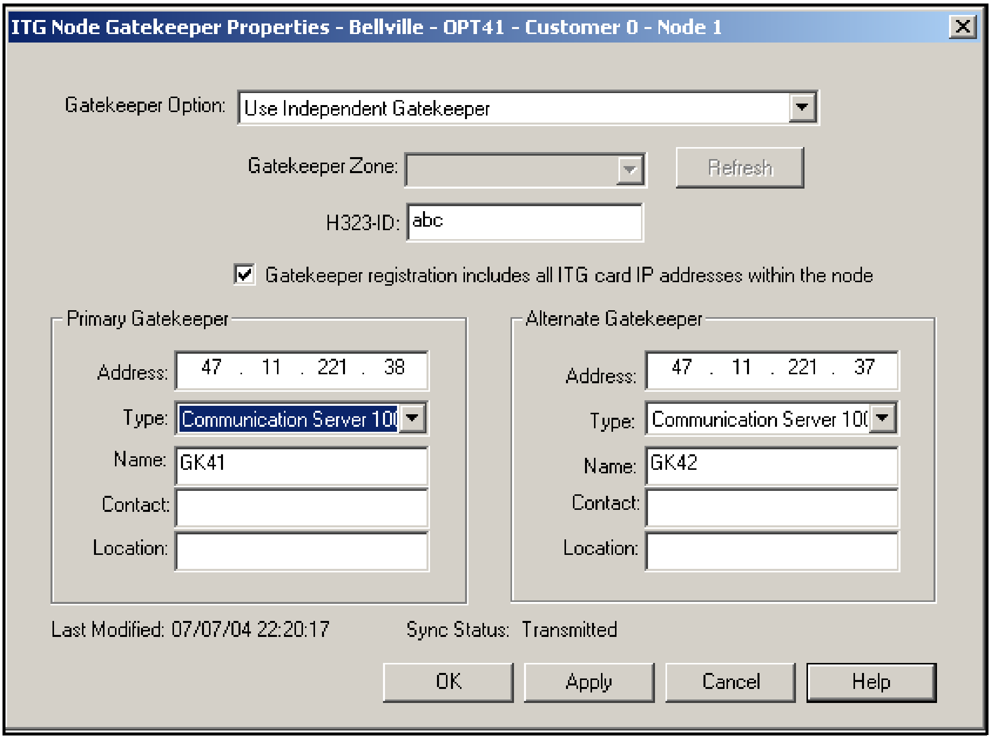
Location:

Last Modified: 07/07/04 22:20:17

Sync Status: Transmitted

Figure 134 shows an example of an independent Gatekeeper that has been provisioned.

Figure 134
Properties defined for Primary Gatekeeper



ITG Node Gatekeeper Properties - Bellville - OPT41 - Customer 0 - Node 1

Gatekeeper Option: Use Independent Gatekeeper

Gatekeeper Zone:

H323-ID: abc

☑ Gatekeeper registration includes all ITG card IP addresses within the node

Primary Gatekeeper

Address: 47 . 11 . 221 . 38

Type: Communication Server 10(

Name: GK41

Contact:

Location:

Alternate Gatekeeper

Address: 47 . 11 . 221 . 37

Type: Communication Server 10(

Name: GK42

Contact:

Location:

Last Modified: 07/07/04 22:20:17

Sync Status: Transmitted

WARNING

The H.323 endpoint ID is case-sensitive and alphanumeric string content-sensitive. The data entered in the H.323 ID field must be an exact match to what is provisioned on the Gatekeeper or calls to the Gatekeeper-controlled destinations fail.

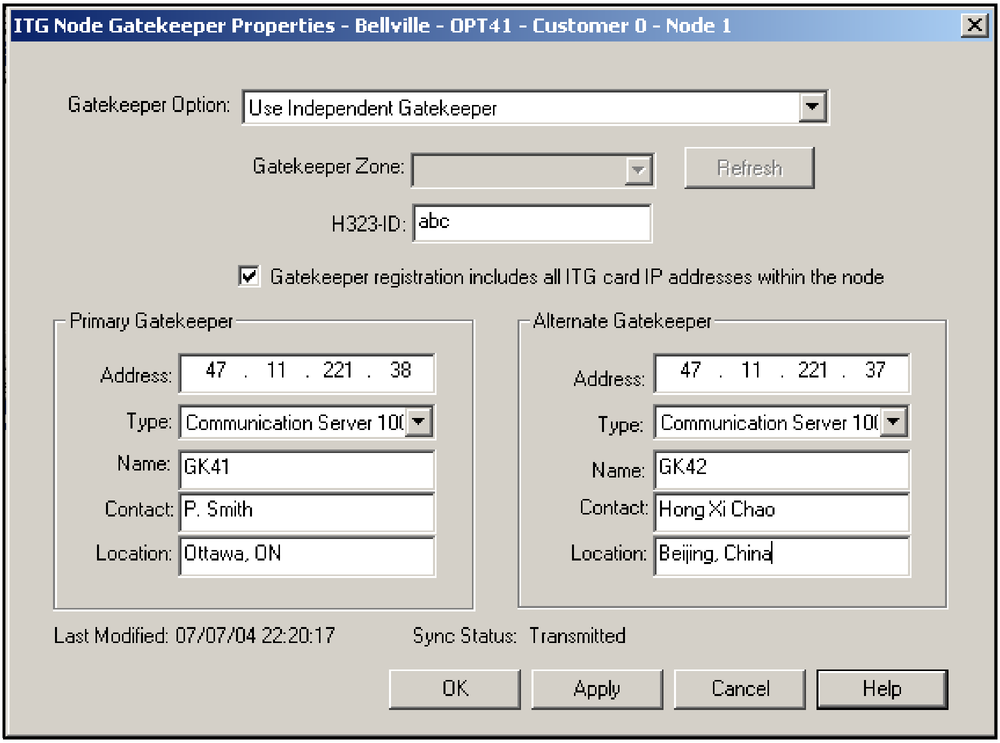
WARNING

When using Gatekeeper zones instead of independent Gatekeepers, if the wrong zone is selected, calls fail because that zone's Gatekeepers have not been provisioned to handle calls from this gateway.

The Gatekeeper registration option in the circled check box, as seen in Figure 134 on page 454, can be ignored as the information defined in this check box is not used by IP Trunk 3.01 (and later).

2 Define an Alternate Gatekeeper, if desired. An example of an IP Trunk 3.01 (and later) node Independent Gatekeeper with both Primary and Alternate Gatekeepers defined is shown in Figure 135.

Figure 135
Properties defined for Primary and Alternate Gatekeepers



ITG Node Gatekeeper Properties - Bellville - OPT41 - Customer 0 - Node 1

Gatekeeper Option: Use Independent Gatekeeper

Gatekeeper Zone:

H323-ID: abc

☑ Gatekeeper registration includes all ITG card IP addresses within the node

Primary Gatekeeper

Address: 47 . 11 . 221 . 38

Type: Communication Server 10(

Name: GK41

Contact: P. Smith

Location: Ottawa, ON

Alternate Gatekeeper

Address: 47 . 11 . 221 . 37

Type: Communication Server 10(

Name: GK42

Contact: Hong Xi Chao

Location: Beijing, China

Last Modified: 07/07/04 22:20:17

Sync Status: Transmitted

3 Click **OK**.

End of Procedure

From the ITG Dialing Plan window, confirm that all required remote end-points have been provisioned.

Download the dialing plan provisioning to the IP trunk cards. For more information on downloading the dialing plan, see “Transmit configuration data” on page 466.

OTM 2.1 (and later) OA&M using OTM 2.1 (and later) applications

Contents

This section contains information on the following topics:

Introduction

This chapter explains how to perform IP Trunk 3.01 (and later) Operation, Administration and Maintenance (OA&M) tasks using OTM Navigator, Maintenance windows and System Terminal Passthru, the OTM Alarm Notification application, and the OTM ITG ISDN IP Trunks application.

Most OA&M tasks are performed from OTM. A few OA&M tasks must be performed through the ITG shell (See “OA&M using the ITG shell CLI and overlays” on page 487.) If OTM is temporarily unavailable, many OA&M tasks can be performed from the ITG shell as an alternative method.

OTM OA&M procedure summary

- “Delete a node” on page 459
- “Database locking” on page 461
- “ITG Card Properties window” on page 462
- “Transmit configuration data” on page 466
- “Add an IP Trunk 3.01 (and later) node on OTM by retrieving an existing node” on page 470
- “Retrieve and add an IP Trunk 3.01 (and later) node for maintenance and diagnostic purposes” on page 474
- “Retrieve IP Trunk 3.01 (and later) configuration information from the IP Trunk 3.0 (and later) node” on page 475

- "Schedule and generate and view IP Trunk 3.01 (and later) OM reports" on page 477
- "Backup and restore operations" on page 479
- "Alarm Notification" on page 480

Delete a node

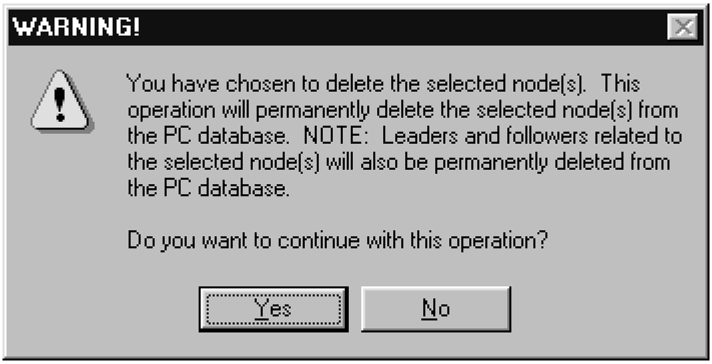
To delete an IP Trunk 3.01 (and later) node, perform the following steps in Procedure 52.

Procedure 52
Deleting an IP Trunk 3.01 (and later) node

1. Double-click the **ITG ISDN IP Trunk** icon from the Services folder in the **OTM Navigator** window.
2. Right-click the node to be deleted in the upper portion of the **IP Telephony Gateway - ISDN IP Trunk** window.
3. Select **Delete** from the menu.

4 The dialog box in Figure 136 appears. Click the **Yes** button to confirm the deletion of the IP Trunk 3.01 (and later) node. The IP Trunk 3.01 (and later) node and all related IP trunk cards are deleted.

Figure 136
Delete Node dialog box



WARNING!

You have chosen to delete the selected node(s). This operation will permanently delete the selected node(s) from the PC database. NOTE: Leaders and followers related to the selected node(s) will also be permanently deleted from the PC database.

Do you want to continue with this operation?

End of Procedure

Delete an IP trunk card

To delete an IP trunk card, perform the steps in Procedure 53.

Procedure 53
Deleting an IP trunk card

1 Double-click the **ITG ISDN IP Trunk** icon in the Services folder in the **OTM Navigator** window.

2 Right-click the node and select menu **Node > Properties.**

3 The **ITG Node Properties** window appears.

4 Select the **Card Configuration** tab.

5 Select the IP trunk card to delete from the list.

6 Click the **Delete** button.

7 Click **OK**.

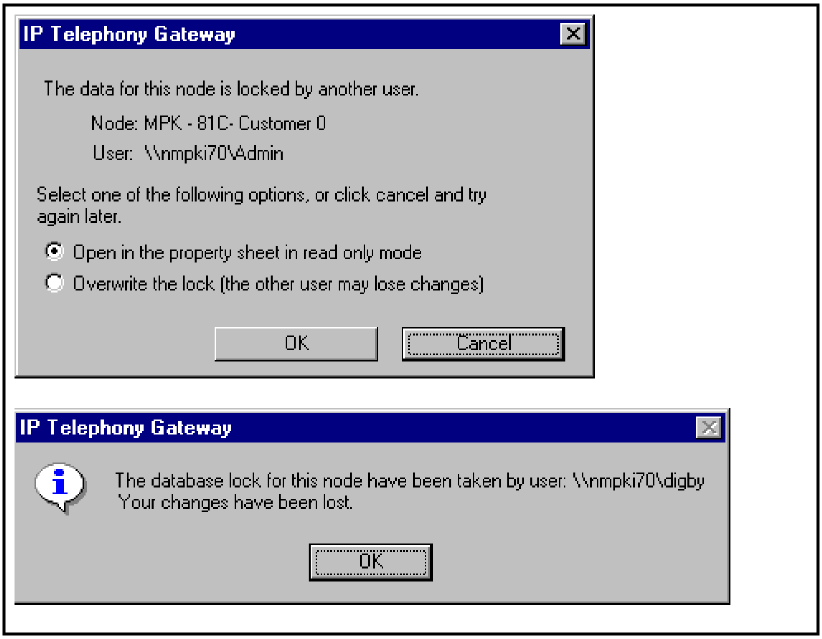
End of Procedure

Database locking

All node and card properties are stored in a single OTM database. When Node or Card Properties are opened, the data for a given node (including card properties) is then locked. If a second user tries to access a property sheet in the same node at the same time, the second user is given the option of overriding the lock. If the second user decides to override the lock and the first user has made changes and then clicked "OK" or "Apply", the first user provided with a message that says that their changes have been lost (see the second dialog box in Figure 137 on page 462). This message only appears if changes have been made.

If an attempt is made to open a property sheet in the node after rebooting the PC, the first dialog box in Figure 137 appears. In this example, a property sheet was open when the database was taken over by another user.

Figure 137
Database lock message



The data for this node is locked by another user.

Node: MPK - 81C- Customer 0
User: \\nmpki70\Admin

Select one of the following options, or click cancel and try again later.

● Open in the property sheet in read only mode
○ Overwrite the lock (the other user may lose changes)

The database lock for this node have been taken by user: \\nmpki70\digby
Your changes have been lost.

ITG Card Properties window

To display the property sheet of an IP trunk card, double-click an IP trunk card in the ITG Main window.

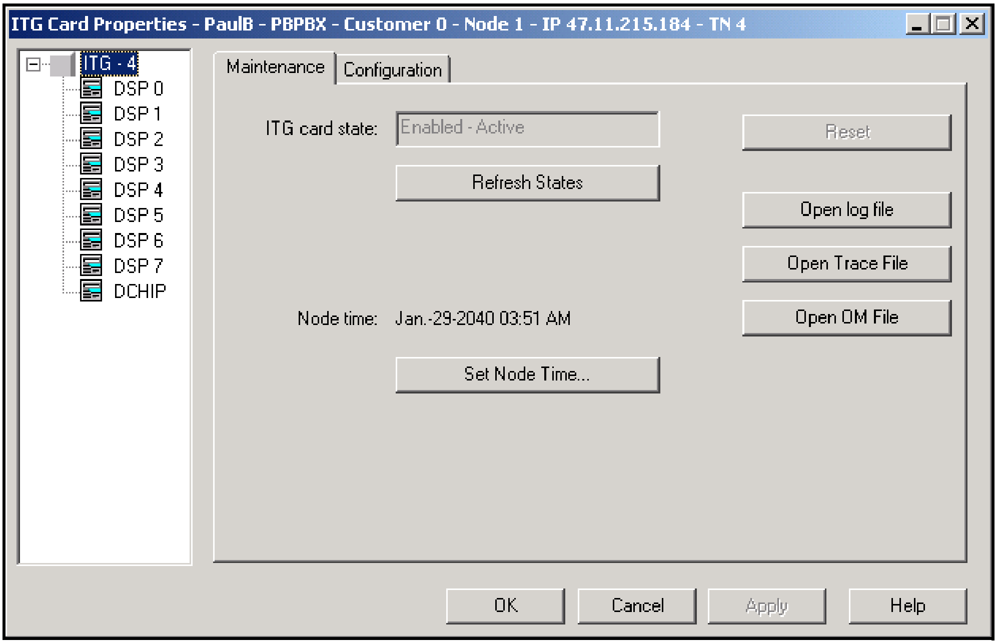
The property sheet has a tree control on the left-hand side of the window, enabling control of the IP trunk card or any of the DSPs. Different property sheets appear for IP trunk cards, DSPs, and D-channels by clicking on the required item in the tree. ITG determines the number of DSPs at run-time when the property sheet opens. If the card is not responding, the number of DSPs is unknown and no DSPs are displayed. The D-channel appears in the tree control only if D-channel hardware exists on the card.

There are tabs across the top of the ITG Card Properties window. The following sections describe the windows that appear when these tabs are clicked.

ITG Card Properties – Maintenance window

Click the Maintenance tab to perform maintenance operations. See Figure 138. click the appropriate button in the Maintenance window to perform the required operation.

Figure 138
ITG Card Properties – Maintenance tab



ITG Card Properties - PaulB - PBPBX - Customer 0 - Node 1 - IP 47.11.215.184 - TN 4

ITG card state: Enabled - Active

Node time: Jan.-29-2040 03:51 AM

The following comments apply to the operations in the ITG Properties Maintenance window:

- To perform Enable, Disable, and Perform operations, use the OTM Maintenance Windows or System Terminal applications.
- The **Reset** button is disabled when the IP trunk card is enabled.
- Use the Set Node Time to change the time and date on the node. The node time is updated every minute while the Card Properties is open.

- Use the **Open log file**, **Open trace file**, and the **Open OM file** buttons to view the related files. These files are transferred from the card using FTP and displayed in Microsoft WordPad on the PC.
- The trace file is for expert level debugging (trace must be turned on through the command line).
- The log file contains error messages.
- The OM file contains the current Operational Measurements.
- Setting the node time is required during initial node installation. OTM sets the Leader card's time. The Leader sets the time on all other cards.

Configure date and time for the IP Trunk 3.01 (and later) node

Configure the date and time on the IP Trunk 3.01 (and later) node in order to have correct time and date stamps in Operational Measurement (OM) reports, RADIUS Call Accounting reports, error messages and error and trace logs.

Follow the steps in Procedure 54 to configure the date and time.

Procedure 54
Configure the date and time

1 Select the IP Trunk 3.01 (and later) node for which the time and date is to be configured from the list in the upper part of the window.

2 Double-click Leader 0 from the list in the lower part of the window.

The ITG Card Properties **Maintenance** tab appears.

3 Click the **Set Node Time** button. The **Set Node Time** dialog box appears.

4 Set the correct date and time.

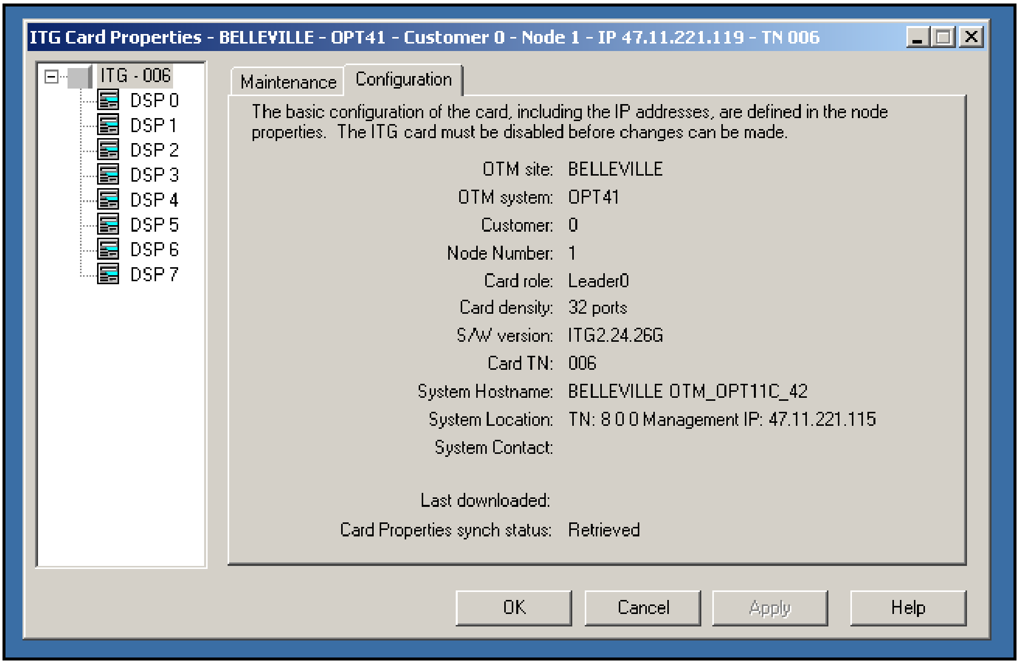
5 Click **OK**. The clock is updated immediately on the Active Leader card (Leader 0 or Leader 1), which in turn updates the other cards in the ITG ISL Trunk node.

End of Procedure

ITG Card Properties – Configuration window

The Configuration window for the IP trunk card contains the information shown in Figure 139. The ITG Card Properties Configuration window provides read-only information. Go to the Node Properties Card Configuration window to change this data. The Software version is retrieved from the card through the MIB. If the card is not responding, the value is set to “Unknown”.

Figure 139
ITG Card Properties – Configuration tab



ITG Card Properties - BELLEVILLE - OPT41 - Customer 0 - Node 1 - IP 47.11.221.119 - TN 006
ITG - 006
DSP 0
DSP 1
DSP 2
DSP 3
DSP 4
DSP 5
DSP 6
DSP 7
Maintenance
Configuration
OK
Cancel
Apply
Help

The basic configuration of the card, including the IP addresses, are defined in the node properties. The ITG card must be disabled before changes can be made.

OTM site: BELLEVILLE
OTM system: OPT41
Customer: 0
Node Number: 1
Card role: Leader0
Card density: 32 ports
S/W version: ITG2.24.26G
Card TN: 006
System Hostname: BELLEVILLE OTM_OPT11C_42
System Location: TN: 8 0 0 Management IP: 47.11.221.115
System Contact:

Last downloaded:
Card Properties synch status: Retrieved

For more information about maintenance commands, see “Maintenance” on page 515.

DSP maintenance window

> ***Note:*** If the IP trunk card is not responding, no DSP icons appear in the tree on the left-hand side of the ITG Card Properties window.

click the required DSP icon in the tree on the left-hand side of the ITG Card Properties window. The DSP Maintenance window appears which contains the state of the DSP and the Self Test command. click the Self Test button to perform a self-test on the DSP. The command is sent to the IP trunk card through SNMP.

> ***Note:*** If the DSP self-test fails, try to reset the card. If it fails again, replace the card.

D-channel maintenance

If the IP trunk card has D-channel hardware, the tree on the left side of the window contains the D-channel. click the D-channel and the D-channel Maintenance window appears. This window allows D-channel maintenance operations to be performed. The commands are sent to the card through SNMP.

> ***Note:*** The menu items are not context-sensitive. For example, it is possible to try to enable an enabled D-channel.

Transmit configuration data

OTM converts the IP Trunk 3.01 (and later) node and IP trunk card configuration data to text files and transmits the files to the IP trunk cards using FTP. The text files are as follows:

- Node properties: **BOOTP.1** (only transmitted to the Active Leader)
- Dialing plan: **DPTABLE.1** (transmitted to every card)
- Card properties: **CONFIG1.INI** (transmitted to every card)

BOOTP.1 is downloaded to the Leader card and copied to the Backup Leader. All other IP trunk cards in the node use BOOTP.1 to retrieve their bootup data from this table. OTM downloads the CONFIG1.INI file to each IP trunk card. It also downloads the DPTABLE.1 file to each IP trunk card.

The ITG Main window displays the synchronization status of each of these fields. Changes to the first two tabs (General and Card Configuration) in the Node Properties sheet affect the Node Synchronization Status. Changes to the other tabs (DSP Profile, SNMP Trap/Routing table IPs, Accounting Server, and Security) in the Node Properties sheet affect the Card Synchronization Status. These changes must be transmitted to each card in the node.

Select the “Configuration” pull-down menu in the Main ITG window. From this menu, select menu **Synchronize > Transmit**. The ITG Transmit Options window appears (see Figure 140. This window allows enables multiple files to be transmitted to one or more IP trunk cards.

Follow the steps in Procedure 55 to transmit configuration data,

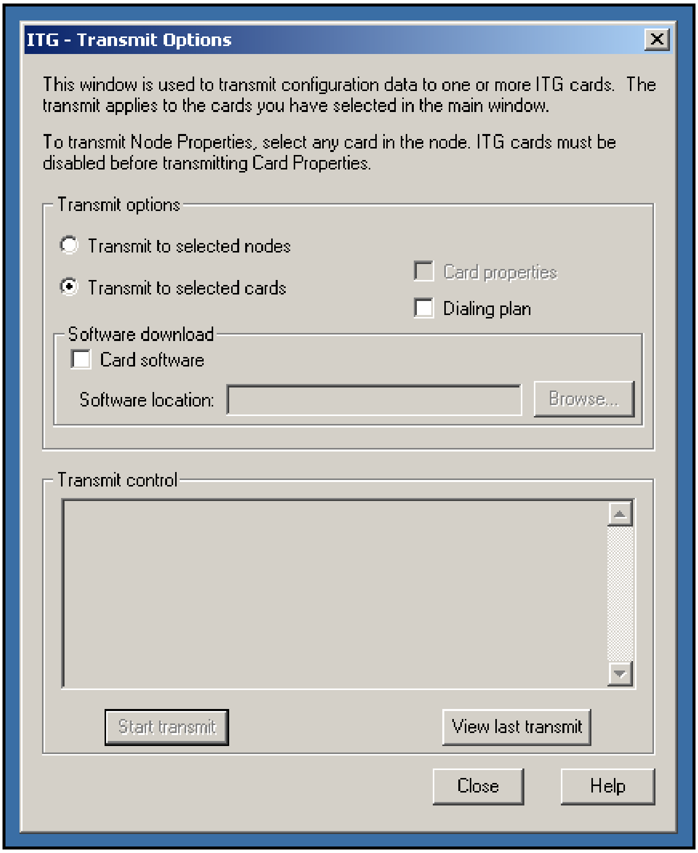
Procedure 55
Transmitting configuration data to the IP trunk cards

1. Select the IP trunk cards in the **ITG Main** window.
2. Select a Transmit option.
3. Click **Start transmit**. See Figure 140 on page 468.

End of Procedure

OTM transfers the data to the appropriate cards using FTP.

Figure 140
ITG Transmit Options window



ITG - Transmit Options

This window is used to transmit configuration data to one or more ITG cards. The transmit applies to the cards you have selected in the main window.

To transmit Node Properties, select any card in the node. ITG cards must be disabled before transmitting Card Properties.

Transmit options

○ Transmit to selected nodes

● Transmit to selected cards

□ Card properties

□ Dialing plan

Software download

□ Card software

Software location:

The following comments apply to the ITG Transmit Options:

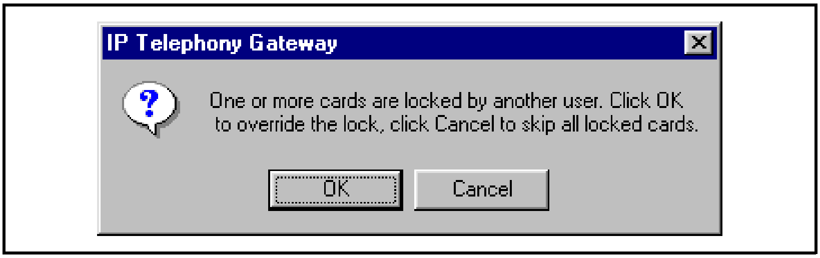
- To transmit Node Properties (BOOTP.1), select the node in the top window.
- Node Properties (BOOTP.1) can be transmitted while the IP trunk cards are enabled, but do not take effect until all the IP trunk cards in the node are rebooted.

- To transmit Card Properties (CONFIG1.INI), the entire node in the top window or an individual card can be selected, but in either case it is necessary to select to transmit to the entire node.
- Card Properties (CONFIG1.INI) can only be transmitted to the IP trunk cards when the cards are disabled.
- For the Card Properties (CONFIG1.INI) to take effect, the IP trunk cards must be re-enabled.
- To transmit the Dialing Plan (DPTABLE.1), select the node in the top window or select each individual card below. In either case, it is necessary to select to transmit to the entire node.
- The Dialing Plan (DPTABLE.1) can be transmitted to the IP trunk cards while the cards are enabled and takes effect immediately.
- The Dialing Plan (DPTABLE.1) stores the Gatekeeper information and updates the Gatekeeper information immediately.
- Transmit Control shows the status of the transmission operation and any errors which might occur (for example, if an IP trunk card is not responding).
- Each time one of the files is transmitted to an IP trunk card or to the node, it is necessary to confirm the transmission by clicking **OK** in the Confirmation window.
- The **Cancel Transmit** button is disabled until has begun. When the transmission begins, the **Close** button is disabled. Cancel the active transmission to close the window.
- The **View Last Transmit** button displays the results of the last transmission on the list box. When a transmission is started, the list clears and the **View Last Transmit** button is disabled.
- If there are no IP trunk cards selected, the Synchronization menus are disabled.
- Transmission of Card Properties fails if the card is not disabled.

