Meridian 1

Meridian Internet Telephony Gateway (ITG) Trunk 2.0/ISDN Signaling Link (ISL)

Description, Installation and Operation

Document Number: 553-3001-202
Document Release: Standard 1.00
Date: April 2000

Printed in Canada

Revision history

April 2000

Standard, release 1.00. This is a global document and is issued for X11 Release 25.0x.

Contents

About this guide

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

This guide describes and explains how to engineer, install, configure, administer and maintain a Meridian Internet Telephony Gateway (ITG) Trunk 2.0 system.

The ITG Trunk 2.0 compresses PCM voice, demodulates Group 3 fax, routes the packetized data over a private internet, or intranet and provides virtual analog ISDN signalling link (ISL) TIE trunks between Meridian 1 ESN nodes.

ITG Trunk 2.0 routes voice traffic over existing private IP network facilities with available under-used bandwidth on the private Wide Area network (WAN) backbone.

Description

The Meridian Internet Telephony Gateway (ITG) Trunk 2.0 supports ISDN Signaling Link (ISL) IP trunks on the NT0961 24-port Meridian Internet Telephony Gateway (ITG) trunk card. It also supports ISL IP Trunks on the NTCW80 8-port ITG 1.0 trunk card that have been upgraded with ITG Trunk 2.0 software and hardware.

An ISDN Signaling Link D-channel (ISL DCH) provides DCH connectivity to the Meridian 1 and signaling control for the 24 ports on the card and any additional ports on other ITG Trunk cards in the same node. The DCH connection expands the signaling path between the Meridian 1 and the gateway. ITG allows Meridian 1 systems to be networked using ISDN, while transmitting H.323 signaling and voice over a standard IP protocol stack.

The ITG ISL Trunk compresses voice and demodulates Group 3 Fax. ITG then routes the packetized data over a private IP network for connections between Meridian 1 nodes, bypassing circuit-switched trunking facilities.

The ITG ISL Trunk 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).

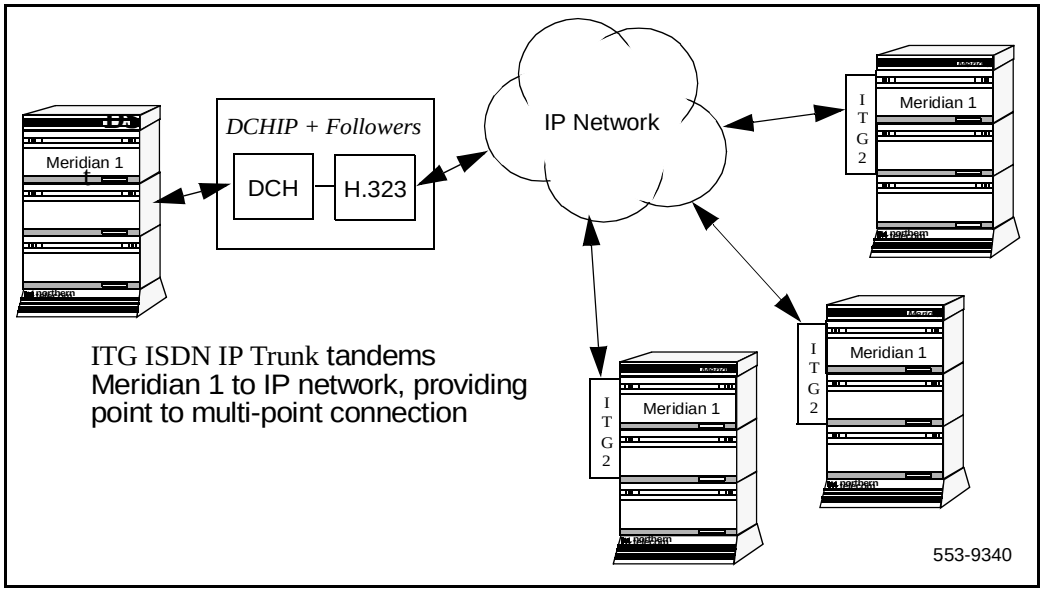
To install the ITG ISL Trunk, the customer must have a corporate IP network with managed bandwidth capacity, and routers available for WAN connectivity between networked Meridian 1 systems. Best VoIP performance is obtained with a QoS-managed network.

LAN connection of the ITG ISL Trunk requires 10BaseT or 100BaseTX Ethernet interfaces for VoIP and 10BaseT for management and D-Channel signaling. There is no restriction on the physical medium of the WAN.

Non-compressing G.711 codecs require 100BaseT Ethernet network connectivity. A 10/100BaseT autosensing Ethernet interface routes the VoIP traffic from the ITG ISL Trunk cards. Signaling between cards and communication with the Meridian Administration Tools (MAT) PC is over a 10BaseT Ethernet connection. The MAT application manages the ITG ISL Trunk.

Figure 1 shows an ITG ISL Trunk configuration example.

Figure 1
ITG ISL Trunk connectivity



Note: In this document, T-LAN refers to the Telephony LAN that transmits the ITG voice and fax traffic. E-LAN (embedded LAN) refers to the management and signaling LAN for the Meridian 1 site.

ITG ISL Trunk 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

ITG is available for Meridian 1 options 11C, 11C Mini, 51C, 61C, 81 and 81C systems running X11 release 25 or later software. See Table 1, “Software packages for Meridian 1 ITG ISL Trunk,” on page 22 for required software packages.

ITG requires MAT 6.6 or later including Alarm Management. MAT Common Services include the Meridian Internet Telephony Gateway applications.

Customers must have the NTAK02BB (minimum vintage) SDI/DCH card (Option 11C) 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.

A modem router must be installed on the E-LAN in order to provide remote support access for ITG Trunk and other IP-enabled Nortel Networks products. The Nortel Networks 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.

Customers with ITG Trunk 1.0 Basic Per Trunk Signaling 8-Port ITG trunk cards have the option of upgrading to ITG Trunk 2.0 ISDN Signaling trunks. Port capacity remains 8 ports per card. 8 and 24-Port cards can be mixed in the same ITG ISL Trunk node. The section “Upgrade an ITG Trunk 1.0 node to support ISDN signaling trunks” on page 235 describes the upgrade.

Table 1
Software packages for Meridian 1 ITG ISL Trunk

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)	263 (large systems)	Optional
QSIG GF Transport (QSIG GF)	305 (large systems)	Optional
Advanced ISDN Network Services (NTWK)	148	Optional
Coordinated Dialing Plan (CDP).	59	Optional
Flexible Numbering Plan (FNP)	160	Optional

List of ITG ISDN components

Table 2 lists ITG ISDN components.

Note 1: MAT 6.6 or later, or OTM 1.0, including the Common Services, Alarm Management, and ITG ISDN applications, is a prerequisite and must be ordered separately.

Note 2: Nortel Networks Netgear RM356 Modem Router or equivalent is required for remote support and must be ordered separately from retail outlets.

Note 3: You must 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. The NT8D81BA is compatible with 10BaseT T-LAN, but if you require a 100BaseT T-LAN, you need to replace it with the NT8D81AA Backplane to I/O Panel ribbon cable assembly.

Table 2
Hardware components for Meridian 1 ITG ISL Trunk (Part 1 of 3)

Component	Product codes
System Packages	
ITG ISDN Signaling Trunk Large Systems Package including D-Channel (NT0961AA 24-Port ITG ISL Trunk with RTU and pre-installed software, I/O cables, DCH PC card, 50-pin I/O Panel Filter connector with ITG specific filtering for 100BaseTX, and NTP)	NTZC44AA A0786079
ITG ISDN Signaling Trunk Small Systems (Option 11C) Package including D-Channel (ITG Trunk 2.0 card with RTU license and pre-installed software that supports 24 ports, required cables, DCH PC card, and NTP)	NTZC44BA A0786080
ITG ISDN Signaling Trunk Small and Large Systems Package without DCH PC Card or NTP	NTZC45AA A0786081

Table 2
Hardware components for Meridian 1 ITG ISL Trunk (Part 2 of 3)

Component	Product codes
Upgrade Packages	
Upgrade Kit for Large Systems from ITG Trunk 1.0 to 2.0 (includes required cables, DCH PC card, and NTP)	NTZC47AA A0786085
Upgrade Kit for Small Systems from ITG Trunk 1.0 to 2.0 (includes required cables, DCH PC card, and NTP)	NTZC47BA A0786086
Spare cards	
Meridian ITG Trunk 2.0 card (24 ports) (NT0961AA 24-Port ITG ISL Trunk with RTU and pre-installed software)	NT0961AA A0786146
Cables	
E-LAN, T-LAN, RS232 and DCH Ports cable for the NT0961AA 24-Port ITG ISL Trunk DCHIP card.	NTCW84KA A0784208
E-LAN, T-LAN, and RS232 Ports cable for the NT0961AA 24-Port ITG ISL Trunk card	NTMF94EA A0783470
E-LAN, T-LAN, RS232 and DCH Ports cable for the NTCW80CA 8-Port ITG ISL Trunk DCHIP card	NTCW84LA A0784437
E-LAN, T-LAN, RS232 and DCH Ports cable for the NTCW80AA 8-Port ITG ISL Trunk DCHIP card	NTCW84MA A0789752
DCH PC Card Pigtail cable	NTCW84EA A0744403
MSDL DCH cable (included in Large System package):	
6 ft.	NTND26AA
18 ft.	NTND26AB
35 ft.	NTND26AC
50 ft.	NTND26AD
50 ft. MSDL DCH Extender cable	NTMF04AB A0774842

Table 2
Hardware components for Meridian 1 ITG ISL Trunk (Part 3 of 3)

Component	Product codes
10 ft. Inter cabinet cable NTCW84KA to SDI/DCH cable	NTWE04AC A0794156
1 ft. Intra cabinet cable NTCW84KA to SDI/DCH cable	NTWE04AD A0794157
Shielded four-port SDI/DCH cable for the NTAK02BB SDI/DCH card (included in Small System package)	NTAK19FB A0403450
PC Maintenance cable (for faceplate RS232 maintenance port to local terminal access)	NTAG81CA A0655007
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 A0783483
Backplane to I/O Panel ribbon cable assembly compatible with NTCW84JA I/O Panel Filter Connector Block with ITG-specific filtering for 100BaseTX T-LAN connection (replaces NT8D81BA Backplane to I/O Panel ribbon cable assembly equipped with non-removable Molded Filter Connectors)	NT8D81AA A0359946
Documentation	
Meridian Internet Telephony Gateway (ITG) Trunk 2.0/ISDN Signaling Link NTP	P0906569
PC Cards	
C7LIU DCH PC Card with Layer 2 DCH Software	NTWE07AA A0794155
ITG Trunk 2.0 24-Port Software Upgrade on 8Mb ATA Flash Rom PC Card	NT0963AA A0786148
ITG Trunk 2.0 8-Port Software Upgrade on 8Mb ATA Flash ROM PC Card	NT0962AA A0786147

Ordering rules and guidelines

Ordering rules for ITG ISL Trunk node initial configuration

Initial configuration of an ITG ISL Trunk node requires either:

- one NTZC44AA ITG ISDN Large Systems package, or
- one NTZC44BA ITG ISDN Small Systems package,

as appropriate for your system. These packages include all Meridian 1 components needed for a single-card node, except for the cables that provide interface to the MSDL and SDI/DCH cards. DCH interface cables are included:

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

The following packages are required for ITG ISL Trunk:

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

MAT 6.6 or OTM 1.1 is required and must be ordered separately. The MAT Alarm Notification application is not included with MAT 6.6 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 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 you are installing ITG ISL Trunk cards in IPE modules equipped with NT8D81BA Backplane to I/O Panel ribbon cable assembly with Molded Filter Connectors, and you are using 100BaseTX T-LAN, order:

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

  Note: You must 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 T-LAN connections.

Ordering rules for ITG ISL Trunk node expansion

To expand an ITG ISL Trunk node requires:

- For each additional non-DCHIP card:
  - — one NTZC45AA ITG ISDN Small and Large Systems Package without DCH PC Card or NTP.
- For each additional DCHIP card, either:
  - — one NTZC44AA ITG ISDN Large Systems Package including D-Channel, or
  - — one NTZC44BA ITG ISDN Small Systems (Option 11C) Package including D-Channel,

  as appropriate for your system. Make sure that there are sufficient DCH ports on the MSDL or SDI/DCH cards and associated cables.

Sparing ratios for ITG Trunk components

Sparing ratios for selected components are as listed in Table 3.

Table 3
Sparing ratios

Component	Sparing ratio
NT0961AA Spare Meridian Trunk ITG 2.0 card (24 ports) (for repair only -- no RTU license)	10:1
NTWE07AA C7LIU DCH PC Card with NTCW84EA PC Card DCH Pigtail cable	10:1
I/O cable assemblies	20:1

ITG ISL Trunk card description

The ITG ISL Trunk card provides a cost-effective solution for high quality voice and fax transmissions over an IP network.

The ITG ISL Trunk card is a two-slot, IPE-based assembly designed for installation in a Meridian 1 IPE shelf. An ITG ISL Trunk card can have a maximum of 24 ports. A Peripheral Component Interconnect (PCI)-based DSP daughterboard provides voice processing and installs on the assembly. The daughterboard compresses speech into packets and supplies the packets to the IP network using a Pentium host processor.

The ITG ISL Trunk card monitors the IP network for delay (latency) and packet loss. The card reroutes 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 ITG ISL Trunk node to make sure that the ITG Trunk route is not used for new calls if the network QoS degrades below an acceptable level.

Card roles

The ITG ISL Trunk card can have one or more of the following roles:

- Follower
- Active Leader

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

The ITG ISL Trunk 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 is usually configured with the following:

- one ITG ISL Trunk card that acts as an Active Leader
- one ITG ISL Trunk card that acts as a Backup Leader
- at least one ITG ISL Trunk card that provides DCHIP functionality
- one or more ITG ISL Trunk cards identified as Followers.

In the MAT ITG application, the term Leader 0 refers to the ITG ISL Trunk card initially configured to perform the role of the Active Leader. The term Leader 1 refers to the ITG ISL 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 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 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 E-LAN connections.

Follower

A Follower card is an ITG ISL Trunk card which converts telephone signals into data packets and data packets into telephone signals. Follower cards also provide dialed number to IP address translation.

Active Leader

The Active Leader card is an ITG ISL Trunk card that acts as a point of contact for all other Meridian 1 in the network.

The Active Leader card is responsible for the following:

- distribute incoming H.323 calls to each registered Follower card in its node, and balance load among the registered cards for incoming IP calls
- IP addresses for other cards in its node
- work as a time server for all ITG ISL Trunk cards in its node
- perform network monitoring for outgoing calls in its node
- voice processing

All calls from a remote Meridian 1 ITG node are presented to the Active Leader card. The Leader card maintains a resource table of all the ITG ISL Trunk cards in its node. The Active Leader card consults its internal Follower card resource table to determine which Follower card has the most idle channels. The Active Leader card selects this card to receive the new call. The Active Leader sends a message to the selected Follower card, informing it to reserve a channel for the new call. It redirects the call to the selected Follower. The Follower card performs dialed number to IP address translation.

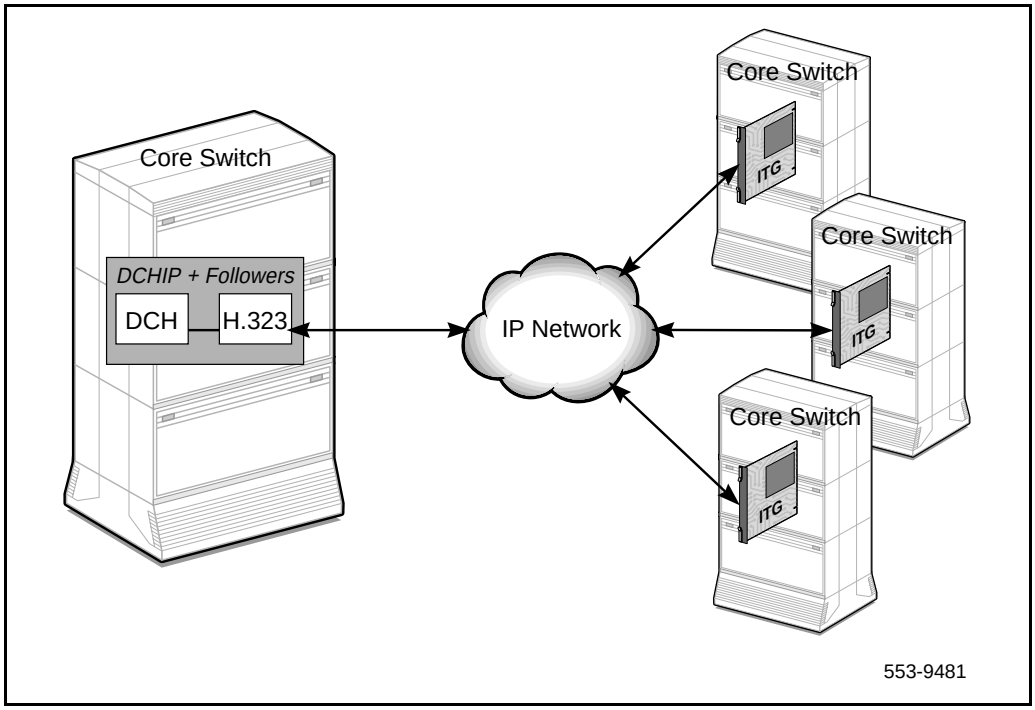
Backup Leader

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

D-channel IP gateway (DCHIP)

The ITG ISL Trunk card with DCHIP functionality (DCHIP Card) is connected by the RS-422 cable to the Multi-purpose Serial Data Link (MSDL) card on the Meridian 1 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 Meridian 1. The DCHIP Card is the network side of the Meridian 1 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 and the IP network (see Figure 2).