When transmitting to an IP trunk card which is locked by another user, the second user is provided with the option to override the lock. See Figure 141. The lock is only checked during the Transmit operation. If multiple cards are involved in the operation, the second user is only provided with the Locked ITG dialog box once.

When the OM reports have been scheduled, the locked card is bypassed and the event is noted in the OM error log and in the PC event log.

Figure 141
Locked IP trunk card message



One or more cards are locked by another user. Click OK to override the lock, click Cancel to skip all locked cards.

Add an IP Trunk 3.01 (and later) node on OTM by retrieving an existing node

After an IP Trunk 3.01 (and later) node is manually configured and installed, that node can be added to another OTM 2.1 (and later) PC by retrieving the configuration data from the existing IP Trunk 3.01 (and later) node.

Use this **optional** procedure to perform the following actions:

- To combine existing IP Trunk 3.01 (and later) nodes on the network that were originally configured from different OTM PCs onto one OTM 210 PC to manage the IP Trunk 3.01 (and later) network from a single point of view.

- To restore the IP Trunk 3.01 (and later) configuration database to an OTM 2.1 (and later) PC whose hard drive had failed. (The OTM IP Trunk 3.01 (and later) nodes can also be restored from the Full OTM Backup.)
- To temporarily create a copy of the IP Trunk 3.01 (and later) node configuration on another PC for maintenance and diagnostic purposes. For example, a copy of an IP Trunk 3.01 (and later) node database can be created on an OTM 2.1 (and later) PC located at a remote technical support center.

The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the OTM 2.1 (and later) Navigator before a new IP Trunk 3.01 (and later) node can be added. Multiple IP Trunk 3.01 (and later) nodes can be added in the OTM ITG ISDN IP Trunks application for each Meridian 1 customer.

> ***Note:*** If multiple OTM 2.1 (and later) PCs are used to manage the same IP Trunk 3.01 (and later) network and the PCs are not using file-sharing, caution must be taken to synchronize the different copies of the IP Trunk 3.01 (and later) database. Use the OTM 2.1 (and later) ITG menu **Configuration > Synchronize > Retrieve** function to synchronize the OTM IP Trunk 3.01 (and later) database with the IP Trunk 3.01 (and later) node's database.

Retrieve and add an IP Trunk 3.01 (and later) node for administration purposes

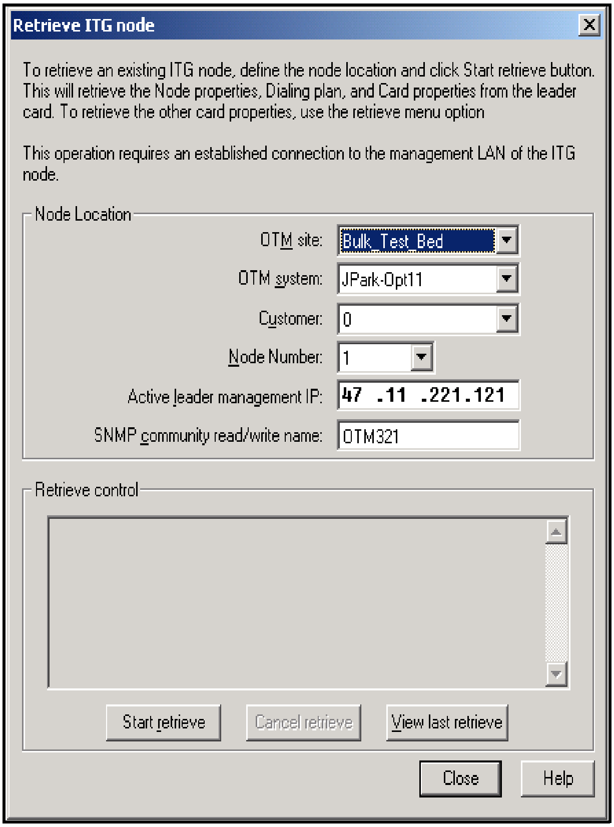
Follow the steps in Procedure 56 to retrieve and add an IP Trunk 3.01 (and later) node for administration purposes.

Procedure 56
Retrieving and adding an IP Trunk 3.01 (and later) node for administration purposes

1. Double-click the **ITG ISDN IP Trunks** icon from the **Services** folder. The **IP Telephony Gateway** - **ISDN IP Trunk** window opens.
2. In the **IP Telephony Gateway** - **ISDN IP Trunk** window, select the drop-down list **Configuration** > **Node** > **Add**. The ADD ITG Node dialog box appears.

3 Click the second option **Retrieve the active configuration from an existing node**. Leave “Meridian 1” as the default “System type”. Click **OK**. The **Retrieve ITG Node** window appears. See Figure 142.

Figure 142
Retrieve ITG node window



Retrieve ITG node

To retrieve an existing ITG node, define the node location and click Start retrieve button. This will retrieve the Node properties, Dialing plan, and Card properties from the leader card. To retrieve the other card properties, use the retrieve menu option

This operation requires an established connection to the management LAN of the ITG node.

Node Location

OTM site: Bulk_Test_Bed

OTM system: JPark-Opt11

Customer: 0

Node Number: 1

Active leader management IP: 47 .11 .221.121

SNMP community read/write name: OTM321

Retrieve control

4 In the **Retrieve ITG node** window, select the **OTM Site**, **OTM System**, and **Customer** number from the drop-down lists.

Note: The site name, system name, and customer number must exist in the OTM Navigator before a new IP Trunk 3.01 (and later) node can be added.

5 Enter the ELAN network interface IP address field for Leader 0 or Leader 1 on the existing node.

6 Enter the **SNMP read/write community name** string. The default is “otm321”.

Note: To retrieve an ITG card, the SNMP read community name string cannot be used.

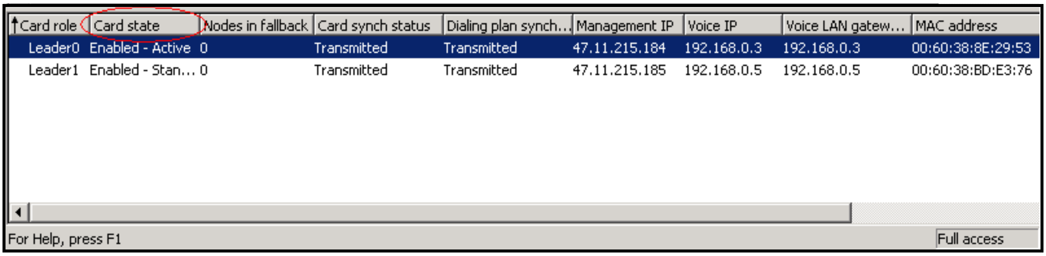
7 Click the **Start Retrieve** button.

The Retrieve control dialog box displays the results of the retrieval. The node properties, card properties and dialing plan are retrieved from the Leader card.

8 Click **Close** when the download is complete.

9 Refresh the card status and check that the cards in the new node are responding.To determine the IP trunk card status, in the **IP Telephony Gateway – ISDN IP Trunk** window click **View > Refresh > All.**
Look at the IP trunk card in the bottom window and see what is under the title “Card State”. See Figure 143.

Figure 143
Determine IP trunk card status



Card role	Card state	Nodes in fallback	Card synch status	Dialing plan synch...	Management IP	Voice IP	Voice LAN gatew...	MAC address
Leader0	Enabled - Active	0	Transmitted	Transmitted	47.11.215.184	192.168.0.3	192.168.0.3	00:60:38:8E:29:53
Leader1	Enabled - Stan...	0	Transmitted	Transmitted	47.11.215.185	192.168.0.5	192.168.0.5	00:60:38:BD:E3:76

For Help, press F1

Full access

End of Procedure

Retrieve and add an IP Trunk 3.01 (and later) node for maintenance and diagnostic purposes

Follow the steps in Procedure 57 to create a "dummy" IP Trunk 3.01 (and later) node for retrieving and viewing the real IP Trunk 3.01 (and later) node configuration, without overwriting the existing IP Trunk 3.01 (and later) configuration data for an existing node in the OTM IP Trunk 3.01 (and later) database. Retrieving the real IP Trunk 3.01 (and later) node configuration to the "dummy" node is useful in the following cases:

- isolating IP Trunk 3.01 (and later) node configuration faults
- determining which copy of the database is correct, so that the required direction of database synchronization can be determined:
  - transmit the OTM IP Trunk 3.01 (and later) database to the IP Trunk 3.01 (and later) node
  - retrieve the database from the IP Trunk 3.01 (and later) node for the OTM IP Trunk 3.01 (and later) node

Add the dummy node manually or by retrieving the IP Trunk 3.01 (and later) node configuration data from an existing IP Trunk 3.01 (and later) node.

The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the OTM Navigator before a new IP Trunk 3.01 (and later) node can be added.

The following is the recommended method to create the "dummy" IP Trunk 3.01 (and later) node.

Procedure 57
Creating a 'dummy" IP Trunk 3.01 (and later) node

1. In OTM Navigator, add a site named "Retrieve ITG data".
2. Add system named "Dummy," of type "Meridian 1," under the site named "Retrieve ITG data".
3. Add Customer Number "99" on the "dummy" Meridian 1 system.

End of Procedure

To view the data of a real IP Trunk 3.01 (and later) node, select the "dummy" node and change the ELAN network interface IP address in the node properties to access the needed node. Use the menu **Configuration > Synchronize > Retrieve** function to retrieve data from that node and overwrite the dummy node's data.

Configuration audit

In this procedure, retrieve the card properties and dialing plan from each IP trunk card in the selected IP Trunk 3.01 (and later) nodes. OTM compares the retrieved data with the card properties and dialing plan currently stored in the OTM 2.1 (and later) database. OTM 2.1 (and later) provides a report that shows cards where the data matches and cards where the data is different. To view the differences, use the menu **Configure > Node > Add** to add a temporary node. Then use the menu **Configure > Synchronize > Retrieve** to retrieve the IP trunk card properties or dialing plan from the selected IP trunk card. Double-click the temporary node to view the IP trunk card properties and open the dialing plan for the temporary node to view the dialing plan entries. Compare the data with the properties and dialing plan for the currently stored IP Trunk 3.01 (and later) node in OTM 2.1 (and later).

Retrieve IP Trunk 3.01 (and later) configuration information from the IP Trunk 3.0 (and later) node

Use the optional Procedure 58 on page 476 in the following situations:

- when adding an IP Trunk 3.01 (and later) node on OTM by retrieving an existing node
- when it is known that the IP Trunk 3.01 (and later) node configuration on the IP trunk card is different from the OTM IP Trunk 3.01 (and later) database (for example, during maintenance and fault isolation procedures)
- when there are multiple OTM PCs with multiple instances of the database (administration)

Use the OTM ITG menu **Configuration > Synchronize > Retrieve** command to retrieve the IP Trunk 3.01 (and later) configuration information from the IP Trunk 3.01 (and later) node.

Procedure 58
Retrieving the IP Trunk 3.01 (and later) configuration data from the IP Trunk 3.01 (and later) node

1 Launch OTM and double-click the ITG ISDN IP Trunks icon from the **Services** folder. The **IP Telephony Gateway - ISDN IP Trunk** window opens.

2 Select Leader 0 or any card from the node.

3 Select menu **Configuration > Synchronize** > **Retrieve.** The **ITG - Retrieve Options** window appears.

4 Check the boxes for the IP Trunk 3.01 (and later) configuration data to be retrieved.

Note 1: Select **Node Properties**, **Card Properties**, and **Dialing Plan** if the OTM IP Trunk 3.01 (and later) data is out of date and all OTM IP Trunk 3.01 (and later) node data is to be synchronized with the data from the IP trunk cards on the node.

Note 2: Select **Card Properties** to add an IP Trunk 3.01 (and later) node on OTM by retrieving from an existing node that contains more than one card.

Note 3: Select any combination of check boxes as indicated by problem symptoms when attempting to isolate a problem on a particular IP trunk card. Use the "dummy" node for this purpose.

5 Select **Prompt user for community name** if required.

6 Click the **Start retrieve** button.

End of Procedure

Monitor the status of the retrieval in the **Retrieve control** box. The retrieved **Node Properties**, **Card Properties**, and **Dialing Plan** over-writes the existing OTM IP Trunk 3.01 (and later) configuration data for the respective node or IP trunk card.

When a dialing plan table is retrieved, OTM IP Trunk 3.01 (and later) compares it against the existing node dialing plan and discards it if it is identical. If the dialing plan table is different, it is necessary to confirm the overwrite before the existing IP Trunk 3.01 (and later) node dialing plan on OTM IP Trunk 3.01 (and later) is overwritten.

Schedule and generate and view IP Trunk 3.01 (and later) OM reports

Operational Measurement (OM) reports are a collection of OM data from all the IP trunk cards defined on the OTM PC or server. A report can be generated on request or the report scheduled to generate at a selected time. Each time a report is generated, the application retrieves the latest OM data from each Media Card 32-port and ITG-Pentium 24-port trunk card defined in OTM. This data is then added to a comma separated file on the OTM PC. A new file is created for each month of the year for which OM data is collected. The files are named for the month and year (for example, itg_04_1999.csv).

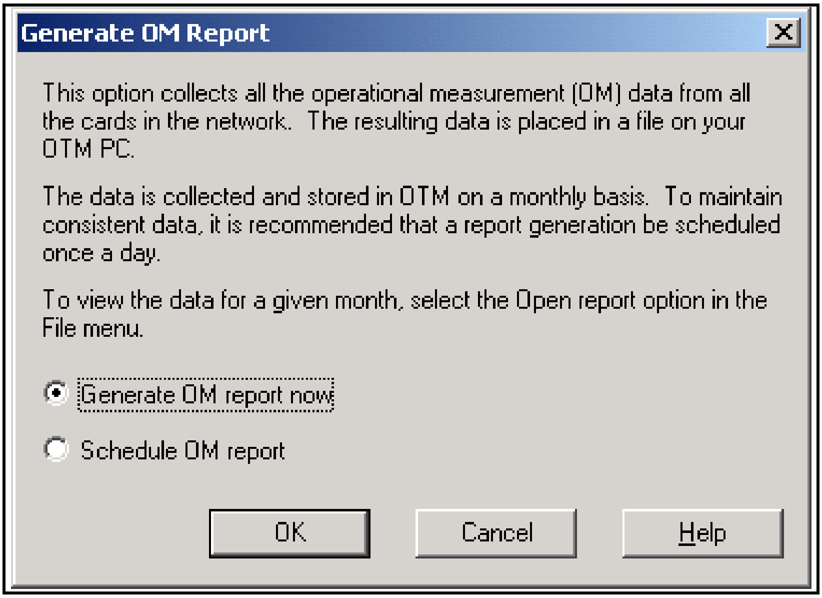
Follow the steps in Procedure 59 to schedule, generate, and view IP Trunk 3.01 (and later) OM reports.

Procedure 59
Scheduling, generating, and viewing IP Trunk 3.01 (and later) OM reports

1 To generate or schedule a report:

- **a.** From the **IP Telephony Gateway Main** window, select **File > Report > Generate**. The **Generate OM Report** window appears. See Figure 144 on page 478.

Figure 144
Generate OM Report



This option collects all the operational measurement (OM) data from all the cards in the network. The resulting data is placed in a file on your OTM PC.

The data is collected and stored in OTM on a monthly basis. To maintain consistent data, it is recommended that a report generation be scheduled once a day.

To view the data for a given month, select the Open report option in the File menu.

● Generate OM report now

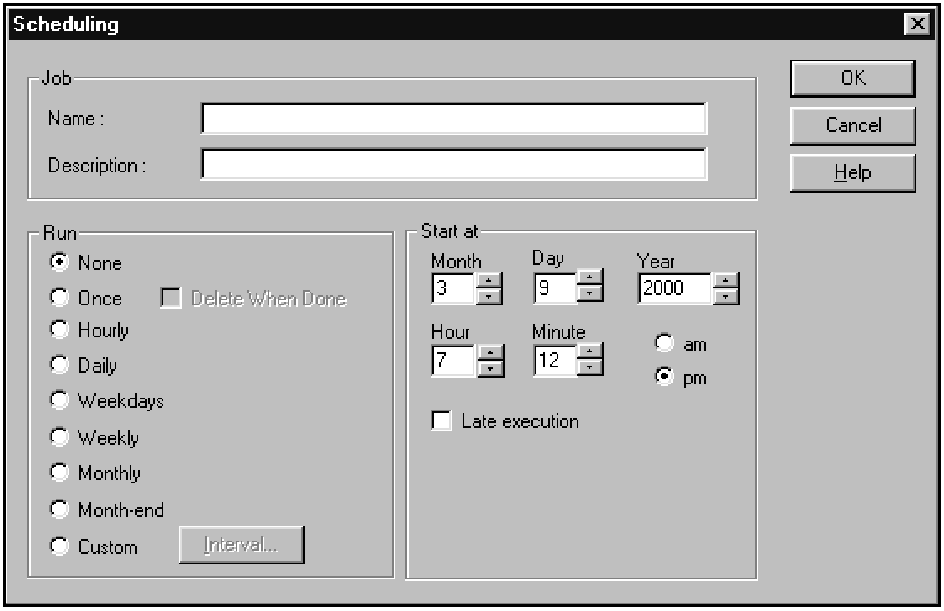
○ Schedule OM report

- **b.** To generate a report immediately, click **Generate OM Report**. OTM 2.1 prepares the report and displays the information in a .csv spreadsheet format.
- **c.** To schedule a report, click **Schedule OM Report**. A Scheduling window appears (see Figure 145 on page 479). Fill in the fields to schedule the report and define the times and information. Schedule report generation at least once a day. Click **OK**.

2 To open and view a report:

- **a.** Select **File > Report > Open**. The **Open OM Report** dialog box appears.
- **b.** Double-click an OM report. The report appears in Microsoft Excel. If Excel is not available, use an application that recognizes .csv (comma-separated) files to view the report.

Figure 145
OM Report scheduling window



Scheduling

Job
Name :
Description :

Run
● None
○ Once □ Delete When Done
○ Hourly
○ Daily
○ Weekdays
○ Weekly
○ Monthly
○ Month-end
○ Custom

Start at
Month: 3
Day: 9
Year: 2000
Hour: 7
Minute: 12
○ am
● pm
□ Late execution

End of Procedure

Backup and restore operations

The Media Card 32-port and ITG-Pentium 24-port trunk cards support backup and restore procedures for critical configuration data. If a failed IP trunk card is replaced with a spare, the dialing plan tables, DSP configuration, passwords, and other configuration data are restored from the OTM 2.1 (and later) PC.

The OTM 2.1 (and later) application has a backup and restore procedure for all data downloaded to and from the IP trunk card. If OTM 2.1 (and later) is not available, use the ITG shell Command Line Interface (CLI) to retrieve the configuration files from an FTP server or from a PC card.

IP Trunk 3.01 (and later) data is stored in an Access database file on the OTM 2.1 (and later) PC or server, or in the OM files. These files are only backed up when the “Full OTM Backup” option is selected. This option backs up all OTM data and can be used only to restore all data.

Alarm Notification

IP Trunk 3.01 (and later) uses the OTM Alarm Notification application. This application receives SNMP traps from any device connected to the network. When received, traps appear in an event browser. Write scripts to generate notification messages to pagers, e-mail, and SNMP network management systems. The IP trunk card must be configured to send SNMP traps to the OTM PC, if SNMP traps are being used. See “Configure OTM Alarm Management to receive SNMP traps from the IP trunk cards” on page 367.

> ***Note:*** For more information about Alarm Notification, please refer to Alarm Management in *Optivity Telephony Manager: System Administration* (553-3001-330).

System commands – LD 32

The following system administration commands can be performed in LD 32:

- “Disable the indicated IP trunk card” on page 483.

  Note 1: The IP trunk card must be disabled before card properties can be transmitted from the OTM IP Trunk 3.01 (and later) application to the IP trunk card.

  Note 2: The IP trunk card reset button is only available in the OTM IP Trunk 3.01 (and later) application when the IP trunk card is disabled.

  Note 3: Disabling the IP trunk card in LD 32 does not disable the Active Leader, Backup Leader, or DCHIP functions.

- “Disable the indicated IP trunk card when idle” on page 483.

  Note: This temporarily prevents the IP Trunk 3.01 (and later) node from seizing the port from incoming calls.

- “Disable an indicated IP trunk card port” on page 484.

- “Enable an indicated IP trunk card” on page 484.
- “Enable an indicated IP trunk card port” on page 484.
- “Display IP trunk card ID information” on page 484.

  Note 1: This command displays the PEC (Product Engineering Code) for the card. The ITG PEC is as follows:
  ITG 8-port trunk card – NT0961AA
  ITG-Pentium 24-port trunk card – NT0966AA
  Media Card 32-port trunk card – NT0966BA

  Note 2: The IP trunk card information displays the same IP trunk card serial number that is displayed from the ITG shell using the **serialNumShow**.

- “Display IP trunk card status” on page 485.
- “Display IP trunk card port status” on page 485.

A summary list of IP Trunk 3.01 (and later) system commands available in LD 32 is shown in Table 51.

Table 51
LD 32 – IP Trunk 3.01 (and later) maintenance commands (Part 1 of 2)

Command	Description
DISC l s c	Disable the indicated card, where: l = loop, s = shelf, c = card
DISI l s c	Disable the indicated card when idle, where: l = loop, s = shelf, c = card ***Note:*** Use the DISI command to disable the IP trunk card instead of the DISC command. The disablement of the IP trunk card is indicated by the NPR011 message.
DISU l s c u	Disable the indicated unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the described card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the described unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the described card, where: l = loop, s = shelf, c = card

Table 51
LD 32 – IP Trunk 3.01 (and later) maintenance commands (Part 2 of 2)

Command	Description
STAT l s c	Print the system software status of the indicated card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the system software status of the indicated unit, where: l = loop, s = shelf, c = card, u = unit

Disable the indicated IP trunk card

To disable the indicated IP trunk card in LD 32, use the following command:

DISC l s c	Disable the indicated IP trunk card, where: l = loop, s = shelf, c = card

Disable the indicated IP trunk card when idle

To disable the indicated IP trunk card when idle in LD 32, use the following command:

DISI l s c	Disable the indicated IP trunk card when idle, where: l = loop, s = shelf, c = card

Enable an indicated IP trunk card

To enable an indicated IP trunk card in LD 32, use the following command:

ENLC l s c	Enable the indicated IP trunk card, where: l = loop, s = shelf, c = card

Disable an indicated IP trunk card port

To disable an indicated IP trunk card port in LD 32, use the following command:

DISU l s c u	Disable the indicated ITG unit (port), where: l = loop, s = shelf, c = card, u = unit

Enable an indicated IP trunk card port

To enable a indicated IP trunk card port in LD 32, use the following command:

ENLU l s c u	Enable the indicated ITG unit (port), where: l = loop, s = shelf, c = card

Display IP trunk card ID information

To display the IP trunk card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the IP trunk card, where: l = loop, s = shelf, c = card

Display IP trunk card status

To display the status of a indicated IP trunk card in LD 32, use the following command:

STAT l s c	Display the status of the indicated IP trunk card, where: l = loop, s = shelf, c = card

Display IP trunk card port status

To display the status of a port on the IP trunk card in LD 32, use the following command:

STAT l s c u	Display the status of the indicated ITG port, where: l = loop, s = shelf, c = card, u = unit.

OA&M using the ITG shell CLI and overlays

Contents

This section contains information on the following topics:

Introduction

This chapter explains how to perform IP Trunk 3.01 (and later) Operation, Administration, and Maintenance (OA&M) tasks using the ITG shell Command Line Interface (CLI). The ITG shell can be accessed directly through a serial port connection, or remotely through Telnet from the OTM 2.1 (and later) PC or any Telnet client host.

ITG Shell OA&M procedure summary

The following OA&M tasks can be performed from the ITG shell:

- “Change the default ITG shell password to maintain access security” on page 492.
- “Reset the default ITG shell password” on page 493.
- “Download the ITG operational measurements through the ITG shell” on page 495.
- “Reset the operational measurements” on page 496.
- “Display the number of DSPs” on page 496.
- “Display IP Trunk 3.01 (and later) node Properties” on page 496.
- “Display IP Trunk 3.01 (and later) Gatekeeper status” on page 499
- “Transfer files through the Command Line Interface” on page 501.
- “Upgrade IP trunk card software using FTP” on page 504.
- “Backup and restore from the CLI” on page 506.
- “Recover the SNMP community names” on page 508

- "IP Trunk 3.01 (and later) configuration commands" on page 509.
- "Download the IP Trunk 3.01 (and later) error log" on page 509.

Access the ITG shell through a maintenance port or Telnet

The ITG shell administration and maintenance commands can be accessed in two ways:

- Log in through a direct cable connection between the IP trunk card faceplate maintenance port and a PC.
- Access the ITG shell from the OTM PC. Refer to "Telnet to an IP trunk card through the OTM PC" on page 490 for details.

Connect a PC to the card maintenance port

Follow the steps in Procedure 60 to connect a PC to the IP trunk card maintenance port.

Procedure 60
Connecting a PC to the IP trunk card maintenance port

1 To access the ITG shell, connect a PC to the RS-232 serial maintenance port through DIN-8 connector on the faceplate of the ITG Leader 0 card with an NTAG81CA PC Maintenance cable. If required, use an NTAG81BA Maintenance Extender cable to provide an extension between the NTAG81CA PC Maintenance cable and the OTM PC.

Alternatively, for the ITG-Pentium 24-port trunk card, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTCW84KA ELAN, TLAN, DCH, and Maintenance Port cable (for DCHIP cards), or the NTMF94EA ELAN, TLAN, Maintenance Port cable (for non-DCHIP cards), to create a more permanent connection to the IP trunk card serial maintenance port.

For the Media Card 32-port trunk card, a serial connection can be established by using the DB-9 connector located on the "L-Adaptor" A0852632.

Note: Never connect two terminals to the front and back serial maintenance port connectors at the same time.

2 Use the following communication parameters for the TTY terminal emulation on the PC:

- 9600 baud
- 8 bits
- no parity bit
- one stop bit

3 When prompted to login, enter current username and password. Default is:

VxWorks login: **itgadmin**
Password: **itgadmin**

ITG>

End of Procedure

Only one person can use the ITG shell at a time. Any session, local or Telnet, can be overridden by a second session. The second user receives a warning before the login and must confirm to complete the login. There is a 20-minute Telnet shell activity time-out limit.

Telnet to an IP trunk card through the OTM PC

Follow the steps in Procedure 61 to Telnet to an IP trunk card through the OTM PC.

Procedure 61
Telnetting to an IP trunk card through the OTM PC

1 In the **OTM Navigator** window select the **IP Telephony Gateway** icon from the **Services** folder.

2 Select a card from the lower portion of the window. Click the right mouse button. Select **Telnet to ITG card** (see Figure 146 on page 491). The PC opens a Telnet window and automatically connects to the IP trunk card by using the card Elan network interface IP address.

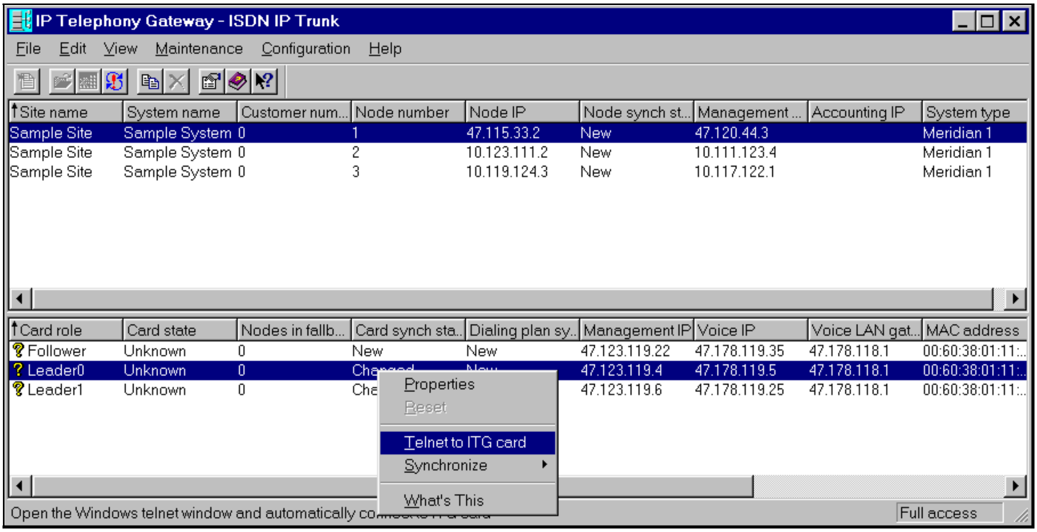
3 When prompted to login, enter current username and password. Default is:

VxWorks login: **itgadmin**
Password: **itgadmin**

ITG>

Only one person can use the ITG shell at a time. Any session, local or Telnet, can be overridden by a second session. The second user receives a warning before the login and must confirm to complete the login. There is a 20-minute Telnet shell activity time-out limit.