Figure 2
ITG architecture

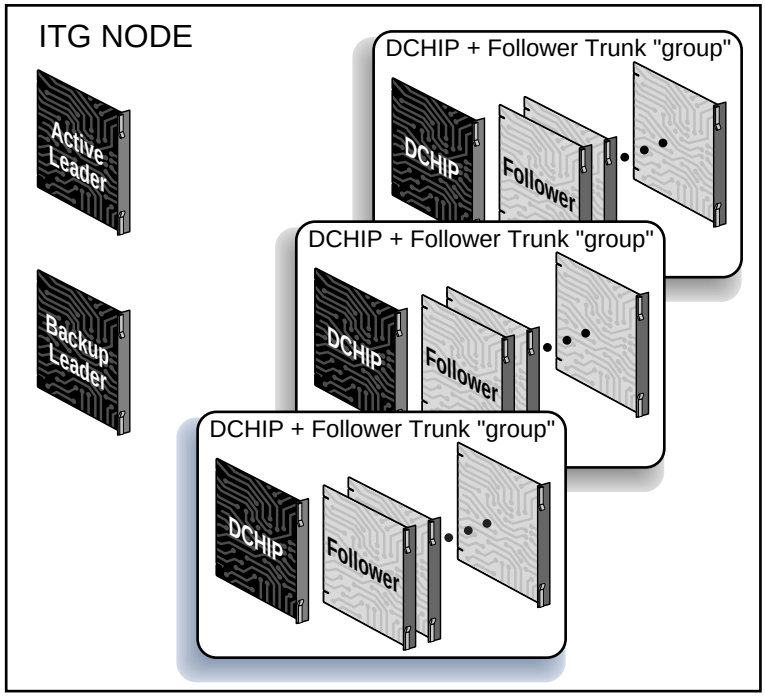


The ISL connection to the Meridian 1 functions as it does in a normal ISDN network. The ISL controls the call processing for calls over analog ITG IDSN Signaling Link (ISL) TIE trunks. These ISL TIE trunks can be on any of the ITG ISL Trunk cards. The ITG ISL D-channel only controls ITG ISL Trunk cards in the same ITG node. MAT administration relates the cards with trunks to the DCHIP ITG Trunk card.

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

Each DCHIP ITG Trunk card can be associated with up to 382 trunks. The trunks reside on 24-port ITG ISL Trunk cards. This creates a functional grouping of trunk cards with the DCHIP ITG Trunk card providing the DCH connectivity. If more than 382 trunks are required, additional DCHIP ITG Trunk card groups are configured, each with a maximum of 382 related trunks. (See Figure 3).

Figure 3
Leader, DCHIP, and trunks in an ITG node



553-9482

Card combinations

The Leader and DCHIP, or Follower and DCHIP, functions can reside on a single card or multiple cards. If a Follower card is equipped with a DCH PC card, it can function as a DCHIP ITG Trunk card. As a ITG Trunk 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 ITG Trunk 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 24-Port Follower cards. This limit is due to the maximum limit of 382 trunks in an ISL route.

> ***Note:*** Each DCHIP controls a separate group of Follower cards. If a DCHIP 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 ITG node to continue handling calls if one DCHIP fails.

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

> ***Note:*** All DCHIPs in an ITG node must be configured with the same DCH protocol. If the user wants to use multiple DCH protocols, the user must configure multiple ITG nodes.

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

It is possible to configure multiple ITG 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 ITG 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 ITG node, please refer to the *Engineering Guidelines* section.

Interactions among card functions

Active Leader and Follower card interaction

The Active Leader card controls the assignment of IP addresses for all new ITG ISL Trunk cards in its node. If a new ITG ISL Trunk card is added as a Follower, the new Card Configuration data, as programmed in MAT, 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. Call processing is maintained on the remaining ITG trunks.

If a Follower card loses communication with the Active Leader, all its ports appear busy to the Meridian 1. 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 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 ITG ISL Trunk cards in the ITG 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 MAT 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 ITG 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 ITG Trunk card failure occurs, the associated trunks' states appear busy to the Meridian 1, 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 ISL Trunk card physical description

The Meridian 24-Port ITG Trunk 2.0 card (NT0961AA) plugs into an Intelligent Peripheral Equipment (IPE) shelf. Each ITG ISL Trunk card occupies two slots. ITG ISL Trunk cards have a E-LAN management Ethernet port (10BaseT) and a T-LAN VoIP Ethernet port (10/100BaseT) on the I/O panel. The ITG ISL 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.

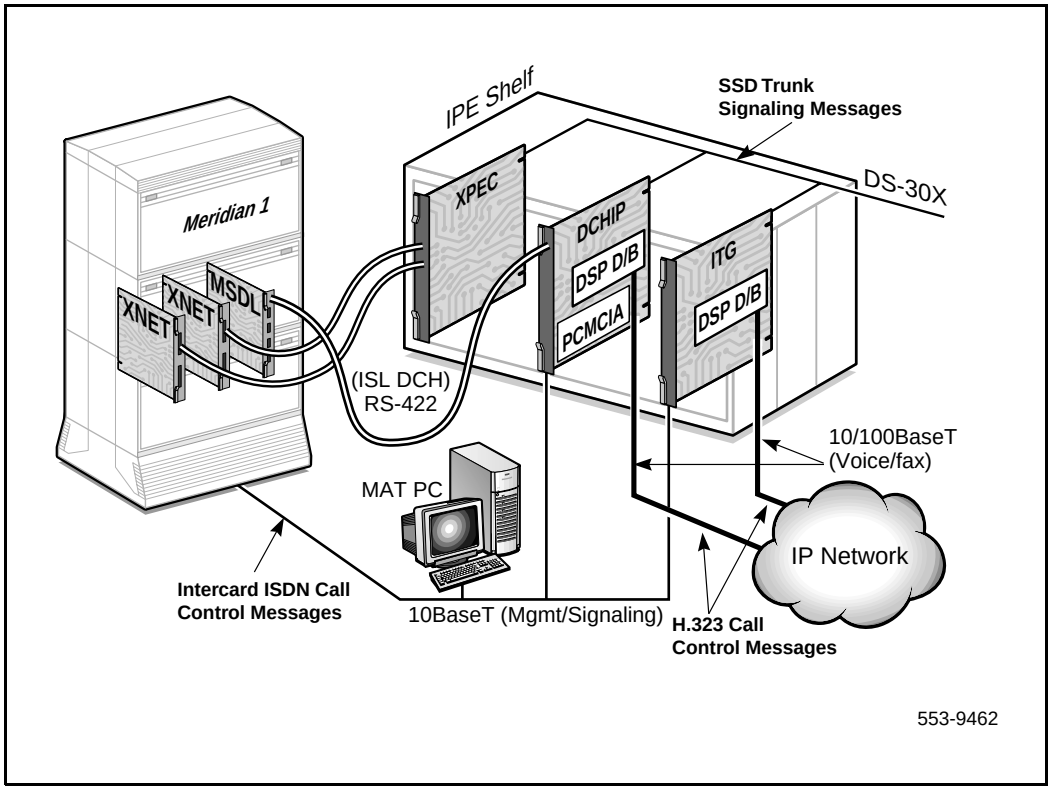
The NT0961AA ITG ISL Trunk card supports 24 ports per card.

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

The ITG ISL 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 4 on page 38 shows ITG ISL Trunk card system connectivity.

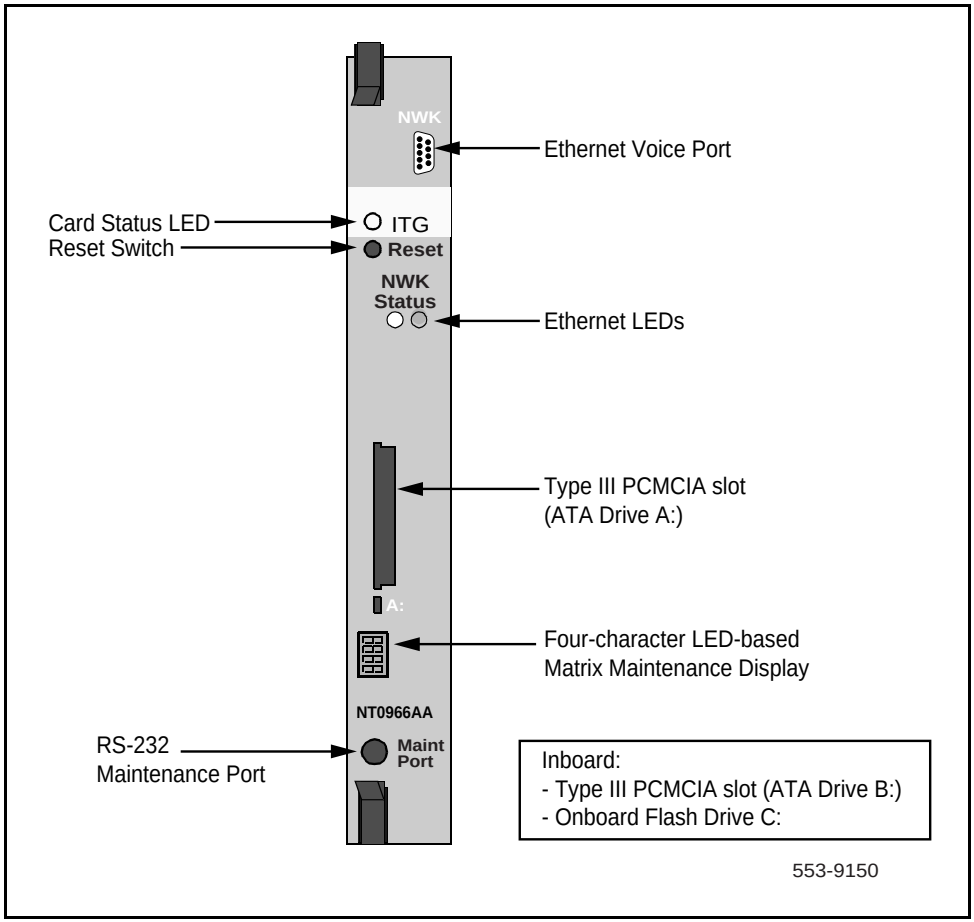
Figure 4
ITG system connectivity and messaging



Faceplate indicators, controls, and interfaces

The ITG ISL Trunk card has a double width faceplate using the shortened lock latches as shown in Figure 5.

Figure 5
ITG ISL Trunk card (NT0961AA)



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 on (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:

- that 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 since Security Devices are not implemented on ITG Trunk 2.0. You can ignore this message.

See "ITG Trunk 2.0 faceplate maintenance display codes" on page 329 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 T-LAN Ethernet hub.
- Yellow flashes when there is data activity on the T-LAN.
- During heavy traffic, yellow can stay continuously lit.

Note: There are no Ethernet status LEDs for the management 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, II, or 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

RS-232 maintenance port

The ITG ISL 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.

Voice Ethernet port (T-LAN)

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

WARNING

Do not connect a T-LAN cable to the Faceplate 9-pin Voice port connector (NWK). You must connect the T-LAN cable to the I/O cable.

Backplane interfaces

The following interfaces are provided on the ITG backplane connector:

DS-30X voice/signaling

Carries PCM voice and proprietary signaling on the IPE backplane between the ITG Trunk card and the Intelligent Peripheral Equipment Controller (XPEC).

Card LAN

Carries card polling and initialization messages on the IPE backplane between the ITG Trunk card and the Intelligent Peripheral Equipment Controller (XPEC).

RS-232 serial maintenance port

An alternative connection to the serial maintenance port 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.

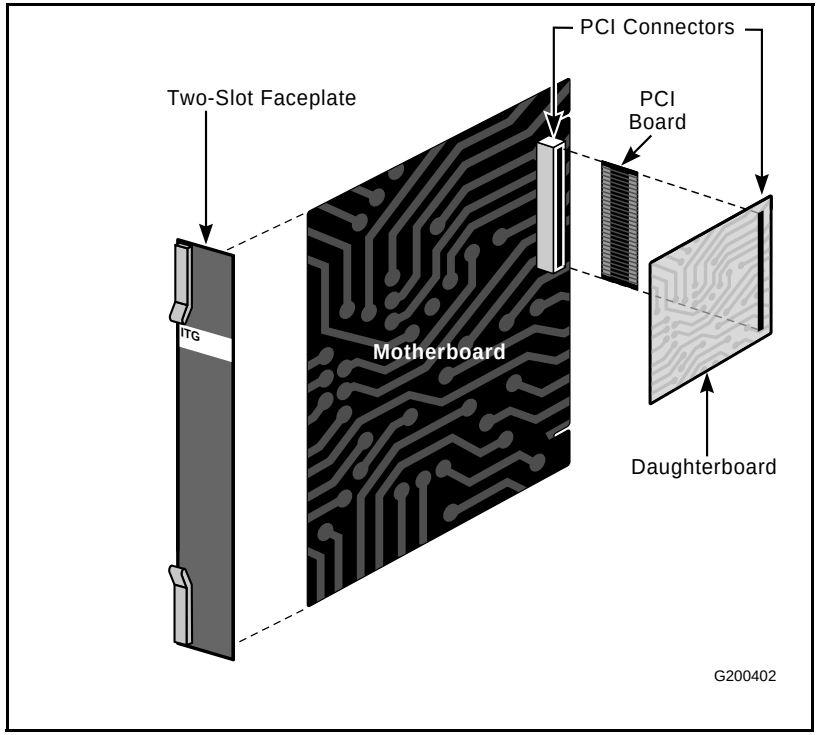
Assembly description

The ITG ISL Trunk card assembly consists of a two-slot motherboard/daughterboard combination, as shown in Figure 6 on page 43. A PCI interconnect board connects the ITG motherboard and the DSP daughterboard.

CAUTION

The ITG ISL Trunk card is not user-serviceable. Figure 6 on page 43 is for information purposes only. Do not remove the daughterboard from the motherboard.