Figure 146
Select card and open Telnet session



IP Telephony Gateway - ISDN IP Trunk

Site name	System name	Customer num...	Node number	Node IP	Node synch st...	Management ...	Accounting IP	System type
Sample Site	Sample System	0	1	47.115.33.2	New	47.120.44.3		Meridian 1
Sample Site	Sample System	0	2	10.123.111.2	New	10.111.123.4		Meridian 1
Sample Site	Sample System	0	3	10.119.124.3	New	10.117.122.1		Meridian 1

Card role	Card state	Nodes in fallb...	Card synch sta...	Dialing plan sy...	Management IP	Voice IP	Voice LAN gat...	MAC address
Follower	Unknown	0	New	New	47.123.119.22	47.178.119.35	47.178.118.1	00:60:38:01:11:...
Leader0	Unknown	0	Changed	New	47.123.119.4	47.178.119.5	47.178.118.1	00:60:38:01:11:...
Leader1	Unknown	0	Cha		47.123.119.6	47.178.119.25	47.178.118.1	00:60:38:01:11:...

Open the Windows telnet window and automatically connect to ITG card

Full access

4 Perform the following action to increase the Telnet terminal buffer size to capture multiple screens of data from the IP trunk card:

From the Telnet “Terminal” menu, select “Preferences”. Set the Buffer Size to a larger value, such as 1000, and click “OK”. The Telnet buffer size has to be only once, because Telnet preferences are automatically saved.

5 To prevent the loss of diagnostic data from the IP trunk card if the Telnet session terminates unexpectedly, enable logging of Telnet sessions on the OTM PC:

From the Telnet "Terminal" menu, select "Start Logging". Use the "Browse" dialog to choose the appropriate folder and file name for Telnet log file for the current Telnet session. Open the Telnet log file using a text editor, such as Windows Notepad, or a word processor for large log files.

End of Procedure

Change the default ITG shell password to maintain access security

Schedule routine changes of user names and passwords to maintain access security. The ITG user name and password protects the maintenance port, FTP, and Telnet access to the IP trunk card over the LAN.

Follow the steps in Procedure 62 to change the default ITG shell password.

Procedure 62
Changing the default ITG shell password

1 From the ITG shell use the command **shellPasswordSet** to change the default user name and password for Telnet to ITG shell and FTP to the IP trunk card file system. The default user name is **itgadmin** and the default password is **itgadmin**.

2 Enter the current user name when prompted:

Enter current username: **itgadmin**
Enter current password: **itgadmin**
Enter new username: ***new name***
Enter new password: ***new password***
Enter new password again to confirm: ***new password***

End of Procedure

If the complete sequence of commands is correctly entered, the system response `value = 0 = 0x0` appears. The new user name and password are now stored in non-volatile RAM on the IP trunk card and retained when the card is reset or power-cycled.

Reset the default ITG shell password

If the ITG shell password is lost, the ITG shell user name and password can be reset to the default: **itgadmin**. This procedure requires physical access to the IP trunk card. This procedure cannot be done through Telnet.

Follow the steps in Procedure 63 to reset the default ITG shell password.

Procedure 63
Resetting the default ITG shell password

1 Connect a terminal to the IP trunk card maintenance port.

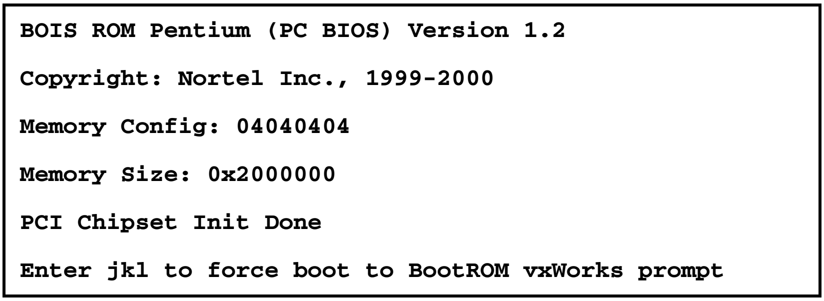
2 Press the reset button on the IP trunk card and observe the sequence of startup messages from the card.

3 Look for the prompt screen to enter the BIOS ROM.
There is a window of only approximately 2-3 seconds to enter the correct prompt (**jkl** for the Media Card 32-port trunk card and **jkl** for the ITG-Pentium 24-port trunk card).

Example of the Media Card 32-port trunk card prompt screen:

```
CPU: IXP1200

Version: 5.4

BSP Version: 5.0

Creation Date: Nov 22 2001, 18:21:11

Enter jkl to force boot to BootROM vxWorks prompt
```

Example of the ITG-Pentium 24-port trunk card prompt screen:



```
BOIS ROM Pentium (PC BIOS) Version 1.2

Copyright: Nortel Inc., 1999-2000

Memory Config: 04040404

Memory Size: 0x2000000

PCI Chipset Init Done

Enter jkl to force boot to BootROM vxWorks prompt
```

If the prompt "**vxWorks login:**" appears, the BIOS ROM prompt has been lost and the card must be reset again.

At the BIOS ROM shell prompt enter the following command:
-> **nvramClear**
This command clears the user configured password, the leader flag, and the IP configuration information from the NVRAM.

WARNING

If the Media Card 32-port trunk card or the ITG-Pentium 24-port trunk card asks for **xxx** to get into the BIOS, the firmware on that IP trunk card must be upgraded. Contact Nortel Technical Support for more information.

4 Press the reset button on the card again.

The IP trunk card starts up and displays "T:20" on the 4-character display. The IP trunk card begins sending BOOTP requests on the ELAN subnet. A series of dots appears on the TTY.

5 Type **+++** to bring up the ITG shell command line prompt:

```
.............. +++
```

When prompted to login, enter the default username and password as:

VxWorks login: **itgadmin**
Password: **itgadmin**

ITG>

6 If this card is Leader 0, use the setLeader command:

ITG> **setLeader xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz** and press **Enter**.

where:

- xxx.xxx.xxx.xxx is the IP address of the ELAN network interface on Leader 0.
- yyy.yyy.yyy.yyy is the gateway IP address for the ELAN network interface on Leader 0. If the OTM PC is connected directly to the LAN and there is no ELAN network interface gateway, then the gateway IP address is “0.0.0.0”.
- zzz.zzz.zzz.zzz is the subnet mask for the ELAN network interface on Leader 0.

7 Do not leave the card with the default user name and password. See “Change the default ITG shell password to maintain access security” on page 492.

8 Configure all the IP trunk cards in the same node with the same password. Repeat this procedure for other cards in the IP Trunk 3.01 (and later) node.

End of Procedure

Download the ITG operational measurements through the ITG shell

The ITG operational measurements file contains counts of incoming and outgoing calls, call attempts, calls completed, and total holding time for voice and fax calls. To download this file from the OTM PC to the IP trunk card, at the ITG shell prompt, type the following:

> **currOMFilePut** *<hostname, username, password, directory path, filename>* for the current file
> **or**
> **prevOMFilePut** *<hostname, username, password, directory path, filename>* for the previous file.

Reset the operational measurements

This command resets all operational measurement (OM) parameters collected after the last log dump.

At the ITG shell prompt, type:

```
resetOM
```

Display the number of DSPs

At the ITG shell prompt, type the following command to display the number of DSPs on the IP trunk card:

```
DSPNumShow
```

Display IP Trunk 3.01 (and later) node Properties

At the ITG shell prompt, type the following command to display information about an IP Trunk 3.01 (and later) node:

```
IPInfoShow
```

The following IP Trunk 3.01 (and later) node information appears on the TTY:

- IP addresses for the ELAN and TLAN network interfaces
- default router for the ELAN and TLAN network interfaces
- subnet mask for the ELAN and TLAN network interfaces
- SNMP manager

At the ITG shell prompt, type the following command to display information about an IP trunk card:

```
itgCardShow
```

The command **itgCardShow** prints out the information that was provisioned in OTM 2.1 (and later), such as the IP trunk card TN, protocol used, card role, IP addresses, and whether the DCH PC Card is on board. If the IP trunk card is enabled, the status of the IP trunk card (Card Mode) and the D-channel (DCH Status) is also displayed.

The following is an example of the **itgCardShow** command:

```
Index: 1
Type: ITG2
Role: Leader
Leader IP: 47.11.215.182
RTP Base Port: 2300,2300=>Default 173300+>Cisco
RTPHeaderCpmpresssion
Card IP: 47.11.215.186
Card MgtIP: 47.11.217.21
Ldr MgtIP: 47.11.217.21
Card TN: 9 0 0
Card State: ENBL
Card Mode: Normal
Codecs: G.711 mu-law (default), G.711 a-law, G.729AB,
G.729A
EC Tail Length: Value from OTM-32
DCHIP IP: 47.11.217.21
DCH Num: 10
DCH ON Card: YES (version 3.1)
DCH Status: ENBL
Protocol: SL1 ESN5
initBchNum: 1
esn5Prefix: |100|
TLAN set to Auto-negotiate Speed and Duplex Settings
TLAN currrently operate at: 100 Mbps (Carrier OK)
ELAN set to 10BaseT Operation
ELAN set to Half Duplex Operation
value = 38 = 0x26 = ‘&’
```

The following commands give additional information about an IP trunk card:

- **ldrResTableShow**
- **ifShow**
- **dongleIDShow**

- **serialNumShow**
- **firmwareVersionShow**
- **swVersionShow**
- **emodelSim**

Display IP Trunk 3.01 (and later) Gatekeeper status

At the ITG shell prompt, type the following command to display information about the IP Trunk 3.01 (and later) registration with a Gatekeeper:

```
gkShow
```

The following information appears on the TTY:

- provisioned information (for example, the H.323 node name, which card to register, and the Gatekeeper IP address)
- operational information, such as whether the IP trunk card is registered with the Gatekeeper and with which Gatekeeper the IP trunk card is registered (Primary or Alternate)
- when the next re-registration attempt will occur
- values from the Gatekeeper, such as Time To Live (TTL) and endpoint ID

Note: The time to re-register is based on the clock on the Leader 0 IP trunk card. If the clocks on the Leader 1 and Follower IP trunk cards are out of synchronization with the Leader 0 clock, the time to re-register might be incorrect. The time that the next re-register will occur is always correct on the Leader 0 IP trunk card.

The following is an example of the output of the **gkshow** command when there is only a Primary Gatekeeper.

```
---------------------------------------
<<PROVISIONED>>
The H.323 ID of this gateway is : [Shane_IPT_cust0]
First place dialed numbers are resolved: ATPM
Second place numbers are resolved : Gatekeeper
Cards that register with the Gatekeeper: All

<<OPERATIONAL>>
The Current Gatekeeper is : Primary
The Current Gatekeeper status is : Registered

<<From the Gatekeeper>>
The Time To Live (TTL) for the node is : 300 seconds
The remaining time to Re-Register is : 276 seconds
The Gateway End Point ID is :
.0.2.6.1.3.1.e.8.2.0.0.3.0.2.0.6.1.4.0.4.0.7.0.0.0.2.
b.3.8.6.2.6.a.7
The Gatekeeper has Pre-Granted ARQ : Not Granted -
direct calls possible

---------------------------------------
Primary Gatekeeper information <<PROVISIONED>>
----------------------------------------
Primary Gatekeeper type is : CSE1000
Primary Gatekeeper IP information is :
*Gatekeeper IP : 47.11.249.140
*QoS Enabled : 0
*Node Capability : 9 - CSE - Interop Format
---------------------------------------

value = 2 = 0x2
```

Transfer files through the Command Line Interface

Type one of the following commands at the ITG shell Command Line Interface (CLI) to enable these actions:

- transfer a file from the IP trunk card to an FTP host
- transfer a file from an FTP host to the IP trunk card

The correct command depends on the type of file to be transferred.

These commands are from the point of view of the IP trunk card. Commands with “Get” as part of the command name refer to file transfer from the FTP host to the IP trunk card. Commands with “Put” as part of the command name refer to file transfer from the IP trunk card to the FTP host.

For security reasons, there is no generic FTP client on the IP trunk card. A DIR or PWD (Print Working Directory) command cannot be performed on the FTP host.

The BOOTP.1 file (transferred by the “**bootPFileGet**” and “**bootPFilePut**” commands) contains node properties information. The DPTABLE.1 file (transferred by the “**DPAddrTGet**” and “**DPAddrTPut**” commands) contains the OTM IP Trunk 3.01 (and later) dialing plan information. The CONFIG1.INI file (transferred by the “**configFileGet**” command) contains card properties and SNMP information. The BOOTP.1 file is only sent to the Active Leader card, while the DPTABLE.1 and CONFIG1.INI files are sent to every IP trunk card.

Software update and file transfer commands

These commands are case-sensitive. The parameters that follow the command must each be enclosed in quotation marks. There must be a comma and no spaces between the parameters.

Refer to “Maintenance” on page 515 for a complete description of the ITG shell file transfer commands.

Hostname refers to the IP address of the FTP host. The FTP host can be a server on the network, the IP trunk card, or another IP trunk card in the same IP Trunk 3.01 (and later) node.

Software upgrade

Use this command in the procedure “Transmit new software to the IP trunk cards” on page 363.

swDownload *“hostname”, “username”, “password”, “directory path”, “filename”*

Generic file transfer:

Use the generic file transfer commands below for debug purposes. The first five parameters refer to the FTP host. The “ITGFileName” parameter refers to the directory path and file name on the IP trunk card. The “listener” parameter in the “hostFileGet” command identifies a software module to be called to parse the file after it has been correctly transferred to the IP trunk card. To avoid damaging the configuration files and the IP trunk card, only use the “hostFileGet” command under the direction of Nortel support personnel.

hostFileGet *“hostname”,"username”,"password”, “directory path”,"filename”,"ITGFileName”,"listener”*

hostFilePut *"hostname","username","password", "directory path","filename","ITGFileName"*

Configuration file transfer

Use these commands to backup and restore files when the preferred method, the OTM PC, is not available.

DPAddrTGet *"hostname","username","password", "directory path","filename"*

DPAddrTPut *"hostname","username","password", "directory path","filename"*

configFileGet *"hostname","username","password", "directory path","filename"*

configFilePut *"hostname","username","password", "directory path","filename"*

bootPFileGet *"hostname","username","password" , "directory path","filename"*

bootPFilePut *"hostname","username","password", "directory path","filename"*

OM trace and log files commands

Use these commands to put files on a host for additional analysis when OTM cannot.

currOmFilePut *"hostname","username","password", "directory path","filename"*

prevOmFilePut *"hostname","username","password", "directory path","filename"*

traceFilePut *"hostname","username","password" , "directory path","filename"*

currLogFilePut *"hostname","username","password", "directory path","filename"*

prevLogFilePut *"hostname","username","password", "directory path","filename"*

Upgrade IP trunk card software using FTP

Use Procedure 66 on page 506 to upgrade the IP trunk card software when the preferred method, described in “Transmit new software to the IP trunk cards” on page 363, is not available.

> ***Note:*** If the OTM PC is remotely connected to the IP Trunk 3.01 (and later) node with a a PPP link through the dialup modem router, then use this procedure to upgrade the IP trunk card from an FTP host. This ensures that the software file is transmitted intact before it is copied to the flash ROM device.

This procedure updates the IP trunk card software with the binary file received from an FTP host or IP trunk card with IP address *hostname*. The IP trunk card FTP client performs a *get* which downloads the file to the IP Trunk 3.01 (and later) flash device. A checksum is calculated to check correct delivery. When the new software version is correctly downloaded, reboot the IP trunk card with **cardReset** to run the new software.

Obtain the new IP trunk card software from the Nortel web site, or obtain a PC Card containing the newest software.

Follow the steps in Procedure 64 on page 504 to download the IP trunk card software from the Nortel web site.

Procedure 64
Downloading IP trunk card software from the internet

1. Download the IP trunk card software from the internet to a PC hard drive. Check the Nortel website to find the latest IP Trunk 3.01 (and later) software release. Go to www.nortel.com. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support.
2. Select the latest recommended software version and select the location on the OTM 2.1 (and later) PC hard drive where it is to be downloaded. Record the OTM 2.1 (and later) PC hard drive location for use later in the procedure.

End of Procedure

Alternatively, order the latest IP Trunk 3.01 (and later) software on a PC Card.

Upgrade IP trunk card software by PC Card

The PC Card can be obtained from Nortel with the latest IP trunk card software version. Update the IP trunk card software version on the PC Card by copying the file from the PC hard drive to the PC Card, which is inserted in a PC Card slot on the PC.

Follow the steps in Procedure 65 to upgrade the IP trunk card software using a PC Card.

Procedure 65
Upgrading IP trunk card software using a PC Card

1 Insert the PC Card containing the software into the A: drive of the IP trunk card, located on the faceplate of the IP trunk card.

2 From the ITG shell, monitor the successful insertion of the PC Card. If the PC Card has been successfully recognized and installed, a message indicating this is displayed.

3 Use the **swDownload** command to copy the software from the PC Card to the IP trunk card flash ROM device, using the FTP client and the FTP host on the IP trunk card. The host name parameter in this command is the ELAN network interface IP address of the IP trunk card. The user name and password are the same as those configured for the ITG shell. The directory path, which is "/A:", and file name indicate the software file on the PC Card in the A: drive.

4 Press **Enter**. Monitor the status of the software upgrade and check that the upgrade correctly finishes. Observe any error messages that indicate problems with parameters or syntax.

5 When the new software has downloaded into the flash ROM device, reboot the IP trunk card to use it. Use the **cardReset** command or press the reset button on the IP trunk card faceplate.

End of Procedure

Upgrade IP trunk card software through an FTP host

Follow the steps in Procedure 66 to upgrade the IP trunk card software through an FTP host.

Procedure 66
Upgrading IP trunk card software through an FTP host

1. Make the latest IP trunk card software, obtained from the Nortel web page, available to an FTP host. This can be an FTP host on the PC. As a special case, the FTP host can be the IP trunk card.

   Alternatively, use an FTP client running on the PC to copy the IP trunk card software file to an IP Trunk 3.01 (and later) host on the network that is available to the IP trunk card.

   For example, any IP trunk card on the same IP Trunk 3.01 (and later) node can serve as the FTP host. The file can be copied onto the C: drive of the IP trunk card serving as the FTP host.

2. Use the **swDownload** command to copy the software from the PC Card to the IP trunk card flash ROM device, using the FTP client and the FTP host on the card. The host name parameter in this command is the IP address of the FTP host, which can be local or remote to the IP trunk card. The user name and password are the user name and password of the FTP host. The directory path and file name are the directory path and file name on the FTP host. As a special case, the FTP host can be the IP trunk card and the directory path is "/C:".

3. Press **Enter**. Monitor the status of the software upgrade and check that the upgrade correctly finishes. Observe any error messages that indicate problems with parameters or syntax.

4. When the new software has downloaded into the flash ROM device, reboot the IP trunk card to use it. Use the **cardReset** command or press the reset button on the IP trunk card faceplate.

End of Procedure

Backup and restore from the CLI

Use Procedure 67 and Procedure 68 to backup and restore when the preferred method, using the OTM PC, is not available. This whole procedure must be performed when a configuration file has been changed.

First, use the 'Put' commands to back up the IP trunk card configuration files. Restore the files later using the "Get" commands.

However, the "DPAddrTGet" file can be used to restore the dialing plan file from another IP trunk card in the same node.

Backup from the CLI

Follow the steps in Procedure 67 to perform a backup from the CLI.

Procedure 67
Backing up from the CLI

1. Identify an appropriate FTP host and obtain the IP address, the user name, the password, and a directory path on the host.
2. Log in to the ITG shell of the Leader 0 IP trunk card of the IP Trunk 3.01 (and later) node.
3. Use the **BootPFilePut** command with the appropriate parameters, to backup the Node Properties file to the FTP host.
4. Use the **DPAddrPut** command with the appropriate parameters, to backup the dialing plan file to the FTP host.
5. For each IP trunk card, log in to the ITG shell and use the **configFilePut** command to backup the card properties files. Each file must be named to identify the card it goes with.

End of Procedure

Restore from the CLI

To restore configuration when the OTM PC is not available to retransmit the IP Trunk 3.01 (and later) configuration data, use the appropriate "Put" commands.

Follow the steps in Procedure 68 to perform a restore from the CLI.

Procedure 68
Restoring from the CLI

1 Use the **BootPFileGet** command with the appropriate parameters, to restore the Node Properties file from the FTP host to the IP trunk card.

2 Log in to the ITG shell for each IP trunk card that requires a dialing plan restore. Use the **DPAddrPut** command with the appropriate parameters, to backup the dialing plan file from the FTP host, or from another IP trunk card in the node that has a valid copy of the dialing plan, to each IP trunk card. Each IP trunk card requires a valid copy of the dialing plan.

3 Log in to the ITG shell for each IP trunk card that requires a Card Properties restore and use the **configFilePut** command with the appropriate parameters, to restore the IP trunk card properties files.

End of Procedure

Recover the SNMP community names

It might be necessary to recover the SNMP community names in the following situations:

- when OTM 2.1 (and later) cannot display the updated status
- to transmit or retrieve data to or from an IP trunk card because of an invalid community name in OTM IP Trunk 3.01 (and later)
- if the OTM PC has crashed and had to be restored from scratch.

The SNMP community names can be read from the IP trunk card in two ways:

- Reset the IP trunk card and monitor the startup messages. Use the **configFilePut** command to backup the Card Properties file to an FTP host. Use a text editor to open the Card Properties file and read the community name.
- Alternatively, use the SNMP client on the OTM PC to connect to the FTP host on the IP trunk card. Log in using the ITG shell user name and password. Get the Card Properties file from the path, which is **/C:/Config/CONFIG1.INI**. Use a text editor to open the Card Properties file and read the community name.

IP Trunk 3.01 (and later) configuration commands

Table 52 lists the IP Trunk 3.01 (and later) configuration commands.

Table 52
IP Trunk 3.01 (and later) configuration commands

Command	Description
setLeader	The one command that performs all the necessary actions to make a Leader. Sets the IP address, gateway, subnet mask, boot method to static, and leader bit in NVRAM.
clearLeader	Enter this command to clear the Leader information in NVRAM and set the boot method to use BOOTP, making the card a Follower.
NVRIPShow	Enter this command to print the values of the IP parameters that exist in NVRAM.

Download the IP Trunk 3.01 (and later) error log

The IP Trunk 3.01 (and later) error log contains error conditions and normal events. Some of the error conditions can be severe enough to raise an alarm through SNMP traps.

The following commands can download an IP Trunk 3.01 (and later) error log:

- **currLogFilePut**
- **prevLogFilePut**

System commands – LD 32

Perform the following system administration commands using LD 32:

- "Disable the indicated IP trunk card" on page 512.

Note 1: Disable the IP trunk card before card properties are transmitted from the OTM IP Trunk 3.01 (and later) application to the IP trunk card.

Note 2: The card reset button is only available in the OTM IP Trunk 3.01 (and later) application when the IP trunk card is disabled.

Note 3: Disabling the IP trunk card in LD 32 does not disable the Active Leader or Backup Leader functions.

- "Disable the indicated IP trunk card when idle" on page 512.

  Note: This temporarily prevents the IP Trunk 3.01 (and later) node from seizing the port from incoming calls.

- "Disable an indicated IP trunk card port" on page 512.
- "Enable an indicated IP trunk card" on page 512.
- "Enable an indicated IP trunk card port" on page 513.
- "Display IP trunk card ID information" on page 513.

  Note 1: This command displays the PEC (Product Engineering Code) for the card. The PEC is as follows:
  ITG 8-port trunk card – NT0961AA
  ITG-Pentium 24-port trunk card – NT0966AA
  Media Card 32-port trunk card – NT0966BA

  Note 2: The IP trunk card ID information displays the same IP trunk card serial number that is displayed from the ITG shell using **serialNumShow**.

- "Display IP trunk card status" on page 513.
- "Display IP trunk card port status" on page 513.

Table 53 shows a summary of the system administration commands available in LD 32.

Table 53
LD 32 – IP Trunk 3.01 (and later) maintenance commands

Command	Function
DISC l s c	Disable the indicated card, where: l = loop, s = shelf, c = card
DISI l s c	Disable the indicated card when idle, where: l = loop, s = shelf, c = card ***Note:*** Use the DISI command to disable the IP trunk card instead of the DISC command. The disablement of the IP trunk card is indicated by the NPR011 message.
DISU l s c u	Disable the indicated unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the described IP trunk card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the described unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the described IP trunk card, where: l = loop, s = shelf, c = card
STAT l s c	Print the system software status of the indicated IP trunk card where: l = loop, s = shelf, c = card
STAT l s c u	Print the system software status of the indicated unit, where: l = loop, s = shelf, c = card, u = unit

Disable the indicated IP trunk card

To disable the indicated IP trunk card in LD 32, use the following command:

DISC l s c	Disable the indicated IP trunk card, where: l = loop, s = shelf, c = card

Disable the indicated IP trunk card when idle

To disable the indicated IP trunk card when idle in LD 32, use the following command:

DISI l s c	Disable the indicated IP trunk card when idle, where: l = loop, s = shelf, c = card

Enable an indicated IP trunk card

To enable an indicated IP trunk card in LD 32, use the following command:

ENLC l s c	Enable the indicated IP trunk card, where: l = loop, s = shelf, c = card

Disable an indicated IP trunk card port

To disable an indicated IP trunk card port in LD 32, use the following command:

DISU l s c u	Disable the indicated IP Trunk 3.01 (and later) unit (port), where:
	l = loop, s = shelf,
	c = card, u = unit

Enable an indicated IP trunk card port

To enable an indicated IP trunk card port in LD 32, use the following command:

ENLU l s c u	Enable the indicated IP Trunk 3.01 (and later) unit (port), where: l = loop, s = shelf, c = card

Display IP trunk card ID information

To display the IP trunk card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the card, where:
	l = loop, s = shelf,
	c = card

Display IP trunk card status

To display the status of an indicated IP trunk card in LD 32, use the following command:

STAT l s c	Display the status of the indicated IP trunk card, where: l = loop, s = shelf, c = card

Display IP trunk card port status

To display the status of a port on the IP trunk card in LD 32, use the following command:

STAT l s c u	Display the status of the indicated IP Trunk 3.01 (and later) port, where: l = loop, s = shelf, c = card, u = unit.

Maintenance

Contents

This section contains information on the following topics:

Introduction

This chapter describes the maintenance, debug, and software upgrade procedures available for the IP trunk cards.

This chapter includes the following sections:

- **ITG-Pentium 24-port trunk card faceplate maintenance display codes** – a list of the Maintenance codes on the diagnostic status of the ITG-Pentium 24-port trunk card.
- **Media Card 32-port trunk card faceplate maintenance display codes** – a list of the Maintenance codes on the diagnostic status of the Media Card 32-port trunk card.
- **System level maintenance** – how to maintain the IP trunk card using overlays, or an OTM 2.1 (and later) PC.
- **ITG shell command set** – how to maintain the IP trunk card using the IP trunk card's CLI.

- **Diagnostics** – how to perform diagnostic tests on the IP trunk card to check correct operation.
- **IP Trunk 3.01 (and later) upgrades** – the different upgrade options available for IP Trunk 3.01 (and later).
- **Replacement** – step-by-step procedures to replace an IP trunk card.
- **Backup and restore procedures** – how to backup the IP Trunk 3.01 (and later) application data.
- **Fault clearance procedures** – potential system faults and how to correct them.

IP Trunk 3.01 (and later) IP trunk card alarms

This section describes the alarms, messages and codes output by the ITG-Pentium 24-port and Media Card 32-port trunk cards. All IP Trunk 3.01 (and later) IP trunk card alarms shown in Table 54 on page 518 can be emitted as SNMP traps. SNMP is the method IP Trunk 3.01 (and later) uses to send alarms to an alarm monitoring center.

IP Trunk 3.01 (and later) displays and logs alarm information in the following ways:

- Displayed on the IP trunk card console through the ITG shell in a Telnet session or on a terminal connected to the local maintenance port.
- Logged in the error log files on the /C: drive of the IP trunk card.
- Events of the type “ITG4xx” (that is, major alarms – immediate intervention required) are displayed on the faceplate maintenance display. They appear in the form “I:4xx”, where “4xx” corresponds to last three digits of the alarm ITG04xx listed in Table 54 on page 518.
- Access the current error log file through OTM IP Trunk 3.01 (and later) IP trunk card properties by clicking the **Open Log File** button on the **Maintenance** tab of IP trunk card properties.

If enabled in the OTM ITG Node Properties **SNMP Trap/Routing table IPs** tab, SNMP sends appropriate traps to OTM Alarm Management or another specific SNMP manager when an error or event occurs. The IP trunk card also puts the system error message in the error log file on the /C: drive of the IP trunk card. View the log file with any text browser after uploading it to an

FTP host. To upload the log file to an FTP host, enter: "**currLogFilePut**" or "**prevLogFilePut**" from the ITG shell.The IP trunk card generates SNMP alarm traps for the following four alarm categories:

- **Alarm Clearance** (ITG01xx) – for information purposes
- **Minor Alarm** (ITG02xx) – no intervention required
- **Major Alarm** (ITG03xx) – intervention required, but not immediately
- **Major Alarm** (ITG04xx) – immediate action required. Card is out of service

Up to eight destination IP addresses can be configured to which these alarms can be sent. The same addresses must be configured for all cards on the same node. Table 54 lists SNMP alarms by severity.

Table 54
IP Trunk 3.01 (and later) alarms (Part 1 of 7)

Alarm	Description	Fault Clearing Action
Alarm Clearance – For information purposes These alarms indicate the clearance of an error condition. As such, no user intervention is required. A number of these alarms indicate the clearance of a major alarm shown later in this table.		
ITG0100	Successful bootup. All alarms cleared.	If this happens due to something other than a known power-on event or a user-invoked card reset, the causes of recurring bootup must be investigated. Contact Nortel technical support.
ITG0101	Exit from QoS fallback. Normal operation restored.	Indicates recovery from ITG0203. Recurrent QoS fallback and recovery can indicate network faults, far-end IP Trunk 3.01 (and later) node failure or network QoS configuration errors.
ITG0102	Ethernet voice port restored to normal operation.	Indicates recovery from ITG0402.

Table 54
IP Trunk 3.01 (and later) alarms (Part 2 of 7)

Alarm	Description	Fault Clearing Action
ITG0103	ELAN network interface restored to normal operation.	Indicates recovery from ITG0403.
ITG0104	DSP successfully reset.	Indicates recovery from ITG0204.
ITG0105	Exit from card fallback. Leader card restored.	
ITG0150	D-channel (Link Layer) restored. Channels returned to service.	Indicates recovery from ITG0450.
Minor Alarms – No intervention required These alarms indicate transient events that do not require technician intervention. Recurring minor alarms indicate potential IP Trunk 3.01 (and later) node engineering issues that require analysis by a technician.		
ITG0200	TLAN network interface buffer exceeded. Packet(s) discarded.	Indicates TLAN network interface hardware problems or excessive TLAN subnet traffic.
ITG0201	ELAN network interface buffer exceeded. Packet(s) discarded.	Indicates ELAN network interface hardware problems or excessive ELAN subnet traffic.
ITG0202	Card recovered from software reboot.	
ITG0203	Fallback to PSTN activated. Bad network condition. This alarm indicates a QoS fallback.	Recurrent QoS fallback and recovery can indicate network faults, far-end IP Trunk 3.01 (and later) node failure or network QoS configuration errors.
ITG0204	DSP device reset. A DSP failed to respond and was reset.	If this alarm occurs repeatedly on the same DSP, replace the card. See “Replace an IP trunk card” on page 551.

Table 54
IP Trunk 3.01 (and later) alarms (Part 3 of 7)

Alarm	Description	Fault Clearing Action

ITG0206	Invalid A07 message received. Message discarded. A07 is a message signaling interface between Meridian 1 and the IP trunk card.	Verify that the card type is correctly configured in the system. Print TNB in LD 20. Ensure that the card is configured as a TIE Trunk with:
		XTRK = ITG1 (for SMC 32-port)
		XTRK=ITG2 (for ITG-Pentium 24-port)

ITG0207	Unknown H.323 message received. Message discarded.	Indicates unsupported H.323 gateway is misconfigured to send messages to IP Trunk 3.01 (and later). Locate address that is sending unsupported messages.
ITG0208	Backup Leader has been activated. Leader card not responding.	Investigate why Active Leader failed. Either Leader 0 or Leader 1 can perform the Active Leader or Backup Leader role.
ITG220	Upgrading with old software version (unknown processor type).	

ITG0250	Invalid X12 message received. Message discarded.	Verify that the card type is correctly configured in the system. Print TNB in LD 20. Ensure that the card is configured as a TIE Trunk with:
		XTRK = ITG1 (SMC 32-port)
		XTRK = ITG2 (ITG-Pentium 24-port)

Major Alarms – Intervention required, but not immediately This fault class can result in a trap that automatically resets a processor on the card and clears the fault after a service interruption of several seconds or minutes. The talk path is cut off for existing calls and no new calls can be made on the card until it finishes resetting. If the problem occurs frequently the IP trunk card requires manual intervention; for example, upgrade to an enhanced software version or replace the IP trunk card.		
ITG0300	Memory allocation failure. Check configuration. Indicates a dynamic memory allocation problem.	If this occurs frequently, contact Nortel technical support.

Table 54
IP Trunk 3.01 (and later) alarms (Part 4 of 7)

Alarm	Description	Fault Clearing Action
ITG0301	DSP channel not responding. DSP channel is disabled. Card sends message to the system to busy the trunk. This ensures that user's calls go through on good DSPs.	These DSP errors are not cleared automatically. If the occurs frequently, replace the card.
ITG0302	DSP device failure. Operating on reduced capacity. DSP failed to return to normal service.	Hardware fault cleared by automatic trap.
ITG0303	DSP subsystem failure. Initiating card reboot. DSP fatal error detected.	Hardware fault cleared by automatic trap.
ITG0304	Cannot write to file. I/O error.	Can indicate /C: drive corruption.
ITG0305	Cannot open configuration file. Using default settings. Can occur after a reboot.	
ITG0306	System messaging error threshold exceeded. Too many invalid A07 or X12 messages.	
ITG0308	Address translation failure. Call is released.	
ITG0309	Unexpected DSP channel closed. Channel is unusable.	
ITG0310	Cannot open DSP channel.	
ITG0311	Unable to get response from Follower card. Card can be unplugged.	
ITG0312	Unable to push BOOTP tab file to Backup Leader.	

Table 54
IP Trunk 3.01 (and later) alarms (Part 5 of 7)

Alarm	Description	Fault Clearing Action
ITG0350	Gatekeeper RAS reject threshold exceeded.	
ITG0351	Cannot open Gatekeeper configuration file. Using default settings.	
Major Alarms – Immediate intervention required These alarms indicate an irrecoverable failure of the IP trunk card. Normal operation can only be restored through manual intervention.		
ITG0400	Fatal self-test failure. Card is out of service. A fatal self-test diagnostic error was found.	
ITG0401	Reboot threshold exceeded. Manual intervention required.	
ITG0402	Ethernet voice port failure. TLAN subnet problem or cable removed.	
ITG0403	ELAN network interface failure. ELAN subnet problem or cable removed.	
ITG0404	Cannot open address translation file. File does not exist or is corrupted.	
ITG0406	Startup memory allocation failure. Card reboot initiated. Indicates insufficient memory installed.	
ITG0407	Cannot get response from Leader card.	
ITG0408	Bad address translation file. Reverting to previous version (if any).	

Table 54
IP Trunk 3.01 (and later) alarms (Part 6 of 7)

Alarm	Description	Fault Clearing Action
ITG0409	Bad configuration file. Reverting to previous version (if any).	
ITG0410	Remote leader not responding. May have incorrect IP address or can be a network error.	
ITG0411	Failed to start UDP server for intercard messaging. Cannot open a socket.	
ITG0412	Failed to start UDP client for intercard messaging. Cannot open a socket.	
ITG0413	Failed to register with Leader card. Defaulting to fallback mode. Leader/Backup Leader can be unplugged or there can be a network error.	
ITG0414	No response from Leader card.	
ITG0415	Task spawn failed. Attempting a reboot.	
ITG0416	Failed to start QoS/Network Probing Timer.	
ITG0417	Failed to send fallback update to Followers.	
ITG0418	H.323 stack failed to initialize.	
ITG0430	Software image not compatible with Target processor. Software upgrade aborted.	

Table 54
IP Trunk 3.01 (and later) alarms (Part 7 of 7)

Alarm	Description	Fault Clearing Action
ITG0450	D-channel loss of signal. Associated channels busied out.	
ITG0451	D-channel hardware failure. Associated channels busied out.	
ITG0452	System messaging failure. Unable to process calls.	
ITG0453	Cannot open Gateway DN file	
ITG0454	Cannot open Gatekeeper password file.	
ITG0455	Bad Gatekeeper configuration file. Reverting to previous version, if any.	
ITG0456	Incorrect gateway password. Calls to/from gateway rejected by the Gatekeeper.	

System level maintenance

Maintenance of an IP trunk card can be performed using the following:

- overlays
- OTM 2.1 (and later) PC
- the CLI of the IP trunk card

Access the IP trunk card

The IP trunk card can be accessed in two ways: by Telnet and through a physical connection to the serial port.

Telnet access

Connect to the IP trunk card using Telnet. This provides access to the ITG shell. A Telnet session has higher priority than a serial session. A Telnet session started during an ongoing serial session disables the serial connection for the period of the Telnet session. The serial session continues when the Telnet session ends.

Serial access

Connect to the IP trunk card by physically connecting to the serial port. This provides access to the ITG shell. If there is an active Telnet session ongoing while the serial connection is established, the serial connection will not be active as Telnet access has priority. The Telnet session must be terminated in order for the serial connection to become active.

IP trunk card LD commands

System level maintenance of the IP trunk card is performed using LD 32 or LD 36. See Table 55 and Table 56 on page 526.

Table 55
Supported LD 32 commands (Part 1 of 2)

Command	Function
DISC l s c	Disable the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
DISI l s c	Disable the indicated IP trunk card when idle, where: l = loop, s = shelf, and c = card.
DISU l s c u	Disable the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.
ENLC l s c	Enable the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
ENLU l s c u	Enable the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.

Table 55
Supported LD 32 commands (Part 2 of 2)

Command	Function
IDC l s c	Print the Card ID information for the specific IP trunk card, where: l = loop, s = shelf, and c = card.
STAT l s c	Print the system software status of the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
STAT l s c u	Print the system software status of the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.
Note 1: For Meridian 1 PBX 11C Cabinet, Meridian 1 PBX 11C Chassis, CS 1000M Cabinet, and CS 1000M Chassis, the TN address < l s c > should be replaced by < s c > and the < l s c u > address replaced by < s c u >.	

Table 56
Supported LD 36 commands (Part 1 of 2)

Command	Function
DISC l s c	Disable the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
DISU l s c u	Disable the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.
ENLC l s c	Enable the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
ENLU l s c u	Enable the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.
LDIC l s c u	List the number of days since the last incoming call on the indicated trunk, where: l = loop, s = shelf, c = card, and u = unit.

Table 56
Supported LD 36 commands (Part 2 of 2)

Command	Function
STAT l s c	Print the system software status of the indicated IP trunk card, where: l = loop, s = shelf, and c = card.
RSET l s c u	Reset thresholds for the indicated trunk, where: l = loop, s = shelf, c = card, and u = unit.
Note 1: For Meridian 1 PBX 11C Cabinet, Meridian 1 PBX 11C Chassis, CS 1000M Cabinet, and CS 1000M Chassis, the TN address < l s c > should be replaced by < s c > and the < l s c u > address replaced by < s c u >.	

Information equivalent to that provided by the **STAT** command can be accessed from the command line on the card.

Identify IP Trunk 3.01 (and later) trunk routes and IP trunk cards in the system

In LD 16, the Route Data Block, use the “DES” prompt to identify the IP Telephony Gateway route.

IP trunk card ELAN network interface MAC address and IP address

In LD 14, use the “DES” prompt to identify the ELAN network interface MAC address and IP address.

Print the IP Trunk 3.01 (and later) trunk route and trunk designators

In LD 21, enter the “LTM” (List Trunk Members) in response to the “REQ” prompt to list the IP Trunk 3.01 (and later) route designator’s and the individual IP Trunk 3.01 (and later) trunk designators’ MAC addresses and IP addresses. When cards are added, deleted, or changed, the trunk designators must be updated.

OTM 2.1 (and later) maintenance commands

When changing DSP parameters in OTM 2.1 (and later), disable the IP trunk card's ports before downloading the new parameters. Modifications to node parameters require the affected cards to be rebooted. A dialing plan can be modified without rebooting or disabling the cards.

Multi-purpose Serial Data Link (MSDL) commands

All system MSDL commands are supported. Use LD 96 to enter MSDL commands. Table 57 lists some of the more important commands.

Table 57
MSDL commands

Command	Description
ENL DCH num	Enables the D-channel.
DIS DCH num	Disables the D-channel.
STAT DCH num	Displays the state of the D-channel application.
RLS DCH num	Releases the D-channel.
EST DCH num	Establishes multiple frame operation on the D-channel.

Simple Network Management Protocol (SNMP)

An SNMP stack sends appropriate traps to OTM 2.1 (and later) or an SNMP manager. A buffer containing received traps is also available through the CLI if no SNMP/Alarm Manager exists.

Error traps

Table 58 shows the error events that cause the SNMP agent to issue a trap.

Table 58
Error events

Event	Description
Loss of Voice Port connectivity	Failure in the Ethernet voice port.
QoS Minor Threshold Exceeded	The QoS minor alarm threshold has been exceeded.
dspResetAttempted	One of the DSP devices has failed and an attempt has been made to reset it.
dspResetFailed	An attempt to reset a DSP has failed. The channels associated with that DSP are unusable.
Leader Not Responding	The Leader card is not responding.
DCHIP Not Responding	A DCHIP card is not responding.
C7 PC Card Failed	The PC Card Device Driver detected that the C7 PC Card has failed. The D-channel link is released.

Other traps

Table 59 shows other events that cause the SNMP agent to issue a trap.

Table 59
SNMP trap causing events (Part 1 of 2)

Command	Function
Card Disabled	The card has been disabled by the system.
Card Enabled	The card has been enabled by the system.
Channel Enabled	A given channel has been enabled by the system.
D-channel Released	The D-channel link has been released.

Table 59
SNMP trap causing events (Part 2 of 2)

Command	Function
Alternate Routing	QoS prevents calls from being completed. Cause value “Temporary failure” is sent to the system for Fallback to PSTN.
Normal Service Restored	Network performance is confirmed as acceptable and IP telephony has been restarted.

TRACE and ALARM/LOG

Call Tracing (TRACE File Command)

This command interfaces with all modules to create an efficient TRACE File. It is a monitor that stores and keeps track of information about events. For all error conditions, a clear log of all actions is available. The TRACE File does not solve these errors; it only indicates that there were errors and shows where the errors originated. The TRACE File asks each module to report all events and records the errors in order in a complete event log. Each event is marked with a severity indicator.

LOG File

All hardware alarms, normal log messages, and severe events are logged in a single LOG file.

ITG shell command set

ITG shell commands are designed to supplement overlay commands and to introduce new features specific to IP Trunk 3.01 (and later).

To access ITG shell commands, connect an OTM PC or a TTY to the RS-232 Maintenance port on the IP trunk card faceplate. Alternatively, connect the OTM PC or a TTY to the Serial I/O Panel port to create a more permanent connection to the IP trunk card maintenance port.

CAUTION

Never connect to the front and back serial ports at the same time.

Note: All ITG shell commands are case-sensitive.

Commands are grouped into eight categories, as shown in Tables 60 – 65.

Table 60
General purpose commands (Part 1 of 4)

Command	Description
cardReset	Perform a warm reboot of the IP trunk card. The card has to be in the OOS state to use this command.
itgCardShow	Show card information.
ldrResTableShow	Show Backup Leader and Followers for a given Leader.
itgChanStateShow	Show state of channels (for example, busy or idle).
h323SessionShow	Show H.323 session information for each channel.
itgMemShow	Show memory usage.
ifShow	Show detailed network interface information, including MAC and IP addresses.

Table 60
General purpose commands (Part 2 of 4)

Command	Description
IPInfoShow	This command will return the following IP information: • IP addresses (for both ELAN and TLAN network interfaces) • default router (for both ELAN and TLAN network interfaces) • subnet masks (for both ELAN and TLAN network interfaces) • SNMP manager
cardStateShow	IP trunk card state (that is Unequipped, Disabled, Enabled).
serialNumShow	Print out IP trunk card serial number and PEC. This command displays the same IP trunk card serial number that is displayed from the system IDC command, and the Product Engineering Code (PEC).
firmwareVersionShow	Print out firmware version number.
numChannelsShow	Print out number of available channels.
numNodesInFallbackShow	List the IP addresses of the IP Trunk 3.01 (and later) nodes that are in fallback to the conventional voice circuit-switched network.
swVersionShow	Print out software version.
resetOm	Reset the Operational Measurement file timer.
logFileOn	Turn on logging.
logFileOff	Turn off logging.
logFileShow	Show if logging is on or off.
logStatus	Show if logging is on or off.
useM1ForRingBack	This command is used to turn off the local ring back generated on the IP Trunk card. By default, the IP Trunk card will generate local ring back for out of band ring back. This command will only be in effect until the card is reset.

Table 60
General purpose commands (Part 3 of 4)

Command	Description
displayClear	Clear the maintenance display on the faceplate of the IP trunk card.
shellPasswordSet	Change the default ITG shell password.
emodelSim	Allow user to interactively determine QoS score.
itgHelp	Show the complete command list. "?" also shows the list.
itgCallTrace	Shows call trace log.
tLanSpeedSet	Set the speed of the TLAN network interface.
tLANDuplexSet	Set the duplex mode of the TLAN network interface.
logout	Exit the shell.
PING	Test remote host is reachable: PING<host><numPackets><option> This command sends an ICMP ECHO_REQUEST packets to a network host. The host matching the destination address in the packets responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or IP trunk cards are properly communicating with the sender card. The <numPackets> parameter specifies how many packets to send; if it is not included, ping runs until it is stopped by Ctrl-C (which also exits the ITG shell). Example: ITG> PING "47.82.33.123", 10
trap_gen	SNMP test alarm (one of each type) generation.
clearLED	Clear the LED display.
esn5PrefixSet	Set the esn5Prefix, default is "100":esn5Prefix<"char string">
esn5PrefixShow	Display the esn5Prefix character string.

Table 60
General purpose commands (Part 4 of 4)

Command	Description
routeAdd “host/ network IP address”, “IP Gateway”	This command adds a route to the network routing table. The route is added to the host portion of the routing table. Example: ITG> routeAdd “47.82.33.123”, “47.82.33.1”
mRouteAdd “host/ network IP address”, “IP Gateway”, “Subnet mask”, “ToS value”, “flags”	This command adds multiple routes to the same destination in the routing table. The route is added to the network portion of the routing table. Multiple route entries for a single destination are possible if entered with this command, as the ToS and subnet mask values are used to distinguish between them. Currently, “flags” should be set to “0”. Example: ITG>mRouteAdd “47.82.33.123”, “47.82.33.1”, “255.255.255.0”, 4, 0
routeDelete “IP address”, “IP Gateway”	Delete a route from the routing table. Example: ITG> routeDelete “47.23.34.19”, “47.23.34.1”
mRouteDelete “IP address”, “Subnet mask”, <ToS value>, <flags>	Delete a route matching the ToS value and flags. Currently, “flags” should be set to “0”. Example: ITG> mRouteDelete “47.23.34.19”, “255.255.255.0”, 4, 0
routeShow	Display the current host and network routing entries. Example: ITG> routeShow

Table 61
File transfer commands (Part 1 of 3)

Command	Description
swDownload hostname, username, password, directory path, filename	Update the software on the IP trunk card with the binary file received from an FTP server corresponding to the *hostname* IP address. The IP trunk card FTP client performs a get which downloads the file to the flash bank. A checksum is calculated to check correct delivery. Once the new software version is successfully downloaded, the IP trunk card must be rebooted with cardReset in order to run the new software. *Hostname* refers to either the IP address of the FTP host, or the IP trunk card itself or another IP trunk card when a PC Card in the A: drive of the IP trunk card contains the software binary file.
Example:	ITG> swDownload “47.82.32.246”, “anonymous”, “guest”, “/software”, “vxWorks.mms”
DPTableGet hostname, username, password, directory path, filename	Update the address table on the IP trunk card with the address table file on the indicated host, account, and path. The host starts an FTP session with the given parameters and downloads the file to the flash file system.
Example:	ITG> DPTableGet “ngals042”, “anonymous”, “guest”, “/dialPlan”, “dialingPlan.txt”
configFileGet hostname, username, password, directory path, filename	Update the config.ini file on the IP trunk card with the config.ini file on the indicated host, account, and path. The configFileGet task on the host starts an FTP session with the given parameters and downloads the file to the flash file system.
Example:	ITG> ConfigFileGet “ngals042”, “anonymous”, “guest”, “/configDir”, “config.ini”
bootPFileGet hostname, username, password, directory path, filename	Update the bootptab file on the IP trunk card with the bootptab file on the indicated host, account, and path. The bootpFileGet task on the host starts an FTP session with the given parameters and downloads the file to the flash file system.

Table 61
File transfer commands (Part 2 of 3)

Command	Description
Example:	ITG> bootpFileGet “ngals042”, “anonymous”, “guest”, “/bootpDir”, “bootptab”
SNMPConfFileGet hostname, username, password, directory path, filename	Update the SNMP configuration file on the IP trunk card with the SNMP configuration file on the indicated host, account and path. The SNMPConfFileGet task on the host starts an FTP session with the given parameters and downloads the file to flash file system.
Example:	ITG> SNMPConfFileGet “ngals042”, “anonymous”, “guest”, “/snmpDir”, “agent.cnf”
hostFileGet hostname, username, password, directory path, filename, ITGFileName, listener	Get any file from the host and does a **get** through FTP to the IP trunk card. ***Note:*** ITGFileName is the full path and filename of where the file is to be placed. The listener parameter indicates which module to inform of the successful file transfer. It can be set to -1 to be disabled.
Example:	ITG> hostFileGet “ngals042”, “anonymous”, “guest”, “/hostfileDir”, “hostFile.txt”, “/C:ITGFILEDIR/ITGFILE.TXT”, -1
currOmFilePut hostname, username, password, directory path, filename	The omFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card’s current Operational Measurements file to the indicated location on the host.
Example:	ITG> currOmFilePut “ngals042”, “anonymous”, “guest”, “/currDir”, “omFile”
prevOmFilePut hostname, username, password, directory path, filename	The omFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card’s previous Operational Measurements file to the indicated location on the host.
Example:	ITG> prevOmFilePut “ngals042”, “anonymous”, “guest”, “/prevDir”, “omFile”

Table 61
File transfer commands (Part 3 of 3)

Command	Description
traceFilePut hostname, username, password, directory path, filename	The traceFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card's call trace file to the indicated location on the host.
Example:	ITG> traceFilePut "ngals042", "anonymous", "guest", "/trcDir", "trcFile"
currLogFilePut hostname, username, password, directory path, filename	The logFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card's current log file to the indicated location on the host.
Example:	ITG> currLogFilePut "ngals042", "anonymous", "guest", "/currDir", "logFile"
prevLogFilePut hostname, username, password, directory path, filename	The logFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card's previous log file to the indicated location on the host.
Example:	ITG> prevLogFilePut "ngals042", "anonymous", "guest", "/currDir", "logFile"
bootPFilePut hostname, username, password, directory path, filename	The bootpFilePut task on the host starts an FTP session with the given parameters and downloads the IP trunk card's BOOTP file to the indicated location on the host.
Example:	ITG> bootpFilePut "ngals042", "anonymous", "guest", "/bootpDir", "bootpFile"
hostFilePut hostname, username, password, directory path, filename, ITGFileName	Transfer any file on the IP trunk card from location ITGFileName and does a put using FTP to the host indicated by hostname, username, password, and directory path. ***Note:*** ITGFileName is the full path (that is, path/filename of where the file is taken from on the IP trunk card).
Example:	ITG> hostFilePut "ngals042", "anonymous", "guest", "/hostDir", "hostFile", "/C:/CONFIG/CONFIG1.INI"

Table 62
NVRAM IP configuration commands

Command	Description
NVRIPSet IP address *Example:*	Set the IP address in NVRAM. ITG> NVRRIPSet “47.23.34.19”
NVRGWSet IP gateway *Example:*	Set the default gateway address in NVRAM. ITG> NVRRGWSet “47.0.0.1”
NVRSMSet subnet mask *Example:*	Set the subnet mask in NVRAM. ITG> NVRRSMSet “255.255.240.0”
NVRIPShow *Example:*	Print the values of the IP parameters that exist in NVRAM. ITG> NVRIPShow
nvramLeaderSet *Example:*	Set the leader bit in NVRAM. ITG> nvramLeaderSet
nvramLeaderClr *Example:*	Clear the leader bit in NVRAM, but does not erase the IP parameters in NVRAM. ITG> nvramLeaderClr
NVRClear *Example:*	Clear IP parameters in NVRAM. ITG> NVRClear
setLeader IP address, IP gateway, subnet mask *Example:*	The one command that does all the necessary actions to make a Leader. Sets IP address, gateway, subnet mask, boot method to static, and Leader bit in NVRAM. ITG> setLeader “47.23.45.67”, “47.0.0.1”, “255.255.240.0”
clearLeader *Example:*	The one command that does all the necessary actions to clear the Leader information in NVRAM and set the boot method to use BOOTP, thus, making the card a Follower. ITG> clearLeader

Table 63
DSP commands

Command	**Description**
DSPReset DSP Number *Example:*	Reset the indicated DSP. ITG>DSPReset 0
DSPSelfTest DSP Number *Example:*	Run self-test on the DSP. ITG>DSPSelfTest 0
DSPNumShow *Example:*	Print number of DSPs on IP trunk card. ITG>DSPNumShow
DSPPcmLpbkTestOn	Start PCM loopback test on the indicated DSP.
Example:	ITG>DSPPcmLpbkTestOn
DSPPcmLpbkTestOff *Example:*	Stop PCM loopback test on the indicated DSP. ITG> DSPPcmLpbkTestOff
DSPSndLpbkTestOn *Example:*	Start Send loopback test on the indicated DSP. ITG> DSPSndLpbkTestOn
DSPSndLpbkTestOff *Example:*	Stop Send loopback test on the indicated DSP. ITG> DSPSndLpbkTestOff
DSPRcvLpbkTestOn *Example:*	Start Receive loopback test on the indicated DSP. ITG> DSPRcvLpbkTestOn
DSPRcvLpbkTestOff *Example:*	Stop Receive loopback test on the indicated DSP. ITG> DSPRcvLpbkTestOff

Table 64
Operational Measurement command

Command	Description
resetOM	This command returns all Operational Measurement parameters collected since last log dump, including: • outgoing calls tried • outgoing calls completed • incoming calls tried • total voice time • total fax time • outgoing packets discarded • incoming packets out–of–sequence • average packet delay • average packet loss • number of Fallback-to-PSTN calls

Table 65
DCHIP-only commands (Part 1 of 2)

Command	Description
DCHenable	Enable the DCH application on the card.
DCHdisable	Disable the DCH application on the card.
DCHestablish	Establish the DCH link when it is in release mode.
DCHrelease	Release the DCH link when it is in establish mode.
DCHstatus	Display the DCH application state.

Table 65
DCHIP-only commands (Part 2 of 2)

Command	Description
DCHmenu	This command allows the user to access the UIPC Debug Menu. Once in passthru mode, the user has to "exit" the Debug Menu, before issuing any other ITG Shell Commands.
dchipResTableShow	Available from ITG shell. Show the Followers associated with a DCHIP.

IP trunk card self-tests

During power-up, the IP trunk card performs diagnostic tests to check correct operation. Use the faceplate RS-232 port on the IP trunk card to monitor these tests. IP Trunk 3.01 (and later) sends messages indicating the completion of each phase of testing and any detected faults, to this port.

Additionally, the IP trunk card has a four-character LED dot matrix display on the faceplate for the purpose of providing status information during maintenance operations. At power-up and during diagnostic tests, this display provides a visual indication of the status of the self-test and an indication of the first failure detected. For more information about the available Maintenance codes on the Media Card 32-port trunk card, see "Media Card 32-port trunk card faceplate maintenance display codes" on page 560. For more information about the available Maintenance codes on the ITG-Pentium 24-port trunk card, see "ITG-Pentium 24-port trunk card faceplate maintenance display codes" on page 563.