Figure 6
Mechanical assembly



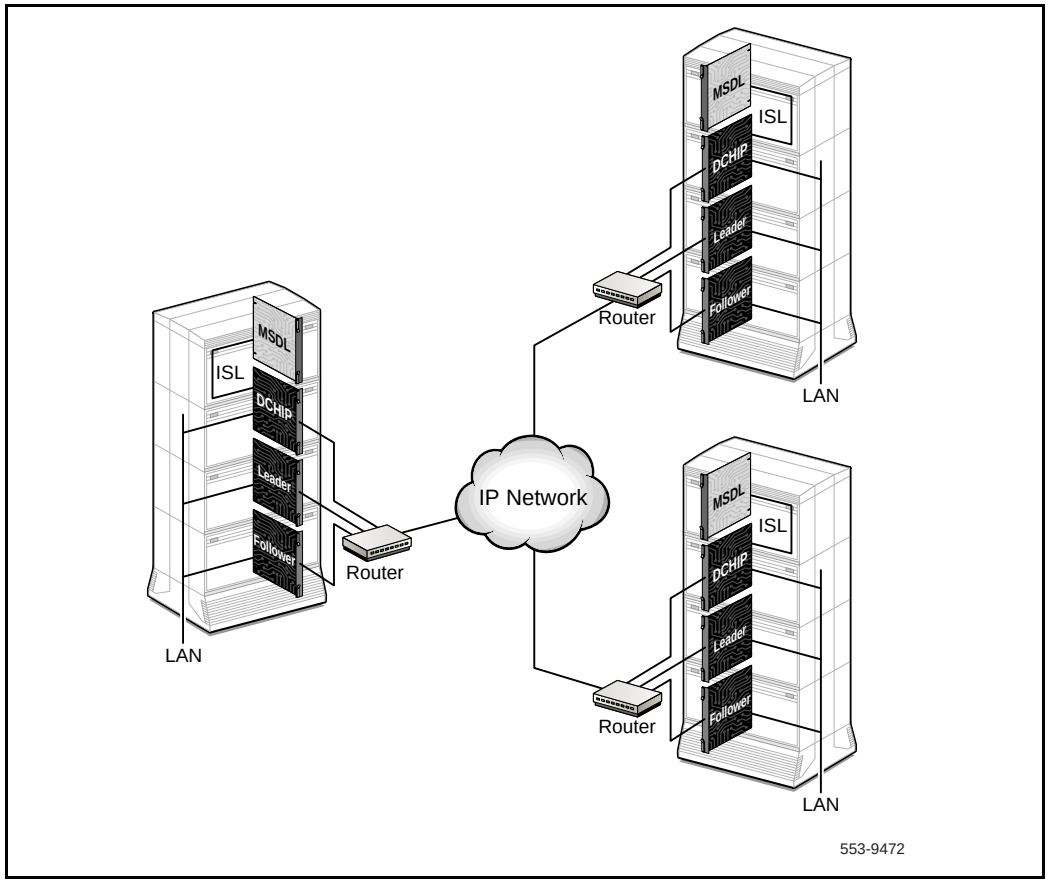
ISDN Signaling Link

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 PRI exists between two Meridian 1 systems, ISL operates in dedicated mode. A dedicated point-to-point signaling link is established between the two Meridian 1 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 VPN between Meridian 1 systems. Instead of a one-to-one connection, multiple switches can be networked through a single ISL interface at each site. Figure 7 on page 45 shows an ITG ISL Trunk configuration with three Meridian 1 systems. ITG ISL Trunk simulates an analog facility. The ISL interface is connected to a DCHIP PC Card which provides ISDN to VoIP tandeming. All ITG ISL Trunk cards (DCHIP, Leader, and Follower) are connected through the Embedded Local Area Network (E-LAN). ITG ISL Trunk cards communicate with remote switches through the IP network.

Figure 7
ITG configuration



ISDN signaling between the Meridian 1 and the ITG ISL Trunk 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 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:

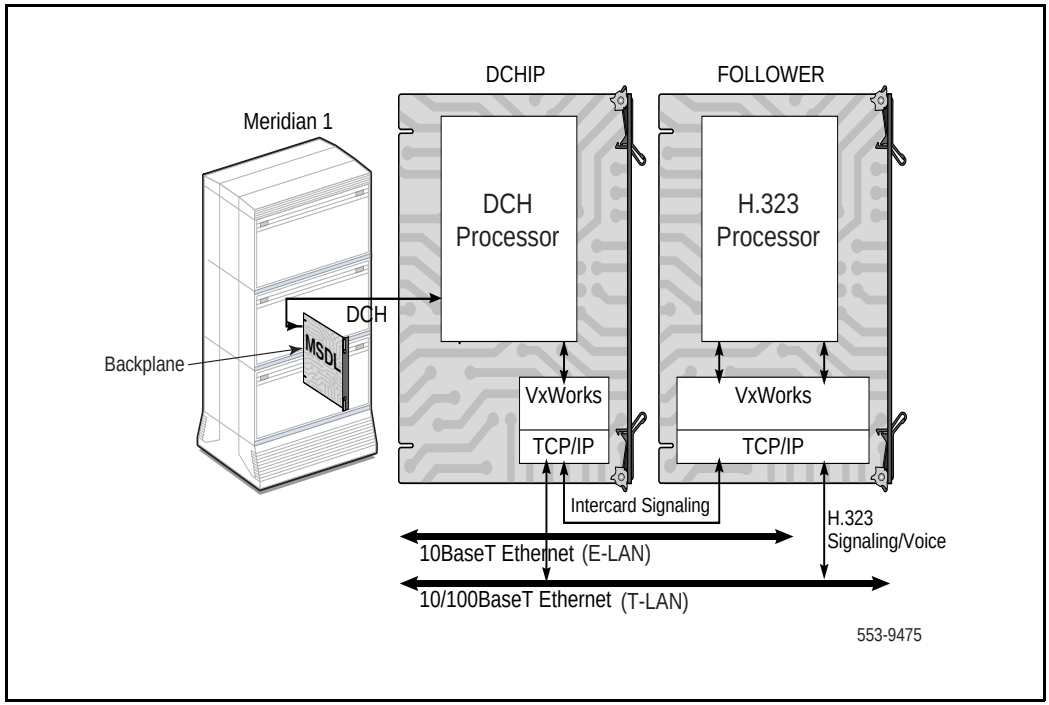
- ISL configuration support
- symmetry (incoming and outgoing call messaging is the same)
- near H.323 standard

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 end points. 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 8 shows the signal flow from the DCH to the H.323 stack.

Figure 8
Signal flow from the DCH to the H.323 stack

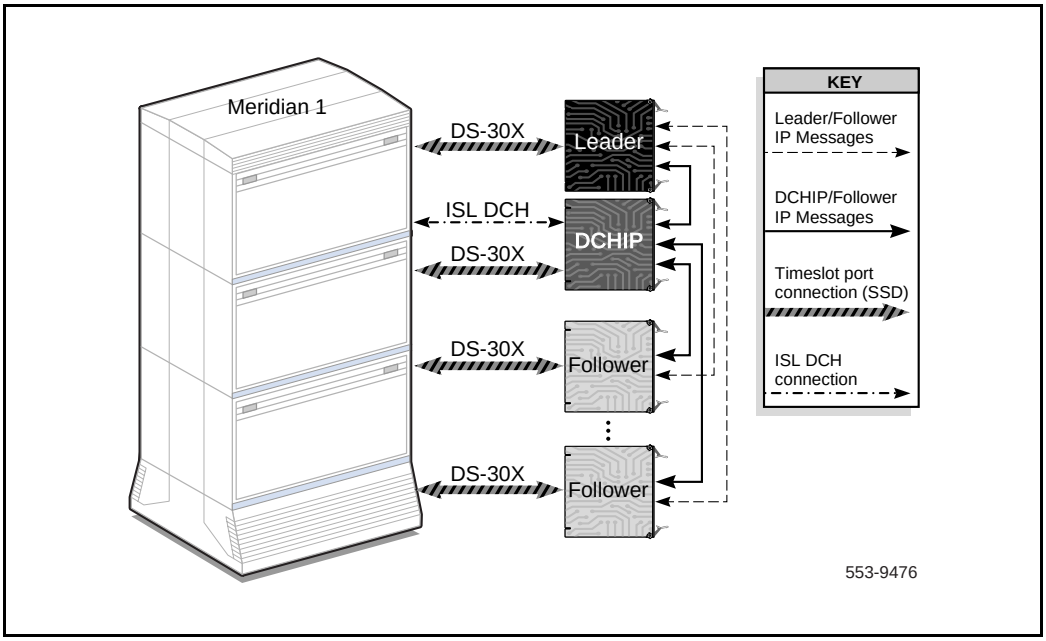


Note: For further information on ISDN Signaling Link (ISL), refer to *X11 System Management Applications* (553-3001-301), *ISDN PRI: Installation* (553-2901-201), and *ISDN PRI: Maintenance* (553-2901-501).

Inter-card signaling paths

The Leader, DCHIP, and Follower cards communicate using their E-LAN IP addresses. Figure 9 illustrates the Meridian 1 IP signaling paths used inter-card, and between the cards and the Meridian 1 system, in the ITG offering.

Figure 9
ITG ISL Trunk card signaling paths



In Figure 9, the DS-30X connection is part of the Meridian 1 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 T-LAN. The DCHIP messages travel over the E-LAN: a 10BaseT LAN connected to each ITG ISL Trunk card and the MAT 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 overlays in the Meridian 1 or MAT. With ESN configuration, the Meridian 1 can route outgoing calls to the ITG ISL Trunk card. Address translation allows the ITG ISL Trunk card call processing to translate the called party number to the IP address of the terminating ITG node, and to deliver calls to the destination through the IP network.

The Meridian 1 ITG ISL Trunk card supports 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 ITG Trunk dialing plan supports a single Meridian 1 customer per ITG node and multiple ITG nodes per Meridian 1. A customer may have multiple nodes in a Meridian 1, but each node can only support the dialing plan of a single customer. Multiple Meridian 1 customers will require multiple nodes per Meridian 1.

Multi-node configuration

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

Meridian 1 switch A has two ITG 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 ITG 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 ITG node (for example, DCH failure or Leader subnet fails) from completely eliminating VoIP service for a Meridian 1 system.

It is desirable to distribute calls to multiple nodes at a remote destination Meridian 1. The configuration of multiple dialing plan entries at the local ITG node allows routing based on the dialed digits.