The 8051XA controller takes control of one of the RS-232 ports and uses it to display the results of the power-up self-test and diagnostics on a maintenance terminal.

The initial tests performed include the following:

- 8051XA controller self-test, including ROM checksum, onboard RAM, and timer tests
- external data/program RAM and dual-port memory tests

Following the successful completion of these tests, the 8051XA controller attempts to bring up the processor by clearing the reset state and entering a timing loop in the anticipation of receiving a message from the processor. If this loop times out, it outputs an error to the RS-232 port. It attempts to bring up the processor two more times before indicating an unrecoverable card failure.

Similarly, if a message is received from the processor, indicating a failure of one or more of the circuit elements, up to two more resets are attempted. The IP trunk card then enters the unrecoverable failure state. This ensures that failures due to erratic power-up, or reset conditions, do not cause an unnecessary failure of the card. When the processor responds correctly, the 8051XA controller switches its serial port to provide Card LAN communication and connects the processor to the external RS-232 port.

Card LAN

The IP trunk card supports the backplane Card LAN interface for communicating self-test errors and allowing maintenance access, including resetting the card remotely.

BIOS self-test

The IP trunk card contains its own VxWorks-based BIOS. At power-up, the BIOS performs its own initial test of the hardware. These tests cover the processor, PCI chipset, cache (if installed), and DRAM memory. The results of the BIOS self-test are displayed on the RS-232 maintenance port.

Base code self-test

The IP trunk card base code performs the following tests:

- flash integrity test
- PGA read/write test
- PC Card controller test (also tests the PCI bus)
- timer and DMA tests
- DSP test

Field-Programmable Gate Array (FPGA) testing

Before communicating with the system, the 8051XA controller downloads FPGA data files and performs tests to check correct programming of the FPGA.

Outgoing calls attempted/completed mismatch

The difference between the attempted and completed outgoing call numbers should never be less than the sum of the QoS Fallback, Address Translation fallback, and Calls Rejected fallback (totaled as “Outgoing Fallback”). It may be more. A caller may release a call before the attempt reaches the far node, but since the originator released before the call could complete, it might not even be recorded as an attempt by the remote ITG card.

For example, a user dials a valid ESN AC1 and LOC, but an incorrect DN (with an incorrect last digit). As soon as the user dials the digit, he or she realizes the mistake and releases the call. The SETUP message has already gone to the ITG card, but the call is cleared before the H.323 SETUP message traversed the IP network, so no call reaches the destination. An outgoing attempt has been made and cleared, so no fallback occurred and no call attempt is recorded at the destination.

The main reasons for valid completed call mismatches are:

- Time of day that the statistics were last read and cleared may vary.

  This is the most common reason for mismatch. For example, although both ITG cards were read at 10:00, it is important to know if the clocks are synchronized, and when statistics were last cleared. A one-minute discrepancy could mean quite a few calls in the difference. Therefore, the first eight calls of one card may have already been counted for the other card. The statistics are more reliable when looked at over the day.

- “Messages in flight”

  This ranges from trivial to extreme. In the extreme case, if a CONNECT message is delayed several tenths of seconds (or even seconds) by traffic bursts, the snapshot may occur while the CONNECT message is still traversing the network. Therefore, one or more calls is still unaccounted for. In the trivial case, even in a lightly loaded network, it still takes finite time for messages to propagate. However, this is usually not a factor.

The main reason for attempted call mismatches are:

- The outgoing side records every SETUP message sent to it by the PBX. The incoming side records SETUP messages sent to the PBX by the ITG card. Every call that is cleared quickly or blocked by fallback skews the results.

IP Trunk 3.01 (and later) upgrades

Several different types of upgrades can be required for the IP Trunk 3.01 (and later); for example, a software upgrade for bug fix and/or the addition of new features. All upgrades are accomplished by updating the on-board application flash memory with the application. Software upgrades are performed from the OTM 2.1 (and later) PC.

Nortel recommends loading the application from the network, rather than the faceplate PC Card.

Application upgrade

On occasion, a field up-issue is done over the network. In this instance, the customer is provided with a customer-specific binary file containing a new software load. The binary file includes both the base code and the application code.

Maintenance or bug fix upgrade

The user installs the new software from the network.

Patching tool

A patch is a piece of code that is inserted or patched into an executable program. The patching tool enables loadware on the Media Card 32-port and ITG-Pentium 24-port trunk cards to be patched or fixed without having to upgrade the IP trunk card loadware and without service interruption.

All patch commands on the Media Card 32-port and ITG-Pentium 24-port trunk cards are accessible at the ITG> shell prompt. These commands are summarized in Table 66 on page 546.

The parameter string supplied to the command must be enclosed with double quotes. For example, the syntax for the pload command is pload "patch1.p".

These commands are used to manage patches on the Media Card 32-port and ITG-Pentium 24-port trunk cards. Patches must be downloaded from a workstation to the Media Card 32-port and ITG-Pentium 24-port trunk cards using a modem, an FTP session, or OTM 2.1 (and later). Patch files are stored in Flash memory and are loaded into DRAM memory. Once a patch is in DRAM memory, it can be activated, deactivated, and its status can be monitored.

Perform the following tasks prior to loading a patch:

1 Check that the patch matches the platform's CPU type.

2 Check the loadware version on the card.

3 Block the installation if there is a mismatch.

The installation of a patch is blocked if either the CPU type or the loadware version of the IP trunk card is different than the patch. If the installation is blocked, the reason for blocking the install is printed at the CLI. The CPU type and loadware version are also checked during a power-up or reboot cycle. This prevents active patches from being re-installed if the loadware version of the IP trunk card is changed.

Table 66 lists the patch commands.

Table 66
Patch commands (Part 1 of 3)

Command	Description
pload	Loads a patch file from the file system in Flash memory into DRAM memory. The loaded patch is inactive until it is put into service using the pins command. When a patch is successfully loaded, the pload command returns a **patch handle number**. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). Syntax: pload "[patch-filename]" where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. If the pload command is issued without a parameter, the technician is prompted for the patch filename and other information.
pins	Puts a patch that has been loaded into memory (using the pload command) into service. This command activates a patch. If issued successfully, the pins command indicates that global procedures, functions, or areas of memory are affected by the patch. The technician is then prompted and has the choice to proceed or not to proceed. Syntax: pins "[handle]" where [handle] is the number returned by the pload command If the pins command is issued without a parameter, the technician is prompted to enter a handle.

Table 66
Patch commands (Part 2 of 3)

Command	**Description**
poos	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state. Syntax: poos "[handle]" If the poos command is issued without a parameter, the technician is prompted to enter a handle.
pout	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. Syntax: pout "[handle]" If the pout command is issued without a parameter, the technician is prompted to enter a handle.
pstat	Gives summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. ***Note:*** Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. Syntax: pstat "[handle]" If the handle is provided, only the information for the specified patch is displayed. If the pstat is issued without a parameter, information for all the patches is displayed.

Table 66
Patch commands (Part 3 of 3)

Command	Description
plis	Gives detailed patch status information for a loaded patch. Syntax: plis "[handle]" If the pout command is issued without a parameter, the technician is prompted to enter a handle.
pnew	Creates memory patches for the Media Card 32-port and ITG-Pentium 24-port trunk cards. • The release of the patch is assumed to be the same as that of the current load. • The address to be patched is checked to ensure that it is in range. • For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. • If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/patch directory. Once a memory patch is created using the pnew command, it is loaded and activated like any other patch. Syntax: pnew ***Note:*** The pnew command has no parameter(s).

Patch Directories

There are two patch directories on an IP trunk card:

1 **/C:/u/patch**

This is the default directory for patch files. Patch files should be copied to this directory.

2 **/C:/u/patch/reten**

Use this directory to store patch retention control files. Do not use this directory to store patches and do not remove files from this directory.

Flash storage upgrades

These are provided through standard 5 Volt ATA-compatible PC Cards. When installed in an IP trunk card ("hot installation" allowed), the additional storage provided by the IP trunk card is made available as A:/.

Software upgrade mechanisms

Use OTM 2.1 (and later) to upgrade software. Reboot the IP trunk card to run the new software.

Upgrade software using OTM

The new IP Trunk 3.01 (and later) software application can be downloaded from the OTM 2.1 PC to the IP trunk card. Follow the steps in Procedure 69 to upgrade software.

Procedure 69
Upgrading software using OTM 2.1 (and later)

1 Download the latest IP Trunk 3.01 (and later) software version from Nortel. Determine the location on the OTM 2.1 (and later) PC hard drive where it is to be loaded. Record the OTM PC hard drive location for use later in this procedure. For more detailed instructions on how to access the latest software version, turn to "Check and download IP trunk card software in OTM 2.1 (and later)" on page 361.

2 Open OTM 2.1 (and later) and launch the ITG ISDN IP Trunks application.

3 Check the current software version of the IP trunk cards to be upgraded. To check the software version, double-click a card and click the **Configuration** tab. “S/W version” displays the current software version as read from the IP trunk card.

4 From the main card list view, select the cards to be upgraded. Upgrade all cards in the node together, unless installing a spare card that has older software.

5 To disable all IP trunk cards to be upgraded, use one of the following:

- the LD 32 DISI command from the OTM Maintenance windows
- the OTM System Passthru terminal
- a system management terminal directly connected to a TTY port on the system

6 In the **OTM IP Telephony Gateway Main** window, select “View/Refresh” and verify that the card status is showing “Disabled.”

7 Select menu **Configuration > Synchronize > Transmit**.

An ITG – Transmit Options dialog box is displayed.

8 In the Transmit Options group box, select the radio button “Transmit to selected cards.”

9 In the Software Download group box, check “Card software.”

10 Click the **Browse** button to locate the IP Trunk 3.01 (and later) IP trunk card software downloaded earlier to the OTM PC hard drive. Select the software file and click “Open” to save the selection. The path and file name of the IP Trunk 3.01 IP trunk card software appears in the edit box next to the **Browse** button.

11 Click the **Start Transmit** button to begin the IP trunk card software upgrade process.

The software is transmitted to each card in turn and is burned into the flash ROM on the IP trunk card.

Monitor the status in the **Transmit Control** window. Confirm that the IP trunk card software is transmitted correctly to all cards. Note any error messages. Examine and correct any problems. Repeat IP trunk card software transmission until it is completed correctly on each IP trunk card. The IP trunk cards continue to run the old software until they are rebooted.

12 Reboot each IP trunk card that received transmitted software, so that the new software can take effect. Start the rebooting with Leader 0, then Leader 1, and lastly the Follower cards. After all the IP trunk cards have been reset and have correctly rebooted, they respond to the OTM IP Trunk 3.01 (and later) status refresh (that is, disabled: active; disabled: backup: disabled).

13 These cards should remain in the disabled state after the upgrade so the technician can issue a "Reset" command from the Maintenance menu or the **Maintenance** tab in the **ITG Card Properties** window to each card to reboot them. Alternatively, reset the cards by pressing the Reset button on the card faceplate using a pointed object.

14 Double-click each upgraded card and check the software version on the **Configuration** tab of the Card Properties.

15 Use the LD 32 ENLC command to re-enable the IP trunk cards.

End of Procedure

Replace an IP trunk card

Following a reboot, if the IP trunk card displays an "F:xx" on the LED Maintenance Display, this indicates an unrecoverable hardware failure. The IP trunk card will not register with the system. For a complete listing of faceplate Maintenance Display codes for the Media Card 32-port trunk card, see "Media Card 32-port trunk card faceplate maintenance display codes" on page 560. For a complete listing of faceplate Maintenance Display codes for the ITG-Pentium 24-port trunk card, see "ITG-Pentium 24-port trunk card faceplate maintenance display codes" on page 563.

Remove the IP trunk card for two to three seconds and then re-install it. If the failure continues, replace the card. Follow the steps in Procedure 70 on page 552 to replace the card.

Procedure 70
Replacing an IP trunk card

1 Locate the node of the defective IP trunk card:

- **a.** Open the **ITG ISDN IP Trunks** application in OTM.
- **b.** In the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window, click the site name. All the cards in the node are listed in the lower part of the window.
- **c.** Locate the defective IP trunk card in the lower window by card TN.

2 Disable the defective IP trunk card in LD 32 using the DISI command.

3 If the card to be replaced is an ITG 8-port trunk card, disconnect the TLAN Ethernet cable from the faceplate of the bad card. Label the cable to identify it as the TLAN Ethernet connection so it can later be reattached to the replacement card.

If the card to be replaced is an ITG 8-port trunk card or a ITG-Pentium 24-port trunk card, disconnect the TLAN Ethernet cable from the I/O cable. Label the cable to identify it as the TLAN Ethernet connection to aid in re-installing the cable on the replacement card. Remove the defective IP trunk card.

If the card to be replaced is an Media Card 32-port trunk card, disconnect the TLAN Ethernet cable from the I/O cable or L-adapter. Label the cable to identify it as the TLAN Ethernet connection to aid in re-installing the cable on the replacement card. Remove the defective Media Card 32-port trunk card from the system.

4 From the lower window, select Leader 0 or any IP trunk card in the node.

5 Select menu **Configuration > Node > Properties** in the **IP Telephony Gateway** window.

6 Click the **Configuration** tab in the **ITG Node Properties** window.

7 In the **Configuration** tab, select the defective IP trunk card from the list of cards in the node.

8 Change the MAC address to the MAC address of the replacement IP trunk card. The MAC address is the “Motherboard Ethernet” address on the faceplate label of the replacement IP trunk card.

9 Click “OK”.

10 Select Leader 0 or any IP trunk card in the node.

11 Select menu **Configuration > Synchronize > Transmit** to transmit the Node Properties from OTM to the Active Leader card of the IP Trunk 3.01 (and later) node. Click the "Node Properties" box and then click "Start Transmit." This updates the node properties of the Active Leader card with the MAC address of the replacement IP trunk card.

12 Install the replacement IP trunk card into the system:

a. Pull the top and bottom locking devices away from the IP trunk card faceplate.

b. Insert the IP trunk card into the card guides and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When the IP trunk cards are installed, the red LED on the faceplate is lit if: the card has rebooted; the card is active but there are no trunks configured on it, or the card is active and has trunks, but the trunks are disabled. If the LED does not follow the pattern described (for example, remaining continuously flashing or weakly lit), replace the card.

Note 2: Observe the IP trunk card Faceplate Maintenance display to see startup self-test results and status messages. A display of the type "F:xx" indicates a failure. Some failures indicate that the card must be replaced. Refer to "Media Card 32-port trunk card faceplate maintenance display codes" on page 560 and "ITG-Pentium 24-port trunk card faceplate maintenance display codes" on page 563 for a complete listing of the codes.

13 Attach the TLAN Ethernet cable to the faceplate of the replacement IP trunk card.

Note: When connecting the IP trunk card to the TLAN subnet, the link status LED on the IP trunk card faceplate associated with the voice interface lights when the connection is made. The 100 Mbit/s link status LED on the Ethernet Switch port also turns on when correctly connected to the IP trunk card. This indicates that the corresponding port is set to operate at 100 Mbit/s and that the link is good.

14 If the card being replaced is an ITG 8-port trunk card and the replacement card is an ITG 8-port trunk card, the I/O cable must be replaced. The following steps describe the I/O cable replacement procedure:

a. Locate the NTCW84LA cable that was included in the ITG Trunk 1.0 to ITG Trunk 2.0 upgrade kit.

b. Remove the NTCW84MA cable from the I/O panel.

c. Disconnect the ELAN network interface CAT5 Ethernet cable and label it as the ELAN subnet connection.

d. If connected, disconnect the DCH and maintenance cable from the NTCW84MA.

e. Connect the new NTCW84LA cable to the I/O panel.

f. Connect the ELAN, TLAN, DCH and Maintenance cables (if previously connected) to the I/O cable. If the card being replaced is an ITG 8-port trunk card, connect the IP trunk card faceplate to the TLAN subnet.

15 In the OTM **IP Telephony Gateway - ISDN IP Trunk** Main window, select **View > Refresh** from the menu. Check that the replacement IP trunk card status is showing “Unequipped”.

End of Procedure

Determine IP trunk card software release

Follow the steps in Procedure 71 to determine the current software release on the IP trunk card.

Procedure 71
Determining the IP trunk card software release

1 In the **IP Telephony Gateway** window in OTM 2.1 (and later), double-click the replacement IP trunk card to open the **Card properties** window. Leave the default selection of the IP trunk card in the **Card Properties** window and click the **Configuration** tab.

2 Check that the “S/W release” shows the latest recommended software version.

3 If the replacement IP trunk card requires a software upgrade, refer to “Software upgrade mechanisms” on page 549.

End of Procedure

Transmit card properties and dialing plan

It is not necessary to disable IP trunk cards when transmitting a dialing plan alone.

Follow the steps in Procedure 72 to transmit IP trunk card properties and the dialing plan.

Procedure 72
Transmitting IP trunk card properties and dialing plan

1 In the **IP Telephony Gateway** window, select the replacement IP trunk card.

2 Click menu **Configuration > Synchronize > Transmit**.
The **ITG – Transmit Options** window appears.

3 Select the **Transmit to selected cards** radio button. Check the **Card properties** and **Dialing plan** boxes only.

Click the **Start Transmit** button.

The transmission status is displayed in the "Transmit control" box. Confirm the card properties and dialing plan are transmitted correctly.

4 When the transmission is complete, click the **Close** button.

5 Use the LD 32 ENLC command to re-enable the IP trunk card.

6 In the **IP Telephony Gateway** main window, select menu **View > Refresh**. The card status displays "Enabled."

7 Check the TN, ELAN network interface MAC address, and IP addresses for each IP trunk card. Compare the displayed values with those on the IP Trunk 3.01 (and later) Installation Summary Sheet.

8 Update the IP Trunk 3.01 (and later) Installation Summary Sheet with the new MAC address of the replacement IP trunk card.

End of Procedure

Backup and restore procedures

IP trunk card

Data configured on the OTM 2.1 (and later) PC (for example, address translation tables and DSP configuration) is locally saved on the OTM PC. The data is also downloaded to the IP trunk cards. The IP trunk card stores this data in its internal Flash File volume (Flash EPROM, which acts as a disk drive). The OTM PC can query the card and retrieve data from it. If the IP trunk card is replaced, the version of data stored on the OTM PC can be used to configure the new IP trunk card with the same data as on the replaced IP trunk card.

Log files, such as Alarm and Trace files, if any, are written to the Flash File volume and not lost when the card fails. Operational Measurement files are recorded hourly and need to be uploaded to the OTM PC or other external device for generating weekly or monthly traffic reports.

OTM 2.1 (and later)

OTM 2.1 (and later) has backup and restore procedures for all data downloaded from, or to, the IP trunk card. When an OTM terminal is connected to the card, user intervention is necessary to transmit all lost data from the OTM terminal to the IP trunk card.

Command Line Interface

If OTM is temporarily unavailable, the ITG shell CLI can be used to retrieve configuration files from an FTP server or from a PC Card.

Fault clearance procedures

This section provides possible solutions to such faults as the following:

- DSP failure
- card failure
- DCH failure
- DCH link failure
- PC Card failure
- DCHIP card failure
- power loss

DSP failure

If one of the DSPs does not respond, a DSP reset is automatically initiated by the host and an *dspResetAttempted* alarm is raised. If the DSP fails to recover after the reset, a *dspResetFailed* alarm is raised and that DSP is marked as unusable. Any channels associated with that DSP cease to respond to the system and are ultimately taken out of service by the system background audit procedures.

If a DSP fails, the following can occur:

- A DSP fails when no channel on it is in use (that is, no existing call uses that DSP). All channels associated with that DSP are marked as DISabled until the DSP recovers. The leader card is notified so that no incoming call is assigned to those channels.
- A DSP fails when at least one of its channels is in use. All calls associated with that DSP are dropped and all its channels are put into the DISabled state. The leader card is notified so that no incoming call is assigned to those channels.

When the system initiates a call at a channel of a failed DSP, the DCHIP card sends a “RELease COMplete” message in response to indicate that the channel cannot be used. Then, the system generates the alarm “PRI0101” and locks out the trunk by marking it “BUSY”. This mechanism is also used to lock out a channel that does not have a corresponding DSP port.

When the DSP recovers, all the associated channels are put into the "IDLE" state. "REStart" messages for all channels are sent to the system to reset the trunks to the "IDLE" state. The leader card is informed and incoming calls can be assigned to those channels.

Card failure

Following a reboot, if the IP trunk card displays a code in the form of F:xx on the faceplate Maintenance display, this indicates an unrecoverable hardware failure. The card does not register with the system.

Remove the card for two to three seconds and then re-seat it in the IPE shelf. If the failure continues, replace the card.

DCH failure

There are three types of DCH failure which can affect the IP trunk card:

1. DCH link failure (DCH releases)
2. PC Card failure
3. DCH card failure

When the DCH fails (with no backup DCH), the following occurs:

- Established calls are maintained.
- Transient calls are dropped.
- No new incoming calls are assigned to trunks associated with that DCH.
- Outgoing calls are blocked from occurring by the associated Follower cards forcing their trunks to a busy state.
- When the far-end user releases an established call, the system uses SSD messaging to the system to inform the core the call is released.
- When the near-end user releases an established call, the system informs the Follower through SSD messages.
- ISDN features across the IP network do not work.

DCH link failure

The DCH link can change to the RLS (Release) state due to technician action in LD 96, MSDL or SDI/DCH card failure, or cable failure. This condition is detected on the DCHIP card by the PC Card signaling that the L2 connection has failed.

PC Card failure

The PC Card failure can be detected in various ways, such as the following:

- missing heartbeat transmission
- a hardware interrupt

When the software does not send “an activity test message” (heartbeat message) to the Card Services of the PC Card Device Driver during a period greater than n seconds, Card Services consider it a breakdown detection. Card Services tries to reset the PC Card. Card Services are responsible to ensure the conformance of the reset timing. Card Services also check and wait for the card to reach the READY state.

Socket Services are responsible for card insertion and removal. There is a single interruption shared for insertion and removal events and a single interruption for device-specific interruptions. Socket Services identify which socket originates the interruption and sends the interruption to the Card Services interruption handler. Card Services then wait and re-initialize the PC Card, if the card is plugged in again and is in the READY state.

Do not insert or remove the PC Card when the IP trunk card is plugged in.

DCHIP card failure

This occurs when the DCHIP IP trunk card goes out of service. The DCHIP IP trunk card failure case is similar to the DCH link failure case. However, all call reference information is gone. As a result, when the DCHIP comes back up, it sends a “REStart” message to the other side to re-initialize all the trunks. All the established calls are terminated.

Power loss

Since the IP trunk card is based on Flash EPROM technology, all configuration data is preserved for 10 years. There is no requirement for a battery backup for the card. The IP trunk card can be removed from the IPE shelf indefinitely and still retain all configuration data.

Media Card 32-port trunk card faceplate maintenance display codes

The maintenance display of the Media Card 32-port trunk card provides startup codes, operating mode and error information on the functional card state. Table 67 lists the startup codes and operating mode codes.

When the Media Card 32-port trunk card starts up, it performs multiple self-tests. The faceplate display shows the test results.

If the internal RAM test, ALU test, address mode test, boot ROM test, timer test, or external RAM test fails (T:00 - T:07), the pack goes into a maintenance loop as no further processing is possible. If a test fails, F:XX shows on the hex display for three seconds after the T:13 message, with the number represented by XX indicating the test that failed. For example, if the 8051 co-processor failed, F:05 displays. If more than one test fails, the message displayed indicates the first failure.

If the hardware self-tests pass and the application starts up successfully, the screen cycles through the display codes to indicate the function and status of the card.

Table 67
Media Card 32-port trunk card faceplate maintenance display message summary (Part 1 of 3)

Code	Description
T:00	Initialization
T:01	Testing internal RAM
T:02	Testing ALU
T:03	Testing address modes
T:04	Testing watchdog

Table 67
Media Card 32-port trunk card faceplate maintenance display message summary (Part 2 of 3)

Code	Description
T:05	Testing 8051 co-processor
T:06	Testing timers
T:07	Testing external RAM
T:08	Testing dongle
T:09	Programming timeswitch FPGA
T:10	Programming ISPDI FPGA
T:11	Testing host dual port RAM
T:12	Testing DS-30 dual port RAM
T:13	Testing SEEPROM
T:14	Booting Host processor, waiting for response with self-test information
T:15	Not used at present
T:16	Not used at present
T:17	Not used at present
T:18	Not used at present
T:19	Not used at present
T:20	Waiting for application startup message from Host processor
T:21	CardLAN enabled, waiting for request configuration message
T:22	CardLAN operational, A07 enabled, display now under host control

Table 67
Media Card 32-port trunk card faceplate maintenance display message summary (Part 3 of 3)

Code	Description
BIOS	Card is running the ROM BIOS. The card detected no valid IP Trunk 3.01 (and later) software image or the JKL escape sequence was entered during startup from the keyboard of a terminal connected to the local maintenance port. If the IP trunk card faceplate displays BIOS, it is not functioning as an IP trunk card.
LDR	Card is running active leader tasks.
BLDR	Card has detected existing Active Leader and is running Backup Leader tasks, or the card is configured as a Leader and is missing its node properties. Transmit node properties from OTM.
FLR	Card has detected the Active Leader and is running Follower tasks.

In addition, if the IXP encounters any failures during its initialization, an H:XX error code displays. The list of error codes is listed in Table 68.

Table 68
List of error codes

Code	Description
H:00	Host Processor not booting
H:01	SDRAM test failure
H:02	SRAM test failure
H:04	PC Card device failure
H:08	Network interface failure
H:10	System interface failure
H:20	DSP interface failure
H:40	NVRAM/EEPROM interface failure
H:80	PCM connector failure

ITG-Pentium 24-port trunk card faceplate maintenance display codes

The maintenance display of the ITG-Pentium 24-port trunk card provides startup codes, operating mode and error information on the functional card state. Table 69 on page 564 lists the startup codes and operating mode codes.

When the ITG-Pentium 24-port trunk card starts up, it performs multiple self-tests. The faceplate display shows the test results.

If self-tests T:00-T:09 fail, the self-test program stops and the faceplate displays an “F:xx” message to indicate which test failed. For example, if the timer test T:05 fails, “F:05” is displayed. If more than one test fails, the message displayed indicates the first failure.

If self-tests T:10-T:17 fail, the display contains the failure message for three seconds and the ITG-Pentium 24-port trunk card goes on to the next test. If more than one test fails, the message displayed indicates the last failure.

Table 69
ITG-Pentium 24-port trunk card faceplate maintenance display message summary (Part 1 of 3)

Normal Code	Fault Code	Description
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing Boot ROM
T:05	F:05	Testing timers
T:06	F:06	Testing watchdog
T:07	F:07	Testing external RAM
T:08	F:08	Testing Host DPRAM
T:09	F:09	Testing DS30 DPRAM
T:10	F:10	Testing for presence of security device. The ITG-Pentium 24-port trunk card has no security device. ***Note:*** For the ITG-Pentium 24-port trunk card, a momentary display of F:10 is normal.
T:11	F:11	Testing flash memory
T:12	F:12	Programming PCI FPGA
T:13	F:13	Programming DS30 FPGA
T:14	F:14	Programming CEMUX FPGA
T:15	F:15	Programming DSP FPGA

Table 69
ITG-Pentium 24-port trunk card faceplate maintenance display message summary (Part 2 of 3)

Normal Code	Fault Code	Description
T:16	F:16	Testing CEMUX interface
T:17	F;17	Testing EEPROM
T:18	F:18	Booting host, waiting for response with self-test information
PT:0	PF:0	Pentium module suspend signal OK
PT:1	PF:1	Pentium module powered OK ***Note:*** If the displays this message, check that the Pentium module is fully seated in the motherboard socket.
T:19		Waiting for application startup message from host
T:20		Card LAN enabled, waiting for Request Config Message. IP trunk card is looking for an active leader by sending BOOTP requests on the ELAN subnet. If no BOOTP response is received on the ELAN subnet, Leader 0 times out first and starts active leader tasks. Leader 1 has a longer time out and normally starts backup leader tasks when it detects an active leader, otherwise Leader 1 times out and starts active leader tasks. A Follower card sends BOOTP requests on the ELAN subnet continuously and never times out. From the keyboard of a terminal attached to the local maintenance port, enter +++ to escape from BOOTP request mode and start ITG shell for manual configuration.

Table 69
ITG-Pentium 24-port trunk card faceplate maintenance display message summary (Part 3 of 3)

Normal Code	Fault Code	Description
BIOS		Card is running the ROM BIOS. The card detected no valid IP Trunk 3.01 (and later) software image or the JKL escape sequence was entered during startup from the keyboard of a terminal connected to the local maintenance port. If the IP trunk card faceplate displays BIOS, it is not functioning as an IP trunk card.
T:21		Card LAN operational, A07 interface to system enabled, display now under IP Trunk 3.01 (and later) software control. ITG > shell is available for manual card configuration.
T:22		ITG-Pentium 24-port trunk card is starting up the IP Trunk 3.01 (and later) application.
LDR		Card is running active leader tasks.
BLDR		Card has detected existing Active Leader and is running Backup Leader tasks, or the card is configured as a leader and is missing its node properties. Transmit node properties from OTM.
FLR		Card has detected the Active Leader and is running Follower tasks.

System performance under heavy load

When the system and IP Trunk 3.01 (and later) are carrying traffic approaching the maximum sustained levels, there can be short bursts of traffic exceeding the maximum threshold level. This is caused by the randomness of call starts. When the maximum threshold levels are exceeded, error messages are printed to the system screen. In extreme cases, it can cause call loss.

The different components within the system each have different maximum thresholds of traffic and have different ways of measuring and reacting to those traffic levels. Most components, such as the D-channel card in the system and the IP trunk card, have the capability to discard messages when necessary. These recovery methods can be mitigated by proper system engineering, but cannot be avoided completely. For example, random calls can create situations where more messages attempt to travel down the D-channel than the D-channel can handle. The D-channel has a fixed maximum bit-rate. When that maximum is exceeded, messages are discarded.

The effects of this recovery process usually appear as certain error messages. These error messages can be viewed by checking log messages on the system.

The following error messages occur when narrow (peak) bursts of traffic or messaging exceed the maximum sustained rate by a significant margin, resulting in call failure or signaling failure.

Message: PRI241

Description

PRI241 is defined as a protocol error where no response to the PRI call occurred at the far end.

Normal cause

Peak traffic caused either the system D-channel or the IP trunk card to discard messages.

Normal resolutions

The following are possible resolutions:

- If the D-channel pack (such as MSDL) has multiple D-channels on it, the D-channel CPU might be unable to sustain the maximum traffic, especially if both or all D-channels peak at the same time. If this traffic level is sustained long enough, it can result in an **MSDL0304** error message.
- If the IP trunk card that houses the C-channel card (DCHIP Leader) also acts as Leader or Backup Leader for the node, it can become severely over-tasked. To resolve this situation, separate the D-channel and IP functions; that is, have the DCHIP Leader reside on a Follower card.
- If none of these apply, consider splitting the IP Trunk 3.01 (and later) node into two or more DCHIP Leader and Follower groups. This reduces the workload of the DCHIP Leader and allows the Leader to carry less of the signaling traffic.

Message: MSDL0304

Description

Message MSDL0304 is usually preceded by or followed by numerous PRI241 messages.

The MSDL0304 message says:
“The Meridian 1/CS 1000M received 100 or more messages from MSDL x within two seconds. At this level of message transfer, there may be some impact to the overall system performance. The level of service does not warrant removing the card from service.”

Normal cause

There are too many high-traffic D-channels on this MSDL card.

Normal resolutions

The following are possible resolutions:

- Carry the D-channel on two or more MSDL CARDS.

- If the MSDL card is an older vintage, it might be possible to upgrade the MSDL pack. This is the exception, rather than the rule; lower-capability MSDL packs have usually already been removed from service.

Message: BUG4005

Description

The system has lost a time slot, idling the applicable Call Register.

Normal cause

Depending on the context, the cause could be traffic levels, to the cause could be another totally unrelated issue. This message must be analyzed to determine the cause and what corrective action should be taken.

Normal resolution

The resolution depends on the root cause of the problem. If the cause is traffic levels, then it might be necessary to balance traffic more evenly across the switch.

Message: BUG085

Description

The system detected an invalid switchhook state when the call was in the RINGING state. The switch-hook state should be off-hook; if it is not, the error message is generated.

Normal cause

The causes can include debounce error and guard timer violation.

Normal resolutions

The problem is usually self-healing; the call recovers and proceeds. Occasionally, if the problem is related to high traffic levels, the specific call could fail. In such a case, a retry occurs.

Appendix A: Patches and advisements

Contents

This section contains information on the following topics:

Introduction

This appendix describes the following patches for IP Trunk 3.0 and IP Trunk 3.01: MPLR17662, MPLR17346, MPLR18142, and MPLR18157.

IP Trunk 3.00.53 patches

The patches applicable to IP Trunk 3.00.53 that are mandatory to interwork with IP Trunk 3.01 are:

- MPLR17662
- MPLR17346

MPLR17662

When upgrading an existing network of IP Trunk 3.00.53 on a node-by-node basis, this patch must be installed on all existing IP Trunk 3.00.53 nodes before upgrading any node. Failure to do so will lead to memory corruption, causing the IP Trunk 3.00.53 application to malfunction or the IP Trunk card to reboot.This patch is not required if all existing IP Trunk nodes are upgraded to IP Trunk 3.01 in a single maintenance window.

Refer to "Interoperability with IP Trunk 3.01 (MPLR17662 patch)" on page 572 for more information.

MPLR17346

Fax calls fail due to the wrong TCF method used for T.38 UDP Fax channel setup. The application on the CS 1000 and the BCM 3.5 use method 2 and IP Trunk 3.0 uses method 1.

IP Trunk 3.01.22 patches

The patches applicable to IP Trunk 3.01.22 are:

- MPLR18142
- MPLR18157

MPLR18142

FIN_WAIT_2 socket loss and related IXP restart avoidance.

MPLR18157

TLAN subnet info not recognized if QSIG uses 7-bit channel address.

Interoperability with IP Trunk 3.01 (MPLR17662 patch)

When upgrading an existing network of IP Trunk 3.0 (3.00.53) nodes to IP Trunk 3.01 (3.01.22), calls from the IP Trunk 3.0 node to the IP Trunk 3.01 node may result in memory being corrupted, causing the IP Trunk application to malfunction or the IP Trunk card to reboot. One scenario where this problem might occur is:

1. Two IP Trunk nodes, Node-1 and Node-2, are connected over the IP network.
2. Node-1 is running on IP Trunk 3.0. Node-2 is running on IP Trunk 3.01, which includes message enhancements to avoid the blocking of valid anti-tromboning requests to prevent call swaps with the Trunk Anti-Tromboning (TAT) enhancement. The Endpoint ID (EPID) is new in IP Trunk 3.01.

3 The EPID is sent, along with other information, in the SETUP and CONNECT messages. A call placed from Node-2 to Node-1 includes this information in the SETUP message.

4 The existing message decoding logic at Node-1, running on IP Trunk 3.0, may incorrectly read the EPID information as ESN5 information.

5 Calls from Node-1 to Node-2 do not have this problem.

Patch MPLR17662, which is put into service on the IP Trunk 3.0 node, prevents this problem. It enables the node to parse and select the correct information and discard the rest. In this scenario, the patch must be loaded on Node-1.

In general, to prevent malfunction or reboot, do one of the following:

- upgrade all existing IP Trunk nodes to IP Trunk 3.01 in a single maintenance window; or
- install patch MPLR17662 on all existing IP Trunks first. Only then can the customer upgrade the existing IP Trunk nodes gradually, node by node, to IP Trunk 3.01.

Since there is no adverse effect caused by installing the patch on IP Trunk 3.0, and upgrading a network on a node-by-node basis simplifies maintenance greatly, Nortel recommends that the second alternative be used.

> ***Note:*** The nodes must use the Nortel H.323 Interoperability format or use a Gatekeeper to resolve destinations.

The applicability of MPLR17662 is limited in certain situations:

- The patch is required if the format of the received SETUP message is CSE, with or without a Gatekeeper. If the format received is not CSE, the patch is not required.

- The patch is not required for ITG Trunk 2.x.26G or ITG Trunk 2.x.25 interworking with IP Trunk 3.01.22, as these older versions of ITG Trunks do not support the CSE format.
- The patch is not required when upgrading a few IP Trunks to IP Trunk 3.01.22 to interoperate with other nodes running IP Trunk 3.00.53, ITG Trunk 2.32.26G, and ITG Trunk 1.0.43, and the format received is SL1, SL1 ESN5, or QSIG. If the format received is CSE, which is not supported on ITG Trunk, the patch is required.

For pairs of nodes in this scenario, the following applies:

- IP Trunk 3.00.53 interworking with 3.01.22 - the patch is required if the CSE format is used.
- IP Trunk 2.32.26G interworking with IP Trunk 3.01.22 - no patch is required.
- IP Trunk 1.0.43 interworking with IP Trunk 3.01.22 - no patch is required.

Appendix B: Cable description and NT8D81BA cable replacement

Contents

This section contains information on the following topics:

Introduction

This appendix describes the NTMF94EA, NTCW84KA, NTAG81CA, NTAG81BA, NTCW84LA, and NTCW84MA cables. This appendix also explains how to replace the NT8D81BA ribbon cable with the NT8D81AA ribbon cable. Replace the NT8D81BA ribbon cable, with a NT8D81AA cable if the a network uses 100-Base-T.

For information on cabling the Media Card 32-port trunk card, see “Cabling for the Media Card 32-port trunk card” on page 276.

NTMF94EA ELAN, TLAN and Serial Port cable

The NTMF94EA cable connects the I/O connector on Meridian 1 Option 11C Cabinet, CS 1000M Cabinet, or Large Systems to the ELAN network interface, TLAN network interface, and one RS-232 port. See Figure 147 and Table 70 on page 577.

Figure 147
NTMF94EA ELAN, TLAN and serial port cable

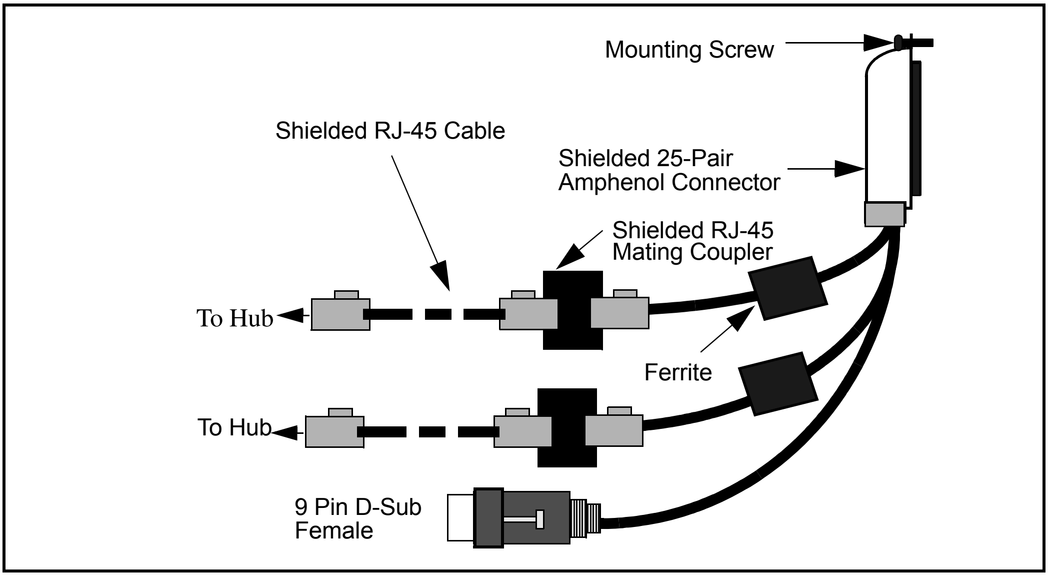


Table 70
NTMF94EA ELAN, TLAN, and Serial Port cable connections

I/O Panel: P1	Signal Name	P2, P3, P4	Color
P1-21	BSOUTB-	P2-2	Red
P1-22	BDTRB-	P2-4	Green
P1-25	SGND	P2-5	Brown
P1-45	BSINB-	P2-3	Blue
P1-46	BDCD-	P2-1	Orange
P1-47	BDSRB-	P2-6	Yellow
P1-9	SHLD GRND		
P1-25	SHLD GRND		
P1-43	SHLD GRND		
P1-50	SHLD GRND		
P1-23	RXDB+	P3-3	Green/White
P1-24	TXDB+	P3-1	White/Green
P1-48	RXDB-	P3-6	Orange/White
P1-49	TXDB-	P3-2	White/Orange
P1-18	RX+	P4-3	Green/White
P1-43	RX-	P4-6	White/Green
P1-19	TX+	P4-1	Orange/White
P1-44	TX-	P4-2	White/Orange

NTCW84KA ELAN, TLAN, DCH & serial cable

The NTCW84KA cable connects the I/O connector on Cabinet or Large systems to the ELAN and TLAN network interfaces with one RS-232 port and D-channel signalling. The DCH serial I/O port has a 15-pin male D-type connector to connect to the MSDL cable. On Large Systems, the NT8D81AA cable connects all 24 tip and ring pair to the I/O panel. (See Figure 148 and Table 71 on page 579.)

Figure 148
NTCW84KA ELAN, TLAN, DCH, and serial cable

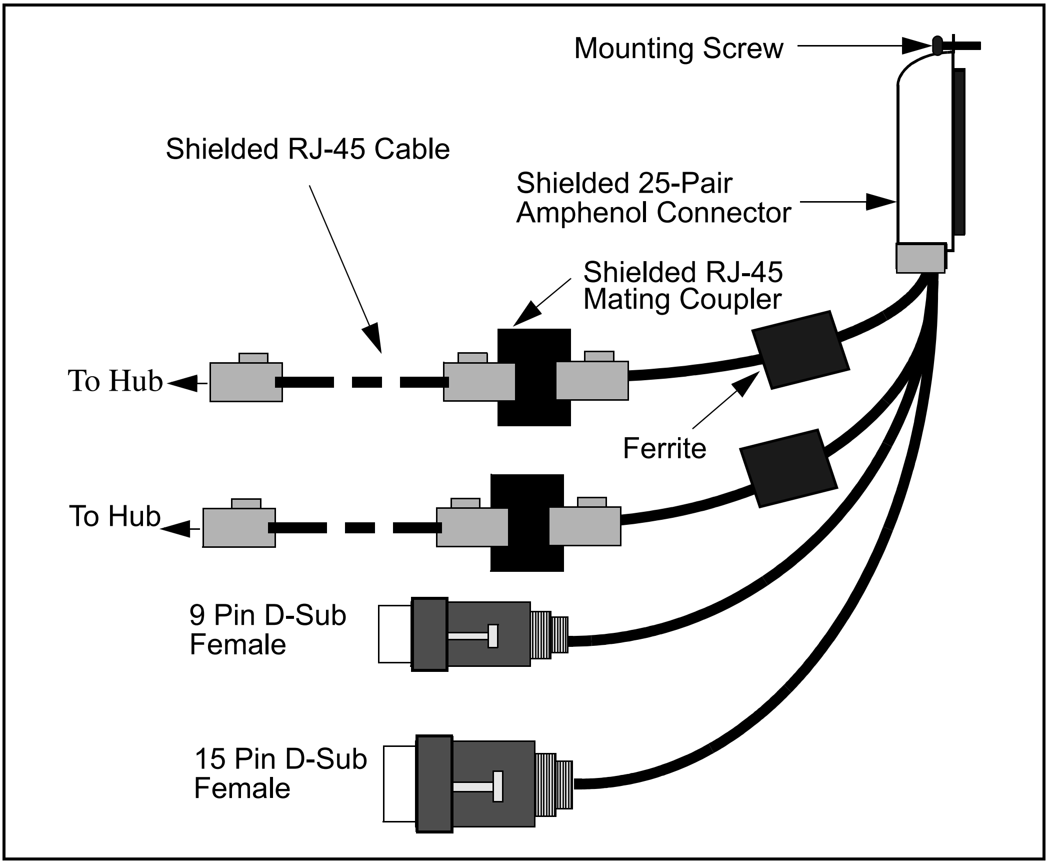


Table 71
NTCW84KA ELAN, TLAN, DCH, & Serial I/O cable connections (Part 1 of 2)

I/O Panel: P1	Signal Name	P2, P3, P4, P5	Color
P1-21	BSOUTB-	P2-2	Red
P1-22	BDTRB-	P2-4	Green
P1-25	SHLD GND	P2-5	Brown
P1-45	BSINB-	P2-3	Blue
P1-46	BDCDB-	P2-1	Orange
P1-47	BDSRB-	P2-6	Yellow
P1-5	P2 SHLD GRND		
P1-6	P2 SHLD GRND		
P1-8	P2 SHLD GRND		
P1-25	P2 SHLD GRND		
P1-30	P2 SHLD GRND		
P1-31	P2 SHLD GRND		
P1-50	P2 SHLD GRND		
P1-23	RXDB+	P3-3	Green/White
P1-48	RXDB-	P3-6	White/Green
P1-24	TXDB+	P3-1	Orange/White
P1-49	TXDB-	P4-2	White/Orange
P1-18	RX+	P4-3	Green/White
P1-43	RX-	P4-6	White/Green
P1-19	TX+	P4-1	Orange/White
P1-44	TX-	P4-2	White/Orange

Table 71
NTCW84KA ELAN, TLAN, DCH, & Serial I/O cable connections (Part 2 of 2)

I/O Panel: P1	Signal Name	P2, P3, P4, P5	Color
P1-10		P5-2	Black
P1-13		P5-10	Red
P1-11		P5-9	Black
P1-14		P5-11	White
P1-35		P5-4	Black
P1-38		P5-12	Green
P1-36		P5-5	Black
P1-39		P5-13	Blue
P1-12		P5-8	Black
P1-37		P5-15	Yellow
P1-25		P5-1	Black
	NC		Brown
P1-25		P5 SHLD GRND	Bare
P1-50		P5 SHLD GRND	Bare

NTAG81CA Faceplate Maintenance cable

The NTAG81CA cable connects an OTM 2.1 (and later) PC or terminal to the IP trunk card through the maintenance port connector on the IP trunk card faceplate. Connect this cable directly to the 9-pin D-type RS-232 input (COM port) on a standard PC. See Figure 149 on page 581 and Table 72 on page 581.

Figure 149
NTAG81CA PC maintenance cable

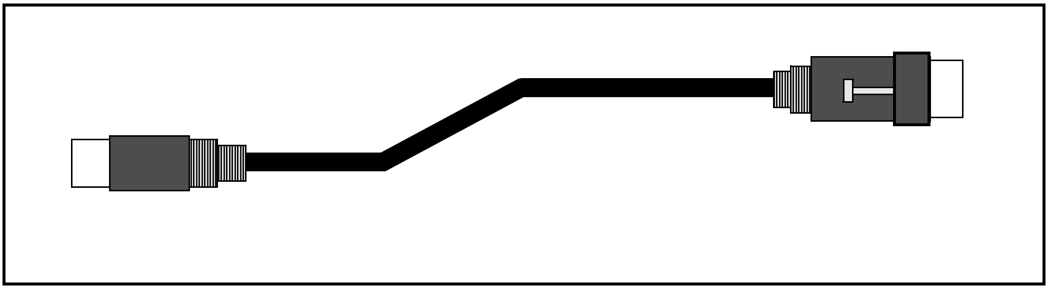


Table 72
NTAG81CA Faceplate Maintenance cable connections

Signals (IP Trunk 3.01 (and later) Side)	8-pin Mini-DIN (ITG Side) Male	9-pin D-sub (PC Side) Female	Signals (PC Side)
DTRB-	1	6	DSR-
SOUTB-	2	2	SIN-
SINB-	3	3	SOUT-
GND-	4	5	GND-
SINA-	5	NC	NC
CTSA-	6	NC	NC
SOUTA-	7	NC	NC
DTRA-	8	NC	NC

NTAG81BA Maintenance Extender cable

The 3m NTAG81BA cable connects the NTAG81CA cable to a PC or terminal. It has a 9-pin D-type connector at both ends: one male, one female. (See Figure 150 and Table 73.)

Figure 150
NTAG81CA Maintenance Extender cable

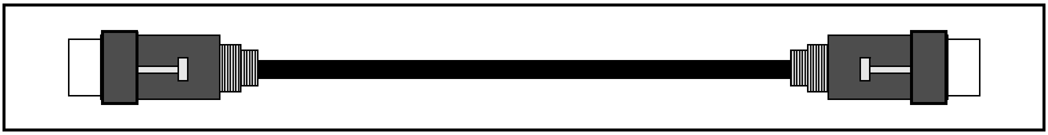


Table 73
NTAG81BA Maintenance Extender cable connections

9-pin D-Sub (Male)	9-pin D-Sub (Female)
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

NTCW84EA DCH PC Card pigtail cable

The NTCW84EA pigtail cable connects port 0 of the DCH PC Card to the J14 pin header on the motherboard. The cable routes the D-Channel signals to the backplane and the I/O panel. The PC Card connector is keyed to allow insertion only in the correct direction. The pin header connector is not keyed. Be careful to align the connector with the pin header. See Figure 151 on page 583 and Table 74 on page 584.

Figure 151
NTCW84EA pigtail cable

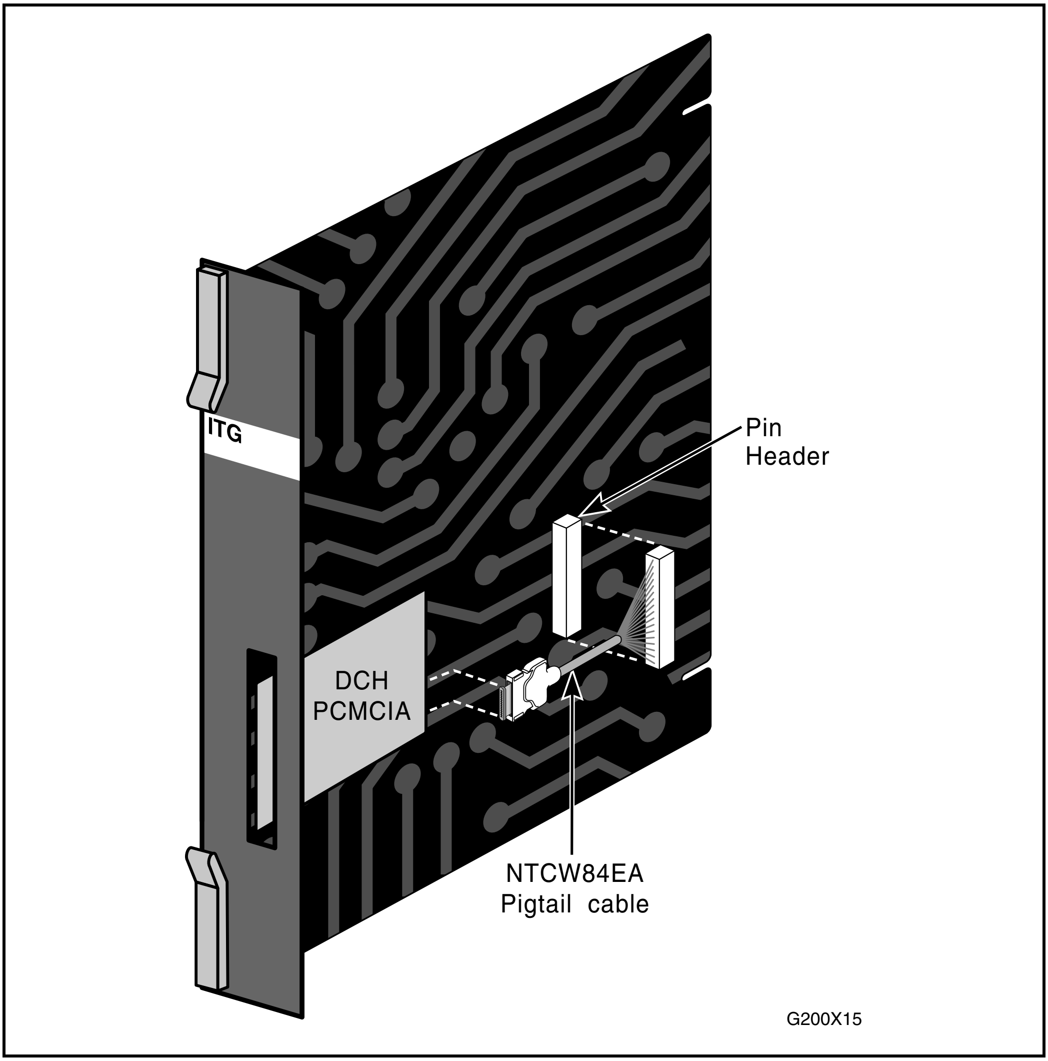


Table 74
NTCW84EA pigtail cable connections

PC Card P1	Signal Name	P2	Color
P1-1	SDAI	P2-1	Black
P1-2	RDAI	P2-2	White
P1-3	STAI	P2-3	Red
P1-4	RTAI	P2-4	Green
P1-5	CTS	P2-5	Brown
P1-8	TRI	P2-6	Yellow
P1-9	SDBI	P2-7	Violet
P1-10	RDBI	P2-8	Grey
P1-11	STBI	P2-9	Tan
P1-12	RTBI	P2-10	Pink
P1-15	GRND	P2-11	Green/Yellow

NTMF04BA MSDL extension cable

The NTMF04BA cable connects the MSDL (D-Channel) port of the NTCW84KA and the NTND26AA at the 15 pin I/O panel Filter Connector on the Network shelf. The male port of the NTMF04BA mates with the female 15-way D-sub port of the NTCW84KA. See Figure 152 on page 585 and Table 75 on page 585.

Figure 152
NTMF04BA MSDL extension cable

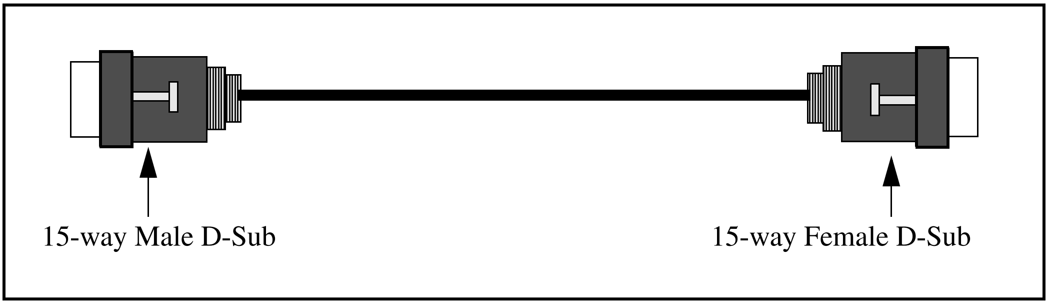


Table 75
NTMF04BA MSDL extension cable connections

P1 – Male	P2 – Female	Color	Signal
P1-2	P2-2	Black	SDA+
P1-10	P2-10	Red	SDB-
P1-9	P2-9	Black	STA+
P1-11	P2-11	White	STB-
P1-4	P2-4	Black	RDA+
P1-12	P2-12	Green	RDB-
P1-5	P2-5	Black	RTA+
P1-13	P2-13	Blue	RTB-
P1-8	P2-8	Black	FR
P1-15	P2-15	Yellow	TR
P1-1	P2-1	Black	SIG GRND

NTCW84LA and NTCW84MA upgrade cables

The following cables are required for the upgraded 8-Port ITG ISL Trunk DCHIP card:

- NTCW84LA for upgraded NTCW80CA cards
- NTCW84MA for upgraded NTCW80AA cards

The NTCW84LA and NTCW84MA shielded cables are required on DCHIP cards for ITG Trunk 1.0 to ITG Trunk 2.0 in field upgrades. It breaks out the signals from the I/O connector on Large systems and Option 11 to the ELAN network interface, TLAN network interface, one maintenance RS-232 port brought out on a 9-way D-type connection, and the D-channel port brought out on a 15-way D-type connection. The NT8D81AA cable is used to bring all 24 tip and ring pairs (on Large systems) from the backplane to the I/O panel and mates with the NTCW84LA cable.

It is very important that the NTCW84LA/MA cable be secured to the system with the mounting screw provided on the top of the 25-pair Amphenol connector.

The NTCW84LA/MA cable provides a shielded RJ-45 to RJ-45 coupler at the end of its ELAN and TLAN network interfaces. This provides the connection point to the customer's ELAN subnet equipment. Shielded CAT5 Ethernet cable must be used for connection from this point to the customer's hub or router. See Figure 153 on page 587 and Table 76 on page 588.

> ***Note:*** For all LAN cables originating from the IP trunk card, standard cable ties should be adopted to bundle these cables together as they route out of the system.