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

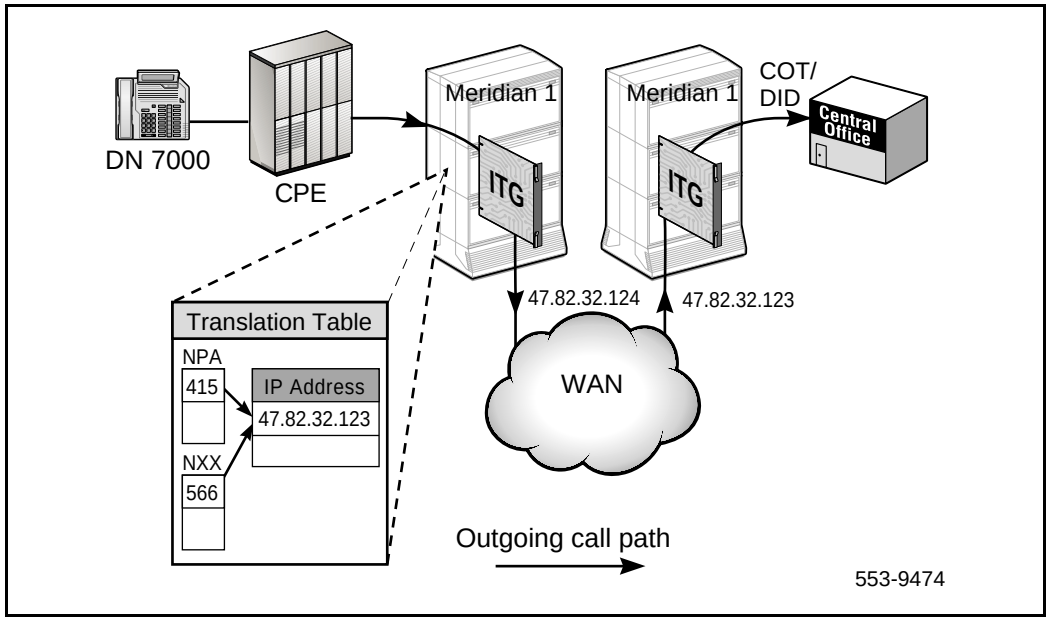
North American dialing plan

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 10 shows DN 7000 placing a public call, through the private LAN, by dialing 1-415-456-1234 or 566-1234. The ITG ISL 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 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 10
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 (ESN) Network Signaling

ITG Trunk 2.0 supports ESN5 Network Signaling protocol only, in addition to standard (i.e., non-network) signaling. ITG 2.0 supports a mixed network consisting of ESN5 and standard network signaling nodes.

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.

Silence Suppression

The purpose of Silence Suppression is to reduce bandwidth consumption. With the H.225 protocol, coders can send silence frames before the end of transmission, during a period of silence. Coders may 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.

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 Silence Suppression set the bit to zero.

DTMF Through Dial

Preservation and transport of tones through the IP network is critical for Interactive Voice Response (IVR) services. The ITG makes sure that DTMF tone information is included in the packets that are sent through the IP network, and that the tones are retransmitted by the far-end gateway. The duration information for DTMF signals is not transmitted, i.e., long DTMF bursts are reduced to a short standard duration.

Callers can access traditional Voice Mail or IVR services, including “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.

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 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:

- 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 59.

Packet jitter related to latency affects the quality of real-time IP transmissions. For good voice quality, the ITG ISL 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 ITG node in MAT. 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 per remote gateway. For example, if a given Leader has three remote leaders in its dialing plan table, it will perform 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 ITG 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 52.

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 ITG ISL 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, PING and Traceroute, are described below. Other utilities can be used to gather information about ITG network performance.

> ***Note:*** These descriptions are for reference purposes only. Traceroute is not part of the ITG 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 ITG node to every other ITG node in your 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

The ITG 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. The ITG 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 network end-to-end latency consists of several components: routing delay on the IP network, frame duration delay and Jitter Buffer delay on codec, and delay on the circuit-switched network. The determination of end-to-end delay depends on the dynamics of the IP 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 ITG node QoS values in MAT.

For instance, assume the end-to-end network latency is 300 milliseconds and the part of that latency which the IP network can contribute 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 the *Engineering Guidelines* section.

Fallback to alternate facilities

The ITG continuously monitors and analyzes QoS data. When the ITG detects IP network congestion, and the QoS is below a pre-defined value, new calls routed to the remote IP gateway are rejected. Instead, the Meridian 1 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 the ITG 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 ITG Trunk destination node, all outgoing calls from the near end Meridian 1 to the far end Leader are re-routed through alternate circuit-switched trunk facilities. That is, all calls that the switch is trying to setup; established calls cannot fallback.

The Meridian 1 provides alternate routing based on BARS or NARS. BARS/NARS translates the dialed location (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).

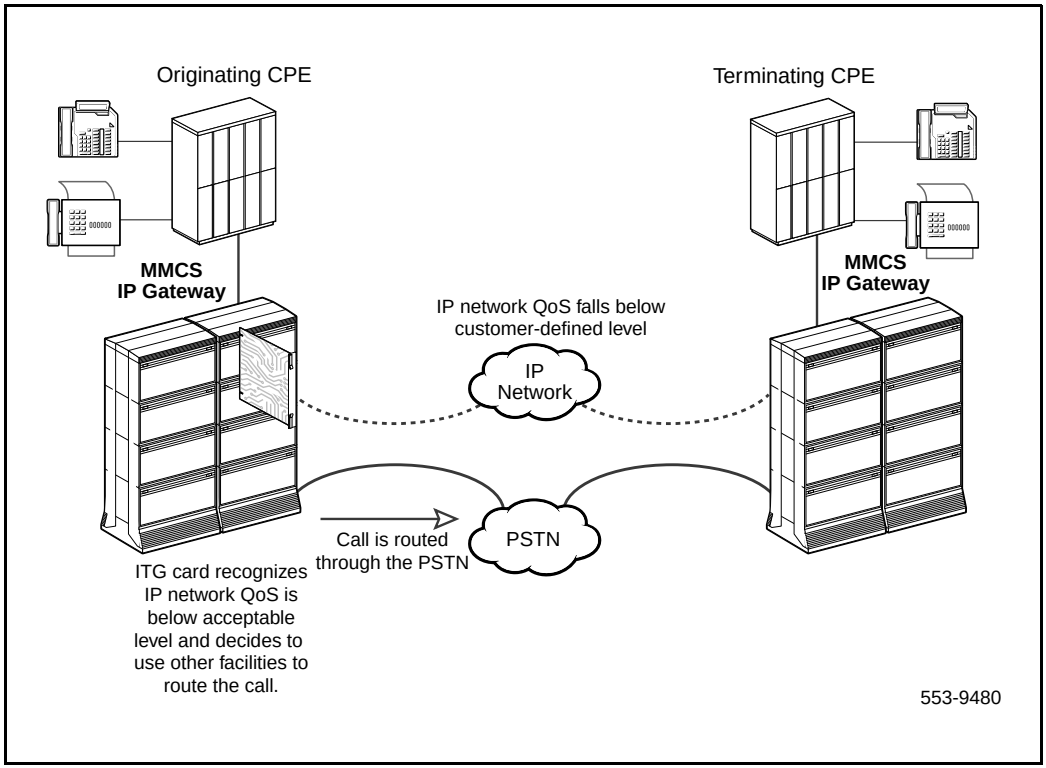
The trigger for Fallback to alternate trunk facilities is defined per call, per customer. The local Active Leader makes the decision to use the Fallback feature. The selection of routes is based on the customer-configured database. The customer must configure the alternate routing to the PSTN in the Meridian 1's 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 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 the IP trunk will be routed to some other treatment. Fallback is optional, based on the configuration of the route list.

Figure 11 shows the Fallback to alternate facilities functionality.

Figure 11
Example of a Fallback to alternate facilities situation



Return to the IP network

Unless the DCH is down and all trunks appear busy to the Meridian 1, it always introduces outgoing calls to the ITG 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 MAT 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 ITG node is configured, ToS bits are initially set to default values. The MAT ITG 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 ITG ISL 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 ITG ISL 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 ITG 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 T-LAN interface.

Local subnet packets is the H.323 call data intended for another ITG 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 T-LAN port 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 ITG ISL 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

You must have detailed knowledge of router capabilities before you change ToS. Improper changes to ToS can degrade network performance.

Fax support

The ITG ISL 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 ITG ISL Trunk uses the T.38 protocol on the connection between a pair of ITG ISL Trunk nodes.