Figure 153
NTMF94LA upgrade cable

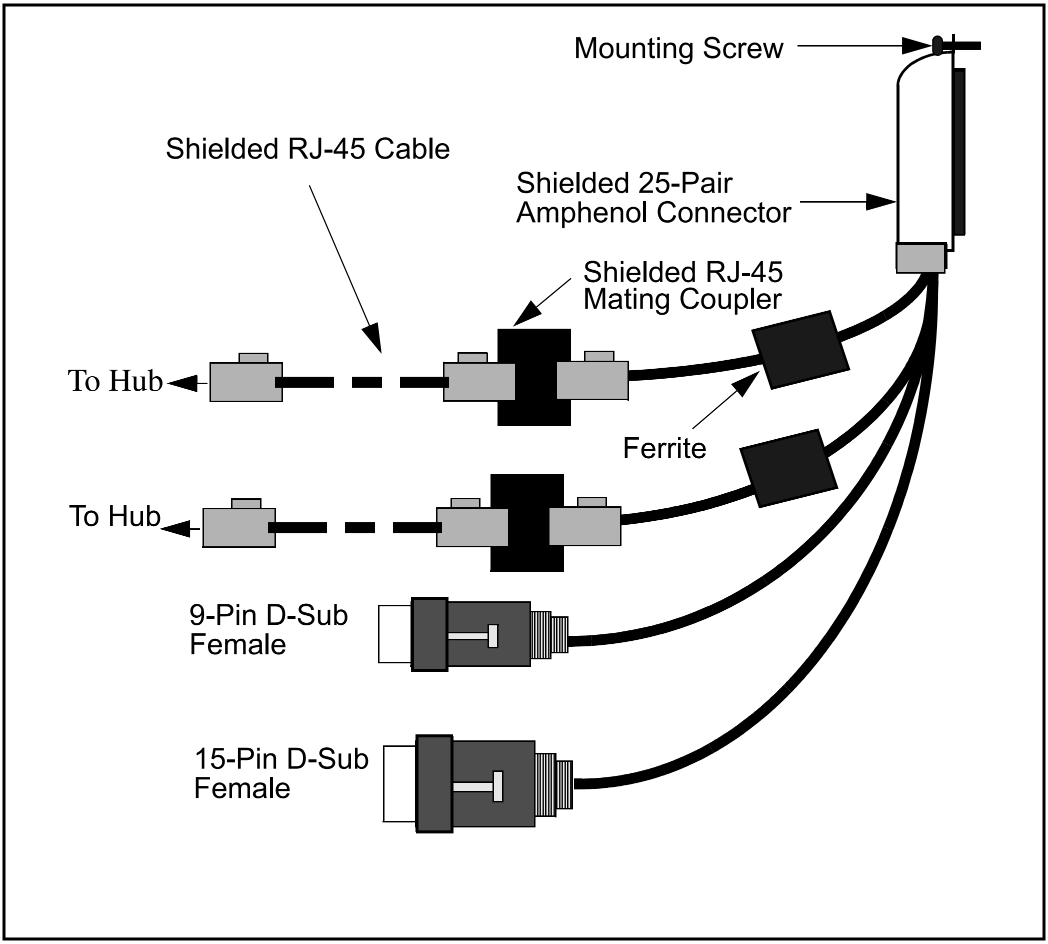


Table 76
NTMF94LA cable connections (Part 1 of 2)

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-21	BSOUTB-	P2-2	RED
P1-22	BDTRB-	P2-4	GREEN
	SGRND	P2-5	BROWN
P1-45	BSINB-	P2-3	BLUE
P1-46	BDCDB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RXDB+	P5-3	GRN/WHT
P1-19	TXDB+	P5-1	ORG/WHT
P1-43	RXDB-	P5-6	WHT/GRN
P1-44	TXDB-	P5-2	WHT/ORG
P1-23	RX+	P3-3	GRN/WHT
P1-24	TX+	P3-1	ORG/WHT
P1-48	RX-	P3-6	WHT/GRN
P1-49	TX-	P3-2	WHT/ORG
P1-10	SDAI	P4-2	BLACK
P1-13	SDBI	P4-10	RED

Table 76
NTMF94LA cable connections (Part 2 of 2)

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-11	STAI	P4-9	BLACK
P1-14	STBI	P4-11	WHITE
P1-35	RDAI	P4-4	BLACK
P1-38	RDBI	P4-12	GREEN
P1-36	RTAI	P4-5	BLACK
P1-39	RTBI	P4-13	BLUE
P1-12	CTS	P4-8	BLACK
P1-37	TRI	P4-15	YELLOW
P1-15	GRND	P4-1	BLACK
P1-25	SHLD GRND		BARE
P1-50	SHLD GRND		BARE

Prevent ground loops on connection to external customer LAN equipment

The shielded RJ-45 coupler is the connection point for the customer’s shielded CAT5 Ethernet cable to the hub, switch, or router supporting the

TLAN subnet and ELAN subnet. Use shielded CAT5 RJ-45 cable to connect to the customer's TLAN/ELAN subnet equipment.

Follow the steps in Procedure 73 to prevent ground loops when connecting to the customer's ELAN/TLAN subnet equipment.

Procedure 73
Preventing ground loops on connection to external LAN equipment

1 Connect the customer-provided shielded CAT5 Ethernet cable to the external LAN equipment. Ensure that the external LAN equipment is powered-up.

2 Use an ohmmeter to measure resistance to ground between the free end of the shielded RJ-45 cable and the building ground.

The ohmmeter *must* measure Open to ground before plugging it into the shielded RJ-45 coupler on the end of the NTMF94DA.

If it does *not* measure Open, install the unshielded RJ-45 coupler (provided) on the end of the NTMF94DA to prevent ground loops to external LAN equipment.

End of Procedure

Replace cable NT8D81BA with NT8D81AA

This section explains how to replace the NT8D81BA cable with the NT8D81AA cable and how to install the NTCW84JA special IPE filter.

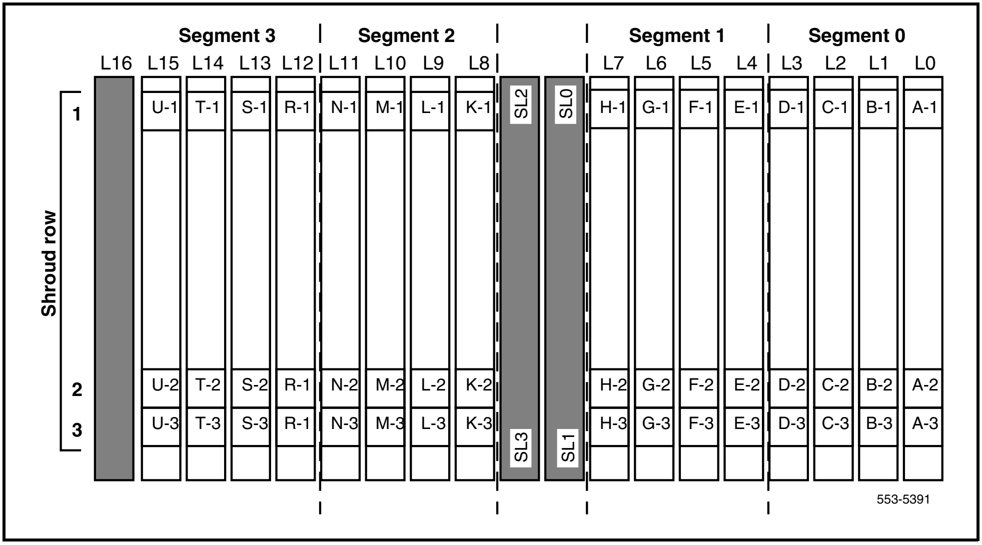
Cables are designated by the letter of the I/O panel cutout (A, B, C, and so on) where the 50-pin cable connector is attached. Each cable has three 20-pin connectors (16 positions are used), designated 1, 2, and 3, that attach to the backplane. Using the designations described, the backplane ends of the first cable are referred to as A-1, A-2, and A-3. The locations of the cable connectors on the backplane are designated by the slot number (L0 through L9 for NT8D11, L0 through L15 for NT8D37) and the shroud row (1, 2, and 3). Using these designations, the slot positions in the first slot are referred to as L0-1, L0-2, and L0-3.

In NT8D37BA and NT8D37EC (and later vintage) IPE modules, all 16 IPE card slots support 24-pair cable connections. Table 77 on page 592 shows the cable connections from the backplane to the inside of the I/O panel. Figure 154 on page 593 shows the designations for the backplane end of the cables, the backplane slot designations for the cable connections, and the associated network segments for the backplane slots.

Table 77
NT8D37 cable connections

Backplane slots–shroud rows	I/O panel/cable designation
L0–1, 2, 3	A
L1–1, 2, 3	B
L2–1, 2, 3	C
L3–1, 2, 3	D
L4–1, 2, 3	E
L5–1, 2, 3	F
L6–1, 2, 3	G
L7–1, 2, 3	H
L8–1, 2, 3	K
L9–1, 2, 3	L
L10–1, 2, 3	M
L11–1, 2, 3	N
L12–1, 2, 3	R
L13–1, 2, 3	S
L14–1, 2, 3	T
L15–1, 2, 3	U

Figure 154
Backplane slot designations


Segment 3
Segment 2
Segment 1
Segment 0
L16 L15 L14 L13 L12 L11 L10 L9 L8 L7 L6 L5 L4 L3 L2 L1 L0
Shroud row
1
2
3
U-1 T-1 S-1 R-1 N-1 M-1 L-1 K-1 H-1 G-1 F-1 E-1 D-1 C-1 B-1 A-1
U-2 T-2 S-2 R-1 N-2 M-2 L-2 K-2 H-2 G-2 F-2 E-2 D-2 C-2 B-2 A-2
U-3 T-3 S-3 R-1 N-3 M-3 L-3 K-3 H-3 G-3 F-3 E-3 D-3 C-3 B-3 A-3
SL2
SL0
SL3
SL1
553-5391

Tools list

- Ty-wrap cutter
- Ty-wraps
- Needle-nose pliers
- Slotted screwdriver

Remove the NT8D81BA cable

Follow the steps in Procedure 74 to remove the NT8D81BA cable.

Procedure 74
Removing the NT8D81BA cable

1 Identify the I/O panel and backplane designation that corresponds to the LEFT slot of the pair of card slots, viewed from the front, in which the Media Card 32-port or ITG-Pentium 24-port trunk card was installed.

2 Disconnect the filter from the I/O panel using a screwdriver and needle-nose pliers. Retain fasteners.

3 Power down the IPE shelf.

4 Remove the IPE module I/O safety panel.

5 To remove the ribbon cables from the IPE backplane:

a. Apply gentle pressure on the tab on the right side of the shroud while pulling on the connector until it pulls free from shroud.

b. Remove connector 1 first, then remove connectors 2 and 3.

6 Discard the NT8D81BA cable.

End of Procedure

Install NTCW84JA filter and NT8D81AA cable

Follow the steps in Procedure 75 to install the NTCW84JA filter and NT8D81AA cable.

Procedure 75
Installing the NTCW84JA filter and NT8D81AA cable

1 Install the NTCW84JA special IPE filter connector in the vacant I/O panel slot using retained hardware.

2 Install NT8D81AA ribbon cable connectors in the IPE module backplane shroud. Be sure to install the connector so the label is facing right with the arrow pointing up and the connector is fully engaged into the shroud:

a. Install connector 1, (labeled UP1^) into backplane shroud 1.

b. Install connector 2, (labeled UP2^) into backplane shroud 2.

   c. Install connector 3, (labeled UP3^) into backplane shroud 3.

3 Dress ribbon cables back individually inside the rear of the IPE module and restore the original arrangement. Start with the cables that are going to be underneath.

4 Attach the NTCW84JA special IPE filter to the NT8D81AA 50-pin connector using bail clips.

5 Restore power to the IPE module.

6 Replace I/O safety panel.

End of Procedure

Appendix C: Environmental and electrical regulatory data

Contents

This section contains information on the following topics:

Environmental specifications

Table 78 lists measurements of performance under test conditions of temperature and shock.

Table 78
Media Card 32-port and ITG-Pentium 24-port trunk card temperature and humidity specifications

Specification	Minimum	Maximum
Normal operation		
Recommended Relative humidity	15° C 10%	30° C 55% (non-condensing)
Absolute (less than 72 hours)	0° C	45° C
Relative humidity	5%	95% (non-condensing)
Rate of change Temperature cycling	Less than 1° C per three minutes 0° C to 65° C, 1° C/min., three cycles	
Storage		
Recommended Relative humidity	–50° C 0%	+70° C 95% (non-condensing)
Temperature shock		
In three minutes In three minutes	–50° C 70° C	25° C 25° C

Mechanical conditions

Refer to Table 79 for Media Card 32-port and ITG-Pentium 24-port trunk card mechanical tolerance ranges.

Table 79
Media Card 32-port and ITG-Pentium 24-port trunk card mechanical specifications

Specification	Minimum	Maximum
Mechanical		
Operating	5-200 Hz 0.1 g	Two hours per axis
Non-operating	5-100 Hz 0.5 g 100-200 Hz 1.5 g	30 min. per axis 30 min. per axis
Shock:		
Handling (Packs, unpackaged)	Free fall onto each face and corner	See IEC 68-2-31, Test Ec
Bounce	1.2 g, 30 min/surface	See IEC 68-2-31 Test Eb
Handling (Packs, packaged)	Free fall onto corner, 3 edges, all surfaces	See NSTA Proj 1A
Earthquake	NEBS GR-63-CORE, Zone 4	

Appendix D: Subnet mask conversion from CIDR to dotted decimal format

Subnet masks can be expressed in Classless Inter Domain Routing (CIDR) format, appended to the IP address (for example, 10.1.1.1/20). The subnet mask must be converted from CIDR format to dotted decimal format to configure ITG IP addresses.

CIDR format expresses the subnet mask as the number of bits counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. A typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format can have a value from 0 to 255, where 255 represents binary 1111 1111.

Follow the steps in Procedure 76 to convert a subnet mask from CIDR format to dotted decimal format.

Procedure 76
Converting a subnet mask from CIDR format to dotted decimal format

1. Divide the CIDR format value by 8. The result is equal to the number of dotted decimal fields containing 255.

   In the example above, (10.1.1.1/20), the subnet mask is /20. 20 divided by 8 is equal to 2, with a remainder of 4. The first 2 fields of the subnet mask in dotted decimal format are 255.255.

2. If there is a remainder, refer to Table 80 on page 602 to get the dotted decimal value for the field following the last field containing “255”.

   In the example of /20 previously given, the remainder is 4. In Table 80 on page 602, a remainder of 4 is equal to a binary value of 1111 0000 and the dotted decimal format value of the next and last field is 240. The first 3 fields of the subnet mask are 255.255.240.

3 If there are any remaining fields in the dotted decimal format, they have a value of 0. The complete subnet mask in dotted decimal format is 255.255.240.0.

Table 80
CIDR format remainders

Remainder of CIDR format value divided by 8	Binary value	Dotted decimal value
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix E: CLI commands

IP Trunk 3.01 (and later) supports the following CLI commands:

- **ectailDefault –** configure IP Trunk 3.01 (and later) to use the default 128ms Echo Canceller Tail length.
- **ectailNonDefault** – configure IP Trunk 3.01 (and later) to use the Echo Canceller Tail length specified in the OTM File.
- **dspFatalErrorCountShow** – details the number of fatal errors per DSP since last boot-up.
- **dspFatalErrorCountClear** – <DSP num> Clears the fatal error count for the DSP, and returns the DSP to service.

  Note: Regarding the commands **rtpPortCompress** and **rtpPortNonCompress**: some routers can perform header compression on RTP packets which can result in bandwidth savings across the WAN. This header compression is only provided by the router if the packet is a valid RTP packet and if the destination IP Socket is within the port range 16384 upwards.

- **rtpPortCompress** – configure RTP packets to originate from ports 17300 to 17350 RTP Header Compression Range.
- **rtpPortNonCompress** – configure RTP packets to originate from ports 2300 (Default).

Appendix F: Configure a Netgear RM356 modem router for remote access

Contents

This section contains information on the following topics:

Introduction

Management and support of the IP Trunk 3.01 (and later) network depends on IP networking protocols including SNMP, FTP, and Telnet. A modem router should be installed on the system site ELAN subnet to provide remote support access for ITG and other IP-enabled Nortel products. The Nortel Netgear RM356 modem router integrates the functions of a V.90 modem, a PPP remote access server, an IP router, and a 4-port 10BaseT Ethernet hub, and provides a range of security features that can be configured to comply with the customer's data network security policy.

Note: Do not install a modem router on the ELAN subnet without the explicit approval of the customer's IP network manager. The RM356 modem router is not secure unless it is configured correctly, according to the customer's network security policy and practices.

Security features of the RM356 modem router

Security features of the RM356 modem router are as follows:

- Password Authentication Protocol (PAP) for dial-in PPP connection
- RM356 manager password
- CLID for dial-in user authentication (requires CO line with Calling Line ID)
- Callback for dial-in user authentication
- Dial-in user profiles
- Static IP routing
- IP Packet Filtering
- Idle time-out disconnect for dial-in PPP connection

Install the RM356 modem router

Follow the steps in Procedure 77 on page 607 to install the RM356 router.

Procedure 77
Installing the RM356 modem router

1. Place the modem router at a conveniently visible and physically secure location near an ac power outlet, an analog telephone line, and 10BaseT Ethernet cables. Up to four hosts or hubs can be connected to the integrated 10BaseT hub in the rear of the RM356 modem router. Use shielded CAT 5 10BaseT Ethernet cables to connect the modem router to the Management interface of a maximum of four IP trunk cards. Other IP-enabled Nortel products on the ELAN subnet can be connected to the RM356 modem router, including the Meridian 1/CS 1000M, a local OTM PC, Symposium Call Center Server, and CallPilot.

   Note: The up-link connection to an additional ELAN hub or optional TLAN network interface gateway requires either a cross-over 10BaseT Ethernet cable, or a special up-link port on the 10BaseT hub to which the RM356 is connected.

2. When the modem router is connected to the AC power source, the power LED is lit. After several seconds, the test LED flashes slowly four times, then stays off. For each of the four 10BaseT ports on the integrated hub there is a link/data LED that is lit steadily to indicate a good received link if there is a cable connection to a host or hub that is powered up, or flashing to indicate data has been received on the LAN.

3. Connect the RJ-45 plug end of the local manager cable to the RS-232 Manager port RJ-45 jack on the rear of the modem router. Connect the other end of the cable to an RS-232 terminal or PC COM port configured for the following communication parameters:

   - 9600 bps
   - 8
   - none
   - 1

   The local maintenance cable connects directly to data terminal equipment (DTE).

4. The analog telephone line should be a CO line or a PBX extension with a Direct Inward Dialing (DID) number if that is in compliance with the customer's network security policy.

End of Procedure

Configure the OTM PC to communicate with a remote system site through a modem router

If the customer's version of OTM does not support the modem router communication profile for Meridian 1/CS 1000M system types, work around the limitation by configuring a Dial-up Networking (DUN) session under Windows to connect to the modem router at a particular system site.

In the OTM Navigator, configure the system communication profile as "Ethernet." Establish the Dial-up Networking session from Windows before attempting to connect to the system from the OTM Navigator. IP Trunk 3.01 (and later) nodes on the same ELAN subnet are also accessible over the same Dial-up Networking connection to the modem router.

Configure the RM356 modem router through the manager menu

Configuring the RM356 modem router by the manager menu can be completed from a TTY or PC connected to the local RS-232 manager port on the rear of the modem router. Alternatively, the manager menu can be accessed by Telnet after the IP addressing and routing have been set up initially from the local manager port.

> ***Note:*** The arrow keys navigate in the RM356 manager menu. The spacebar key toggles pre-defined configuration values for a field. The Enter key saves data changes to ROM and exits the current menu. The Esc key exits the current menu without saving changes. Enter the menu selection number, when prompted, to display a sub-menu, configuration form, or command prompts.

Follow the steps in Procedure 78 to configure the RM356 modem router through the manager menu.

Procedure 78
Configure the RM356 modem router through the manager menu

1 Press the **Enter** key.

The 'Enter Password:' prompt is displayed for 10 seconds.

2 Enter the default RM356 manager password: **1234**

The "RM356 Main Menu" appears.

3 Enter menu selection number 1 to access "General Setup" under the "Getting Started" section of the "RM356 Main Menu."

“Menu 1 – General Setup” is displayed.

4 Type in the system name (19 characters, no spaces), location, and contact person's name for the system site. Use the up and down arrow keys to move the cursor to the prompt “Press ENTER to Confirm or ESC to Cancel:” at the bottom of the menu. Press **Enter** to confirm and save data to ROM.

5 Enter menu selection number 2 under the "Getting Started" section.

“Menu 2 – Modem” is displayed.

6 Type in modem name. Set “Actives”. Use arrow keys to navigate and space bar to toggle values. Set “Direction=Incoming”. Type in the modem router's telephone number for reference. Press **Enter** to confirm and save data to ROM.

7 Enter menu selection number 3, "Ethernet Setup", under the "Getting started" section.

“Menu 3 – Ethernet Setup” sub-menu is displayed.

8 Enter menu selection 2, "TCP/IP and DHCP Setup".

“Menu 3.2 – TCP/IP and DHCP Ethernet Setup” is displayed.

9 Use the space bar to toggle “DHCP=None”.

10 Under “TCP/IP Setup”, type in the IP address and the IP subnet mask for the modem router's ELAN network interface.

11 Toggle “RIP Direction=None”. Press **Enter** to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

12 Enter menu selection number 12, "Static Routing Setup", under the "Advanced Applications" section.

“Menu 12 – Static Route Setup” sub-menu is displayed.

Note 1: If firewall security is properly configured in the customer's Management Gateway router, and if the modem router is permitted access over the TLAN subnet to other IP Trunk 3.01 (and later) nodes on remote ELAN subnets, define a default network route pointing to the Management Gateway IP address on the local ELAN subnet. Alternatively, define up to four different static network routes or host routes in the modem router to limit routing access from the modem router to the TLAN subnet.

Note 2: To prevent access from the modem router to the TLAN subnet through the Management Gateway router on the ELAN subnet, disable RIP by setting “RIP Direction=None”, and remove all static routes or disable a particular static route by setting “Active=No”.

13 Enter menu selection number 1 to edit the first static route.

“Menu 12.1 – Edit IP Static Route” is displayed.

14 Type in a descriptive route name, for example, “DefaultGW” (no spaces). Toggle “Active=Yes/No” for security purposes. The destination IP address can be the default network route “0.0.0.0”, or a specific network or host route for greater security. The gateway IP address is the Management Gateway IP address on the ELAN subnet where the modem router is connected. Press **Enter** to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

15 Enter menu selection number 13, "Default Dial-in Setup", under the "Advanced Applications" section.

“Menu 13 – Default Dial-in Setups” is displayed.

16 Under “Telco Options” toggle “CLIDAuthen=None/Preferred/Required”.

CLID requires a CO line subscribed for CLID service where available. “Preferred” means some dial-in user profiles might require CLID, but others may not. “Required” means no dial-in call is connected unless CLID is provided and user profiles require CLID for authentication.

Under “PPP Options” toggle “Recv Authen=PAP”. Windows 9x Dialup Networking (DUN) is not compatible with CHAP/PAP or CHAP on the modem route; calls are disconnected after a few minutes.

Toggle “Compression=No”. Windows 9x DUN is not compatible with software compression on the modem router: calls are randomly disconnected.

Toggle “Mutual Authen=No”.

Under “IP Address Supplied By:”, toggle “Dial-in User=No”, “IP Pool=Yes”. For “IP Start Addr=” type in the ELAN network interface IP address that will be assigned to the Dialup Networking (DUN) PPP client on the remote OTM PC.

Note: The remote OTM PC receives this ELAN network interface IP address whenever DUN makes a dial-in PPP connection to the modem router. As long as DUN remains connected to the modem router, IP applications on the remote OTM PC function as if the PC were located on the customer's ELAN subnet.

Under “Session Options”, configure input and output filter sets according to the customer's IP network security policy and practices. The default setting is “no filter sets”. Set “Idle Timeout=1200” seconds to provide 20 minutes idle time-out disconnect for remote support purposes.

Press **Enter** to confirm and save data to ROM.

17 Enter menu selection number 14, "Dial-in User Setup", under the "Advanced Applications" section.

“Menu 14 – Dial-in User Setup” is displayed.

Note: Up to eight dial-in user profiles can be defined according to the customer's network security policy.

18 Enter menu selection 1 to edit the first dial-in user profile.

“Menu 14.1 – Edit Dial-in User” is displayed.

19 Type in the user name. Toggle “Actives/No” for security purposes. Type in a password for PAP. The DUN client on the remote OTM PC must provide the user name and password defined here when dialing up the modem router.

Set “Callbacks/No” according to the customer's network security policy and practices. Nortel Customer Technical Services (CTS), does not currently accept callback security calls from the modem router.

Set “Rem CLID=” to the PSTN Calling Number that is displayed when the remote OTM PC dials up the modem router, if CLID authentication is required for the user profile. CLID depends on providing a CO line subscribed for CLID service for the modem router's telephone line connection.

Set "Idle Timeout=1200" seconds to provide 20 minutes idle timeout disconnect for Nortel remote support purposes.

Press **Enter** to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

20 Enter menu selection number 23 to access "System Password" under the "Advanced Management" section of the "RM356 Main Menu."

“Menu 23 – System Password” is displayed.

21 Type in the old password and new password, then retype the new password to confirm. Never leave the RM356 system manager password defaulted to 1234 after the modem router has been installed and configured on the ELAN subnet. The modem router's security features are worthless if the manager password is not changed regularly according to good network security practices.