The call acts in the same way as a gateway-to-gateway H.323 call. The call is setup 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 the following:

- 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 terminals through the ITG ISL Trunk cards over the IP network using the T.38 protocol. In terms of the Internet fax service roles, the ITG ISL 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 ITG to ITG 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 ITG node to ITG node fax calls are supported (although Meridian 1 to third-party fax calls may work).

Remote Access

Remote Access is supported on the ITG. Remote Access allows a MAT user with no ITG data, including Nortel Networks support personnel, to manage the ITG ISL Trunk card remotely.

Management and support of the ITG network depend on IP networking protocols including SNMP, FTP, and Telnet. The Nortel Networks Netgear RM356 modem router or equivalent should be installed on the Meridian 1 site management and signaling LAN (called the embedded LAN or E-LAN as opposed to the customer's enterprise network or C-LAN) in order to provide remote support access for ITG and other IP-enabled Nortel Networks products.

The Nortel Networks 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 E-LAN 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 MAT PC to provide remote access to any PC with a modem. The remote user dials the MAT PC which contains the required ITG data (whether stored locally or on a MAT server). Once connected, the remote user can perform any operation available to that PC.

Per-call statistics support using RADIUS Client

The ITG architecture isolates the IP voice interface from the Meridian 1. However, the Meridian 1 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

ITG uses a Remote Authentication Dial In User Service (RADIUS) client to transmit these statistics from the ITG ISL Trunk card to a network device:

- ITG ISL Trunk card sends a Start record when a call begins.
- ITG ISL 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 MAT Call Accounting application does not correlate RADIUS per call statistics with the Meridian 1 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 ITG ISL 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 ITG ISL Trunk card uses the authentication algorithm based on RFC1321.

Configuration

Use MAT 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 ITG node level and is distributed to all ITG ISL Trunk cards associated with the 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 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 ports.

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 it's 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 will also be 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 MAT ITG alarms or events. Support for the SNMP Management Information Bases (MIB) on the ITG ISL Trunk card is composed of two parts: the standard MIB-2 and extensions for the ITG ISL 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.

ITG SNMP agent

The SNMP agent supports the Operation, Administration, and Maintenance (OA&M) of the ITG, using MAT. It can configure the ITG ISL 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 ITG 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 ITG ISL Trunk card. The G.XXX series of codecs are standards defined by the International Telecommunications Union (ITU). Different codecs have different Quality of Service and compression properties. The specific codecs and the order in which they are to be used for codec negotiation is configured in MAT.

When configuring the ITG Node in MAT, 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.

The ITG supports the following codecs:

- G.711
- G.729A
- G.729
- 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 ITG ISL Trunk node. Voice Activity Detection/Silence Suppression is configurable through MAT. 24 channels per card are supported with G.711.

G.729A

The G.729A codec is the default preferred codec when adding a new ITG Trunk node in MAT. This codec provides near toll quality voice at a low delay. The G.729A codec uses compression at 8 kbit/s (8:1 compression rate). Optional Annex B Voice Activity Detection/Silence Suppression is configurable through MAT. 24 channels per card are supported with G.729A.

G.729

The G.729B codec use compression at 8 kbit/s (8:1 compression rate). Optional Annex B Voice Activity Detection/Silence Suppression is configurable through MAT. Only 16 channels per card are supported with G.729B due to higher DSP resources required for this codec.

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 MAT. 24 channels per card are supported with G.723.1.

Three downloadable DSP profiles support the codecs shown in Table 4.

Table 4
Codecs supported by the ITG

Profile 1 **32 ms. Echo Cancel Tail** **24 ports/card**	**Profile 2** **32 ms. Echo Cancel Tail** **24 ports/card**	**Profile 3** **32 ms. Echo Cancel Tail** **16 ports/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.

Security passwords

If you Telnet into the E-LAN port or use the debug port, you are prompted for a password. 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 the ITG:

- 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 ITG ISL 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 Networks personnel only. It allows low level message monitoring and factory testing.

ITG Engineering Guidelines

Introduction

The Meridian Integrated IP Telephony Gateway (ITG) system:

- 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.

ITG routes voice traffic over existing private IP network facilities with available under-used bandwidth on the private Wide Area network (WAN) backbone.

The ITG is targeted at the Enterprise customer who has both a Meridian 1 system installed for providing corporate voice services, and an intranet for corporate data services. A customer is expected to use the ITG 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 technology will be transported using packet-switched and statistical multiplexing technology.

This chapter provides guidelines for designing a network of ITG nodes over the corporate intranet. It describes how to qualify the corporate intranet to support an ITG network, and 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 local area network (LAN). By following these guidelines, you can design the ITG network so that the cost and quality tradeoff is at best imperceptible, and at worst within a calculated tolerance.

Audience

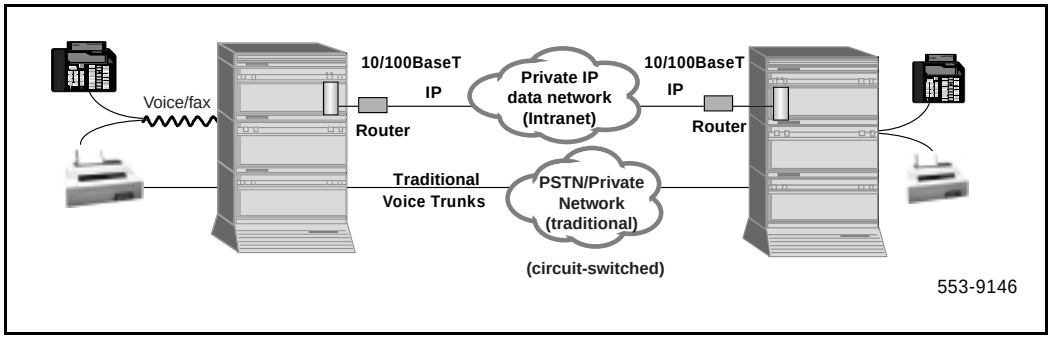
This chapter is addressed to both telecom and datacom engineers who are going to design and install the ITG network. It is assumed that the telecom engineer is familiar with engineering the Meridian 1, and obtaining system voice and fax traffic statistics. It is assumed that the datacom engineer is familiar with the intranet architecture, LAN installations, tools for collecting and analyzing data network statistics, and data network management systems.

ITG equipment requirements

The ITG 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. You must determine the design and configuration of the LAN and WAN that link the ITG system. If the intranet becomes overloaded, new calls to the ITG system fall back to normal circuit-switched voice facilities so that the quality of service does not degrade for new calls.

The ITG product is for intranet use only. ITG provides virtual analog ISL TIE trunks between two Meridian 1 systems in an ESN network, as shown in Figure 12. ITG does not support modem traffic except for Group 3 fax. The technician must configure the Meridian 1 routing controls to route modem traffic over circuit-switched trunks instead of over ITG.

Figure 12
The Meridian Integrated IP Telephony Gateway intranet



The ITG system is available for options 11C, 51C, 61C, 81 and 81C systems running X11 release 25 or later software. It is also compatible with SL-1 systems NT, RT, and XT upgraded to support IPE cards.

The ITG card plugs into the Meridian 1 IPE shelf. A maximum of eight cards can fit on one IPE shelf; each ITG card takes up two slots on the IPE shelf.

Option 11C systems operating under Class B Electro-Magnetic Compatibility (EMC) standards can only hold a total of two cards, divided between the main and expansion cabinets. This may 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 Option 11C systems operating under Class A EMC standards, there are no restrictions.

For Option 11C and Option11C Mini, the SDI/DCH (NTAK02BB) card occupies one slot on the cabinet and is connected to the ITG card through the backplane. Only ports 1 and 3 are available for use as DCHI.

The ITG card uses a 10BaseT Ethernet port located on the card backplane I/O connector to carry ITG system management traffic and connects to the Embedded LAN (E-LAN).

Scope

These engineering guidelines address the design of the ITG network which consists of:

- ITG nodes
- Telephony LANs (T-LANs) to which the ITG nodes are connected
- A corporate intranet which connects the different T-LANs together

These guidelines require that the Enterprise customer has a corporate intranet in place that spans the sites where the ITG nodes are to be installed.

Network engineering guidelines overview

Traditionally Meridian 1 networks depended on voice services[1] such as LEC and IXC private lines. With ITG technology, the Meridian 1 can select a new delivery mechanism, one that uses packet-switching over a data network or corporate intranet. The role of the ITG 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.

In the data world in the late 1960s, 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 ITG nodes to the corporate intranet without preliminary assessments can result in unacceptable degradation in the voice service; instead correct design procedures and principles must be considered.