End of Procedure

RM356 modem router manager menu

This section displays the various menus of the RM356 modem router (application notes on the ELAN subnet installation):

```
                         RM356 Main Menu

     Getting Started                       Advanced Management
       1. General Setup                 21. Filter Set Configuration
       2. MODEM Setup
       3. Ethernet Setup                  23. System Password
       4. Internet Access Setup           24. System Maintenance

     Advanced Applications
       11. Remote Node Setup
       12. Static Routing Setup
       13. Default Dial-in Setup
       14. Dial-in User Setup                  99. Exit

                     Enter Menu Selection Number:
```

```
           Menu 1 - General Setup

  System Name= Room_304_RCH_Training_Center
  Location= Sherman Ave., Richardson, TX
Contact Person's Name= John Smith, 972 555-1212

  Press ENTER to Confirm or ESC to Cancel:

         Menu 2 - MODEM Setup

  Modem Name= MODEM
  Active= Yes
  Direction= Incoming
  Phone Number=
  Advanced Setup= No
  Press ENTER to Confirm or ESC to Cancel:

           Menu 3 - Ethernet Setup

  1. General Setup
  2. TCP/IP and DHCP Setup

        Enter Menu Selection Number:

      Menu 3.1 - General Ethernet Setup

  Input Filter Sets= 2
  Output Filter Sets=

  Press ENTER to Confirm or ESC to Cancel:

  Menu 3.2 - TCP/IP and DHCP Ethernet Setup

  DHCP Setup:
    DHCP= None
    Client IP Pool Starting Address= N/A
```

```
                      Size of Client IP Pool= N/A
                      Primary DNS Server= N/A
                      Secondary DNS Server= N/A

                    TCP/IP Setup:
                      IP Address= 47.177.16.254
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= None
                        Version= RIP-2B

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.


                          Menu 12 - Static Route Setup

                    1. DefaultGW
                    2. ________
                    3. ________
                    4. ________

                          Enter Menu Selection Number:

                        Menu 12.1 - Edit IP Static Route

                    Route #: 1
                    Route Name= DefaultGW
                    Active= Yes
                    Destination IP Address= 0.0.0.0
                    IP Subnet Mask= 0.0.0.0
                    Gateway IP Address= 47.177.16.1
                    Metric= 2
                    Private= No

                    Press ENTER to Confirm or ESC to Cancel:
                         Menu 13 - Default Dial-in Setup

     Telco Options:                      IP Address Supplied By:
       CLID Authen= None                    Dial-in User= No
                                            IP Pool= Yes
    PPP Options:                         IP Start Addr= 47.177.16.253
       Recv Authen= PAP
       Compression= No                        Session Options:
       Mutual Authen= No                        Input Filter Sets=
         PAP Login= N/A                         Output Filter Sets=
         PAP Password= N/A                      Idle Timeout= 1200

     Callback Budget Management:
       Allocated Budget(min)=
       Period(hr)=

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                          Menu 14 - Dial-in User Setup

                    1. itgadmin
                    2. ________
                    3. ________
                    4. ________
                    5. ________
                    6. ________
                    7. ________
                    8. ________

                          Enter Menu Selection Number:

                          Menu 14.1 - Edit Dial-in User
                    User Name= itgadmin
                    Active= Yes
                    Password= ********
                    Callback= No
                      Phone # Supplied by Caller= N/A
                      Callback Phone #= N/A
                    Rem CLID=
                    Idle Timeout= 500

                    Press ENTER to Confirm or ESC to Cancel:
```

```
                       Menu 21 - Filter Set Configuration

     Filter                                Filter
     Set #        Comments                 Set #        Comments
    ------  -----------------            ------  -----------------
       1      NetBEUI_WAN                   7      _______________
       2      NetBEUI_LAN                   8      _______________
       3      _______________               9      _______________
       4      _______________              10      _______________
       5      _______________              11      _______________
       6      _______________              12      _______________


                    Enter Filter Set Number to Configure= 0

                    Edit Comments=

                    Press ENTER to Confirm or ESC to Cancel:
                      Menu 21.1 - Filter Rules Summary

# A Type                      Filter Rules                      M m n
- - ---- ----------------------------------------------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0           N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=138, DA=0.0.0.0           N D N
3 Y IP   Pr=17, SA=0.0.0.0, SP=139, DA=0.0.0.0           N D N
4 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0            N D N
5 Y IP   Pr=6, SA=0.0.0.0, SP=138, DA=0.0.0.0            N D N
6 Y IP   Pr=6, SA=0.0.0.0, SP=139, DA=0.0.0.0            N D F

                Enter Filter Rule Number (1-6) to Configure:
```

```
                          Menu 23 - System Password

                  Old Password= ?
                  New Password= ?
                  Retype to confirm= ?

                   Enter here to CONFIRM or ESC to CANCEL:
```

```
                        Menu 24 - System Maintenance

                       1.  System Status
                       2.  Terminal Baud Rate
                       3.  Log and Trace
                       4.  Diagnostic
                       5.  Backup Configuration
                       6.  Restore Configuration
                       7.  Software Update
                       8.  Command Interpreter Mode
                       9.  Call Control

                        Enter Menu Selection Number:
```

```
                    Menu 24.1 -- System Maintenance - Status

Port Status   Speed  TXPkts  RXPkts  Errs  Tx B/s  Rx B/s   Up Time
 1    Idle    0Kbps   16206   12790     0       0       0   0:00:00

     Total Outcall Time:     0:00:00

     Ethernet:                    Name: Room_304_RCH_Traini
       Status:  10M/Half Duplex  RAS S/W Version: V2.13 | 9/25/98
      TX Pkts: 135579          Ethernet Address:00:a0:c5:e0:5b:a6
       RX Pkts: 662866
       Collisions: 49

     LAN Packet Which Triggered Last Call:

                                Press Command:

            COMMANDS: 1-Drop Port 1  9-Reset Counters   ESC-Exit
```

```
    Menu 24.2 -- System Maintenance - Change Terminal Baud Rate

Terminal Baud Rate: 9600

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
                 Menu 24.3 == System Maintenance - Log and Trace

                    1. View Error Log
                    2. Syslog and Accounting

                             Please enter selection:

   0     179754 PINI  INFO  SMT Session End
   1     179761 PP09  INFO  Password pass
   2     179761 PINI  INFO  SMT Session Begin
```

```
  3     179763 PINI  INFO  SMT Session End
  4     179772 PP09  INFO  Password pass
  5     179772 PINI  INFO  SMT Session Begin
  6     179775 PINI  INFO  SMT Session End
  7     179783 PP09  INFO  Password pass
  8     179783 PINI  INFO  SMT Session Begin
  9     179788 PINI  INFO  SMT Session End
 10     179796 PP09  INFO  Password pass
 11     179796 PINI  INFO  SMT Session Begin
 12     179798 PINI  INFO  SMT Session End
 13     179812 PP09  INFO  Password pass
 14     179812 PINI  INFO  SMT Session Begin
 15     179815 PINI  INFO  SMT Session End
 16     179830 PP09  INFO  Password pass
 17     179830 PINI  INFO  SMT Session Begin
 18      179834 PINI  INFO  SMT Session End
```

```
      Menu 24.3.2 -- System Maintenance - Syslog and Accounting

                 Syslog:
                 Active= No
                 Syslog IP Address= ?
                 Log Facility= Local 1

                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
                Menu 24.4 - System Maintenance - Diagnostic

     MODEM                                System
       1.  Drop MODEM                       21. Reboot System
       2.  Reset MODEM                      22. Command Mode
       3.  Manual Call
       4.  Redirect to MODEM
```

```
TCP/IP
  11. Internet Setup Test
  12. Ping Host

                     Enter Menu Selection Number:

               Manual Call Remote Node= N/A
               Host IP Address= N/A

           Menu 24.7 -- System Maintenance - Upload Firmware

               1. Load RAS Code
               2. Load ROM File

                    Enter Menu Selection Number: 1
```

Appendix G: Upgrade an ITG Trunk 1.0 node to support ISDN signaling trunks

Contents

This section contains information on the following topics:

This Appendix is included as a reference for ITG Trunk 1.0 customers who wish to upgrade their systems to ITG Trunk 2.0 to include ISDN Signaling Link (ISL) capabilities. An upgraded ITG Trunk 2.0 node can support ITG 8-port and ITG-Pentium 24-port trunk cards in the same node. All ITG 8-port trunk cards in a node must be upgraded to ITG/ISL software. ITG Trunk 2.0

also supports inter-working between ITG Trunk 2.0 nodes and ITG Trunk 1.0 (Basic Trunk) nodes in the same network.

IP Trunk 3.01 (and later) cannot be installed on an ITG 8-port trunk card. However, IP Trunk 3.01 (and later) can interwork with ITG Trunk 2.0 nodes. IP Trunk 3.01 (and later) does **not** interwork with ITG Trunk 1.0 nodes.

Upgrade procedure summary

1. If required, select at least one ITG 8-port trunk card to support DCHIP functionality. In some cases, a new ITG-Pentium 24-port trunk card supports DCHIP functionality.
2. Install the DCHIP PC Card and pigtail cable in the selected ITG 8-port trunk card.
3. Remove all ITG Trunk 1.0 software and configuration files from the ITG 8-port trunk cards.
4. Install new ITG/ISL Trunk software on the ITG 8-port trunk cards.
5. Remove ITG 1.0 configuration data the system.
6. Configure the upgraded cards as if performing a new ITG-Pentium 24-port trunk card installation.

   Note: When a node includes both ITG 8-port trunk cards and ITG-Pentium 24-port trunk cards, all ITG 8-port trunk cards must be upgraded to the ITG Trunk 2.0 software. The standard configuration is to have the ITG-Pentium 24-port trunk card support the DCHIP functionality.

Before you begin

Procedure 79 on page 623 describes how to prepare for an upgrade. The steps can be accomplished in any order. The list is numbered for convenience.

Procedure 79
Preparing for an upgrade

1 Upgrade to OTM 2.1 (and later) or later. Make sure all the ITG and Alarm Management applications are installed.

2 Upgrade Meridian 1 software to Release 25 or later. ITG/ISL Trunks require Packages 145 (ISDN) and 147 (ISL). Install additional software packages, such as Package 148 NTWK, as required for advanced ISDN features. Table 3 on page 56 lists required software packages.

3 Check the Nortel website to find the latest ITG 8-port trunk card software. Go to www.nortel.com. Follow the links to Customer Support and Software Distribution or go to www.nortel.com/support.

The file to download is for the ITG 2.8.xx.mms. “ITG 2” indicates it is ITG Trunk 2.0 software, “8” indicates it is for the ITG 8-port trunk card, and “xx” is the software revision level.At the time of release of IP Trunk 3.01 (and later), the latest version of software was for the ITG 8-port trunk card was ITG 2.8.26g.

WARNING

It is critical that only the ITG 8-port trunk card software is installed on the ITG 8-port trunk cards. If the ITG-Pentium 24-port software is installed, the ITG 8-port trunk card becomes unusable and must be returned to Nortel for repair.

4 If ITG-Pentium 24-port trunk cards are added to the ITG 8-port trunk card node as part of the upgrade, verify that the required LAN networking equipment and cables are installed. For networking equipment requirements, refer to “ITG engineering guidelines” on page 125. Leader 0 and Leader 1 must be on the same TLAN subnet.

5 If an ITG 8-port trunk card is being upgraded to support DCHIP functionality, one hardware upgrade kit (NTZC47AA for Large systems, and NTZC47BA for Small systems) is required. Both kits contain a DCH PC Card (NTWE07) a pigtail cable (NTCW84EA) and two versions of the I/O panel breakout cable. The NTZC47AA contains a D-Channel interface cable (NTND26AA) that extends from a 15-pin filter in the I/O panel to the MSDL card. The NTZC47BA contains an external D-Channel cable (NTWE04AD) to connect to the I/O breakout cable on the SDI/DCH card.

6 Open a Telnet session to the ITG 8-port trunk card. At the ITG> prompt, enter

itgCardShow

Write down the IP trunk card's IP address and other card data.

7 If required for an ITG 8-port trunk card upgrade, install an MSDL card (minimum vintage NT6D80) or SDI/DCH card (minimum vintage NTAK02BB). Be sure to install the I/O panel breakout cable for the SDI/DCH card. If cards are in place, make sure each card has an available port.

8 Verify that the customer site has a Nortel Netgear RM356 Modem Router (or equivalent) on the ELAN subnet. The modem router provides remote support access to ITG Trunk and other IP-enabled Nortel products.

9 Identify the TNs of the ITG 8-port trunk cards that are to be upgraded. Open the **OTM ITG Meridian 1 IP Trunk** main window. The TNs are listed.

End of Procedure

Install the DCHIP hardware upgrade kit

Follow the steps in Procedure 80 on page 625 to upgrade an ITG Trunk 1.0 node by installing at least one ITG 8-port trunk card DCHIP hardware upgrade kit.

> ***Note:*** Skip this step if the DCHIP functionality is provided by an ITG-Pentium 24-port trunk card.

Procedure 80
Installing the DCHIP hardware upgrade kit

1 Disable all ITG 8-port trunk cards in the node to be upgraded. Disable the cards in LD 32 (DISI l s c for Large systems, DISI c for Cabinet systems). Wait for the NPR0011 message, which indicates that all units on each card are disabled.

CAUTION WITH ESDS DEVICES

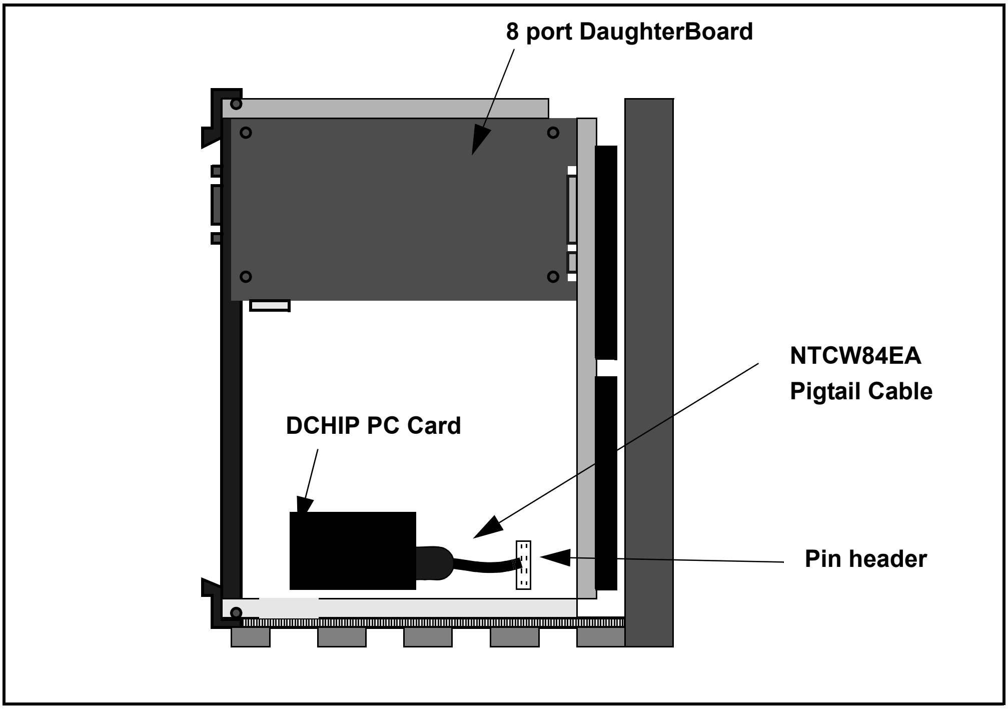
Whenever working on the trunk card, be sure to wear an anti-static wrist strap

2 Select the card in which the DCHIP hardware upgrade kit is to be installed. Disconnect the TLAN cable from faceplate (NTCW80AA only) and label the cables for reconnection. Remove the trunk card from the shelf or cabinet. Place card on a static-safe surface. Avoid touching electronic components.

3 Install the NTWE07AA DCHIP PC Card into the internal PC Card slot on the ITG 8-port trunk card that has been selected to provide the DCHIP function. See Figure 155 on page 626.

4 Connect the NTCW84EA pigtail cable from port 0 of the DCHIP PC Card to the J14 pin header on the motherboard of the DCHIP card (see Figure 155 on page 626). The cable routes the D-Channel signals to the backplane and the I/O panel. The PC Card connector is keyed to allow insertion only in the correct direction. The J14 pin header connector is not keyed. Be careful to align the connector with the pin header.

Figure 155
DCHIP PC Card and NTCW84EA pigtail cable



5 Pull the top and bottom locking devices away from the trunk card faceplate. Insert the trunk card into the card slots and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

End of Procedure

Install the DCHIP I/O Panel breakout cable from the upgrade kit

The breakout cable provides one D-channel connector.

If installing the DCHIP upgrade kit for the NTCW80AA ITG 8-port trunk card, use the NTCW84MA I/O Panel breakout cable.

If installing the DCHIP upgrade kit for the NTCW80CA ITG 8-port trunk card, use the NTCW84LA I/O Panel breakout cable.

Procedure 81
Installing the DCHIP I/O Panel breakout cable from the upgrade kit

1. For the Large System, locate the I/O connector that corresponds to the leftmost card slot of the ITG 8-port trunk card that is undergoing the hardware upgrade.
2. Disconnect existing ELAN network interface and serial cables. Remove the existing I/O panel breakout cable.
3. Install the new cable (NTCW84LA or NTCW84MA). Be sure to use the screw provided.
4. Reconnect ELAN network interface and serial connectors. For NTCW80CA cards, install a shielded TLAN cable.
5. Turn to “Install filter and NTND26 cable (for MSDL and DCHIP cards in same Large System equipment row)” on page 270 to install the DCHIP connector and MSDL cable.

End of Procedure

Upgrade the ITG 8-port trunk card ITG basic trunk software to ITG/ISL trunk software

Use the OTM ITG Basic Trunk application to perform this procedure. Once OTM has been upgraded to 6.6 or later, all the configuration data for the ITG trunk node will have been converted.

Step 1 - Remove ITG Trunk 1.0 configuration files

Follow the steps in Procedure 82 on page 628 to remove the ITG 1.0 Trunk configuration files from the TABLE, BOOTP and CONFIG directories of every card in the node to be upgraded.

Procedure 82
Removing the ITG Trunk 1.0 configuration files

1 From the **OTM IP Telephony Gateway - ISDN IP Trunk** Main window, select the card from the lower half of the window and right-click. A context menu appears. Select **Telnet to ITG card.** OTM automatically launches a Telnet session to the selected card.

2 Login to the ITG shell. At the ITG> prompt, enter **setLeader setLeader "xxx.xxx.xxx.xxx", "yyy.yyy.yyy.yyy", "zzz.zzz.zzz.zzz"**

where:

- "xxx.xxx.xxx.xxx" is the ELAN network interface IP address of Leader 0,
- "yyy.yyy.yyy.yyy" is the ELAN network interface gateway (router) IP address. If the OTM PC is connected locally to the LAN, and there is no ELAN network interface gateway, then the gateway IP address is "0.0.0.0".
- "zzz.zzz.zzz.zzz" is the subnet mask for the ELAN network interface IP address of Leader 0.

Note 1: All ITG shell commands are case-sensitive. A space separates the command from the first parameter. The three parameters must each be enclosed in quotation marks, and there must be a comma and no spaces separating the three parameters.

Note 2: The **Management Gateway (router) IP address** is used on reboot to create the IP route table default network route only if
(1) there is no active leader that has this card's ELAN network interface MAC address in its node properties file, and
(2) this card's node properties file is empty (size 0 Kb).

Note 3: IP addresses and subnet masks must be entered in dotted decimal format.

Note 4: If the network administrator has provided the **subnet mask** in CIDR format, convert it to dotted decimal format before entering it. For example: 10.1.1.1/20 must be converted to IP address 10.1.1.1 with subnet mask 255.255.240.0. To convert subnet mask from CIDR format to dotted decimal format refer to "Subnet mask conversion from CIDR to dotted decimal format" on page 601.

3 Press **Enter**.

4 The ITG shell displays value = 0 = 0 x 0 to indicate successful completion of the **setLeader** command. If the ITG shell displays **command not found**, check the spelling of the command. If the ITG shell displays a value of –1, contact Nortel customer technical support.

5 Return to the **OTM IP Telephony Gateway - ISDN IP Trunk** Main window.

6 Telnet to Leader 1 and Follower cards in the node.

7 Log into the ITG shell.

At the ITG>prompt, enter **clearLeader “xxx.xxx.xxx.xxx”, “yyy.yyy.yyy.yyy”, ”zzz.zzz.zzz.zzz”**
(see notes in step 2). The ITG shell outputs value = 0 = 0 x 0 to indicate successful completion of the **clearLeader** command.

Note: Enter **clearLeader** command even when removing configuration files from Follower cards.

End of Procedure

Step 2 - Transmit ITG Trunk 2.0 software to the ITG 8-port trunk cards

Follow the steps in Procedure 83 to transmit the ITG Trunk 2.0 software to the ITG 8-port trunk cards.

Procedure 83
Transmitting ITG Trunk 2.0 software to the ITG 8-port trunk cards

1 Launch OTM 2.1 (and later). Double-click **ITG Meridian 1 IP Trk** in the Services folder.

2 In the **IP Telephony Gateway** window, select Leader 0 from the ITG trunk node that is being upgraded.

3 Select menu **Configuration > Synchronize > Transmit**. The **ITG-Transmit Options** window appears.

4 Make sure to set the radio button to **Transmit to selected nodes**. Check the **Card Software** check box only.

5 Locate the ITG28xx.mms software file on the OTM PC. If the path to the ITG28xx.mms software file is known, type the path information in the **Software** field. Or click the **Browse** button to find and select the file. Click the **Open** button in the Browser so that the software path and filename appear in the **Software** field in the I**TG-Transmit options** window.

6 Click the **Start Transmit** button.

Monitor progress in the **Transmit control** window. Confirm that the card software is transmitted successfully to all the ITG 8-port trunk cards. The window identifies the cards by their TNs.

If the message in the control window indicates the software transmit is unsuccessful, do not press Cancel. Leave the **Transmit Control** window open displaying the location of the software file on OTM.

If the trunk card can be reached by Telnet from OTM, but OTM shows the card status as Not Responding, OTM ITG SNMP MIB is incompatible with the ITG 8-port trunk card software version. In this case, the software upgrade must be executed from the ITG shell CLI of each ITG 8-port trunk card in the node (see step a, and Figure 156 on page 631).

a. ITG> swDownload “IP address of OTM PC”, “itguser”, “obtuser”, ” “,”ITG28xx.mms” where xx indicates the latest version of the ITG Trunk 2.0 software for the ITG 8-port trunk card.

Note: Be sure to hit the space bar after typing in swDownload. Enter the quotation marks and commas exactly as described in the step a and as shown in Figure 156 on page 631.

7 Reset the card. There are three ways to do this:

a. From the **IP Telephony Gateway** Main window, double-click each card to open the Card Properties. Click the **Reset** button if the trunk card is showing responding. Close the Card Properties and go to the next card in the list.

b. If the card is showing “Not responding”, Telnet to the card and enter the following command:

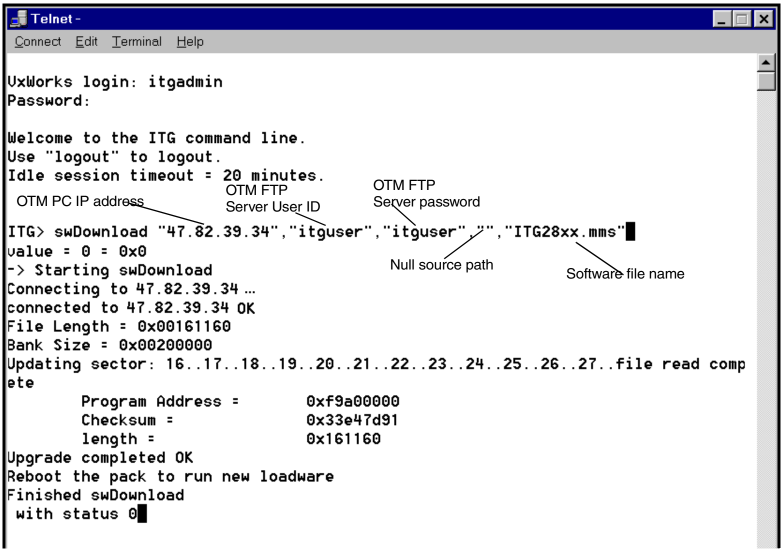
ITG> card Reset

c. Press the **Reset** button on the trunk card faceplate.

The trunk card faceplate shows T.20 in the maintenance display window.

8 At this point, the trunk cards have ITG 2.0 ISDN functionality and are in the state of new ITG 8-port trunk cards that need to be configured. Refer to “Configure IP Trunk 3.01 (and later) data” on page 290.

Figure 156
Software download example



```
UxWorks login: itgadmin
Password:

Welcome to the ITG command line.
Use "logout" to logout.
Idle session timeout = 20 minutes.

ITG> swDownload "47.82.39.34","itguser","itguser","","ITG28xx.mms"
value = 0 = 0x0
-> Starting swDownload
Connecting to 47.82.39.34 ...
connected to 47.82.39.34 OK
File Length = 0x00161160
Bank Size = 0x00200000
Updating sector: 16..17..18..19..20..21..22..23..24..25..26..27..file read comp
ete
        Program Address =       0xf9a00000
        Checksum =              0x33e47d91
        length =                0x161160
Upgrade completed OK
Reboot the pack to run new loadware
Finished swDownload
 with status 0
```

9 To verify the software upgrade on Leader 0, telnet to the IP address of the Leader 0 card. Leader 0 is the only card that has an IP address configured at this stage of the upgrade. Enter the following command:

ITG> **swVersionShow**

10 Configure the ITG Trunk 2.0 data on the OTM ITG ISDN IP Trunk application. See “Configure IP Trunk 3.01 (and later) data in OTM 2.1 (and later)” on page 316.

11 Transmit configuration data to the upgraded ITG 8-port trunk cards using normal ITG Trunk 2.0 installation procedures.

12 Upgrade Meridian 1 to Release 25 software.

End of Procedure

Remove ITG Trunk 1.0 configuration data from Meridian 1

Follow the steps in Procedure 84 to remove the ITG Trunk 1.0 configuration data from Meridian 1.

Procedure 84
Removing the ITG Trunk 1.0 configuration data from Meridian 1

1 Out existing ITG basic trunks that are being upgraded to ITG ISL trunks:

  a. Identify TNs of trunks that are to be outed. Look in OTM ITG ISDN IP Trunks application for ITG trunks or, in LD 21, request an LTN of existing basic ITG TIE trunk route. The LTN gives a list of every single unit. Observe if there are 8 or 4 TNs on the same card. Note which units are on each card and which is the starting unit. Count the number of units on each card. If using the G.729 codec, there might only be four units on the card.

  b. Load LD14 and out the cards one at a time. Enter OUT x, where x is the number of units on each card and TN = y, where y is the lowest unit on the card. Give the starting unit on the card.

  c. When all the trunks on the LTN of the basic ITG trunk TIE route have been outed, then out the Route Data Block.

2 Out the Route Data Block for ITG basic trunks. Use LD 16. REQ = OUT. When prompted for the customer number and route number, press **Enter**. The Route Data Block is then deleted.

End of Procedure

Configure the Meridian 1 ITG/ISL trunk data

Upgrade considerations

If leaving the ITG 8-port trunk cards in the same card slots, use the same card TNs and route number when building the new ITG/ISL Trunk Route.

To re-use the same ESN route list blocks and the ESN translation tables, then use the same route number when building the new ITG ISL TIE route and the RLB entries will still be correct.

Remember to make certain changes to the RLB entry in LD 86. For the ITG/ISL TIE Trunk Route, configure SBOC = RRA to enable Fallback routing to circuit-switched trunks.

In ITG Trunk 2.0, the digit manipulation tables are not required to reinsert AC1 or AC2. Therefore, change the DMIs accordingly.

Verify customer data block (see "LD 15 – Configure ISDN feature in Customer Data Block" on page 296). See "LD 17 – Configure the ISL D-channel for the DCHIP card (Large Systems)" on page 290 or "LD 17 – Configure the ISL D-channel for the DCHIP card (Small Systems)" on page 292, as appropriate.

Follow the steps in Procedure 85 to configure the Meridian 1 ITG/ISL trunk data.

Procedure 85
Configuring the Meridian 1 ITG/ISL trunk data

1. Build a new route data block for the ITG/ISL trunks using the same route number. Set INAC=YES in the Route Data Blocks (RDB) for the ITG ISL routes at all Meridian 1 ESN nodes. See "LD 16 – Configure the IP Trunk 3.01 (and later) TIE Trunk Route Data Block" on page 297.

   Note: Any references to the ITG trunk route number in ESN route list blocks will still be valid when completed.

2. Use LD 14 to add ISL trunks to the new ISL route. See "LD 14 – Configure Media Card 32-port and ITG-Pentium 24-port trunk cards and units" on page 302 for more information.

3. In LD 14, at prompt **REQ**, enter **new 8**.

   Note: Perform this configuration on a card-by-card basis.

4. At prompt, **XTRK**, specify **itg2.**

5. In LD 14, at prompt **MAXU**, enter **8**.

6. Look at the OTM dialing plan. Go to LD 90 and determine which RLBs are used for ITG translations that are used for ITG destinations. Print NPA, Nxx or LOC.

7 In LD 86, remove digit manipulation and print out RLBs. Do not use ESN digit manipulation tables for the ITG ISL Trunks.

Note: Determine which RLBs are used for the ITG trunks. Note which ESN translations are using the ITG RLB.

8 Inspect entries in the RLB.

9 Find the entry that refers to ITG basic trunk route.

10 Under those entries, find the DMI and record it.

11 Remove the DMIs that were previously used for ITG basic trunks.

End of Procedure

Verify ROM-BIOS version

When the ITG trunk card is reset, it displays a series of startup messages on the local TTY. Verify that the ROM-BIOS is 1.1 or greater. If not, contact Nortel technical support.

Upgrade Troubleshooting

This section provides two procedures to correct OTM upgrade problems.

OTM cannot refresh view (card not responding)

If OTM cannot see card status through refresh, but the card can be Telnetted from OTM, the OTM version is incompatible with the ITG 8-port trunk card software.

How to upgrade software using the ITG shell

Use Procedure 86 on page 635 if OTM displays a Card status of Not Responding.

Procedure 86
Upgrading software using the ITG shell

1 Prepare the OTM ITG FTP server to find the software image file when it is requested from the ITG card BIOS shell using the upgrade or swDownload command.

2 Select **Synchronize > Transmit from the OTM ITG ISDN IP Trunk** application Configuration menu.

3 Check the box for Card Software. Browse for the software image file on the OTM PC. When the software image file is found, open it from the Browser so the path and file name appear in the **OTM ITG Transmit** window.

4 Leave the radio button default setting of **Transmit to selected nodes**. Check the **Node Properties**, **Card Properties** and **Dialing Plan** check boxes.

5 Click the **Start Transmit** button.

   Monitor progress in the **Transmit Control** window. Confirm that the Node Properties, Card Properties and Dialing Plan are transmitted successfully to the Leader 0 ITG trunk card TN. At this point, it is normal for transmission to Leader 1 and Follower cards to fail.

6 When the transmission is complete, click the **Close** button.

7 Reboot the Leader 0 ITG trunk card.

End of Procedure

Index

Nortel Communication Server 1000

IP Trunk

Description, Installation, and Operation

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Publication number: 553-3001-363
Document release: Standard 5.00
Date: July 2006
Produced in Canada

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.