1. For the sake of abbreviation, the term voice services also includes fax services.

A good design of the ITG network must begin with an understanding of traffic, and the underlying network that will transmit the traffic. There are three preliminary steps that you must undertake.

1 Calculate ITG traffic. The technician must estimate the amount of traffic that the Meridian 1 system will route through the ITG network. This in turn will place a traffic load on the corporate intranet. This is described in “ITG traffic engineering” on page 76

2 Assess WAN link resources. If resources in the corporate intranet are not enough to adequately support voice services, it is normally caused by not enough WAN resources. “Assess WAN link resources” on page 101 outlines how this check can be made.

3 Measure existing intranet's Quality of Service (QoS). The technician must estimate the quality of voice service the corporate intranet can deliver. “Measure intranet QoS” on page 114 describes how to measure prevailing delay and error characteristics of an intranet.

After the assessment phase, you can design and implement the ITG network. This design not only involves the ITG elements, but can also require making design changes to the existing customer intranet. “Fine-tune Network QoS” on page 119 and “Implement QoS in IP networks” on page 126 provides guidelines for making modifications to the intranet.

ITG traffic engineering

To design a network is to size the network so that it can accept some calculated amount of traffic. The purpose of the ITG network is to deliver voice traffic meeting the QoS objectives. Since traffic determines network design, the design process needs to start with the process of obtaining offered ITG traffic forecast. The traffic forecast will drive:

- WAN requirements
- ITG hardware requirements
- T-LAN requirements

Use of Ethernet and WAN bandwidth

Table 5 on page 77 lists the Ethernet and WAN bandwidth use of ITG ports with different codecs with silence suppression enabled, and Table 6 on page 80 lists the use 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, the total route traffic should be divided by 36 CCS and multiplied by the bandwidth use to get the data rate requirement of that route. All traffic data must be based on the busy hour of the busy day.

Note that to calculate resource requirements (ITG ports and T-LAN/WAN bandwidth), traffic parcels are summarized in different ways:

1 Add all sources of traffic for the ITG network, e.g., voice, fax sent, fax received, together to calculate ITG port and T-LAN 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 T-LAN and WAN are different. The following calculation procedure is for T-LAN (the modification required for WAN engineering is included in these procedures).

A WAN route with bandwidth of 1.536 Mbit/s or more can be loaded up to 80% (voice packets must have priority over data), a smaller WAN pipe (64 kbit/s) is recommended to a loading of 50%.

When the WAN route prioritizes VoIP application over data traffic, the route bandwidth can be engineered to 90% loading level. Otherwise, only 80%.

In Tables 5 and 6, the first WAN bandwidth is without Frame Relay or ATM overhead.

The Frame Relay overhead is eight 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, etc. Within the same number of cells, the bandwidth requirements are the same for packets with different sizes.

MAT input for FAX is in bytes (ranged from 20 to 48), 30-byte is the default. It is different from voice applications where payload size is the input.

Table 5
Silence suppression enabled, T-LAN Ethernet and WAN IP bandwidth usage per ITG port (Part 1 of 2)

Codec type	Codec Multi - frame duration in ms (payload) (one way)	Voice/fax payload Multi - frame in bytes (one way)	IP voice packet in bytes (one way)	Ethernet voice packet in bytes (one way)	Bandwidth use on T-LAN in kbit/s (two way)	Bandwidth use on WAN in kbit/s (one way)	WAN with Frame Relay overhead in kbit/s (one-way)	WAN with ATM overhead in kbit/s (one-way)
G.711 (64 kbit/s)	**10**	**80**	**120**	**146**	**140.2**	**57.6**	**61.4**	**76.3**
	20	160	200	226	108.5	48.0	49.9	63.6
	30	240	280	306	97.9	44.8	46.1	59.4
G.729AB G.729A (8 kbit/s)	10	10	50	76	73.0	24.0	27.8	50.9
	20	20	60	86	41.3	14.4	16.3	25.4
	30	**30**	**70**	**96**	**30.7**	**11.2**	**12.5**	**17.0**

Table 5
Silence suppression enabled, T-LAN Ethernet and WAN IP bandwidth usage per ITG port (Part 2 of 2)

Codec type	Codec Multi - frame duration in ms (payload) (one way)	Voice/fax payload Multi - frame in bytes (one way)	IP voice packet in bytes (one way)	Ethernet voice packet in bytes (one way)	Bandwidth use on T-LAN in kbit/s (two way)	Bandwidth use on WAN in kbit/s (one way)	WAN with Frame Relay overhead in kbit/s (one-way)	WAN with ATM overhead in kbit/s (one-way)
G.723.1 (5.3 kbit/s)	**30**	**20**	**60**	**86**	**27.5**	**9.6**	**10.9**	**17.0**
G723.1 (6.3 kbit/s)	**30**	**24**	**64**	**90**	**28.8**	**10.2**	**11.5**	**17.0**
T.30/T38 G3 Fax Modem (14.4 kbit/s)	**16.6**	**30**	**70**	**96**	**46.1**	**33.6**	**37.5**	**50.9**
	25	30	70	96	30.7	22.4	25.0	33.9

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 the MAT.
Note 3: T-LAN data rate is the effective Ethernet bandwidth consumption.
Note 4: 40% voice traffic reduction due to silence suppression; no suppression for fax.
Note 5: T-LAN kbit/s for voice traffic = (1-40%)*2*Ethernet frame bits*8/frame duration in ms
Note 6: WAN kbit/s for voice traffic = (1-40%)*IP packet bytes*8/frame duration in ms
Note 7: 24 ports per card for all codecs
Note 8: 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 9: The above bandwidth calculation does not include an Interframe gap, because of the low probability of occurring in this type of application.

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 Meridian 1 equipped with an ITG 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, will degrade the quality of service by causing choppiness of speech. Under tandem switching conditions with

where loss level cannot compensate, silence suppression should be disabled using the MAT ITG ISDN Trunk Node Properties DSP profile tab codec options sub-tab. See Step 8 on page 203.

Disabling silence suppression *approximately doubles* LAN/WAN bandwidth use. Disabling silence suppression consumes more real-time on the ITG card.

Table 6 shows the bandwidth requirement when silence suppression is disabled.

Note that this does not impact the data rate for fax, since it does not have silence suppression enabled to begin with.

Simultaneous voice traffic with silence suppression

When voice services with multi-channel requirements are extensively used in an ITG network, such as Conference, Music-on-hold, and Message-Broadcasting, additional voice traffic peaks to the IP network will be 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 ITG card, the more conservative bandwidth calculations of Table 6 with silence suppression disabled is recommended to calculate the portion of the bandwidth requirement that is caused by simultaneous voice traffic.

Table 6
Silence suppression disabled T-LAN Ethernet and WAN IP bandwidth usage per ITG port

Codec type	Codec Multi - frame duration in ms (payload) (one way)	Voice/fax payload Multi - frame in bytes (one way)	IP voice packet in bytes (one way)	Ethernet voice packet in bytes (one way)	Bandwidth use on T-LAN in kbit/s (two way)	Bandwidth use on WAN in kbit/s (one way)	WAN with Frame Relay overhead in kbit/s (one-way)	WAN with ATM overhead in kbit/s (one-way)
G.711 (64 kbit/s)	**10**	**80**	**240**	**292**	**233.6**	**96.0**	**102.4**	**127.2**
	20	160	400	452	180.8	80.0	83.2	106.0
	30	240	560	612	163.2	74.6	76.6	98.9
G.729AB/ G.729A (8kbit/s)	10	10	100	152	121.6	40.0	46.4	84.8
	20	20	120	172	68.8	24.0	27.2	42.4
	30	**30**	**140**	**192**	**51.2**	**18.6**	**20.8**	**28.3**
G.723.1 (5.3 kbit/s)	**30**	**20**	**120**	**172**	**45.8**	**16.0**	**18.1**	**28.3**
G723.1 (6.3 kbit/s)	**30**	**24**	**128**	**180**	**48.0**	**17.0**	**19.2**	**28.3**
T.30/T.38 G3 Fax Modem 14.4 Kbit/s	**16.6**	**30**	**70**	**96**	**46.3**	**33.7**	**37.5**	**50.9**
	25	30	70	96	30.7	22.4	25.0	33.9

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 the MAT.

Note 3: T-LAN data rate is the effective Ethernet bandwidth consumption.

Note 4: T-LAN 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: 24 ports per card for all codecs

Note 7: 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 8: An Interframe gap is not included in the above bandwidth calculation, because of the low probability of occurring in this type of application.

T-LAN traffic calculations

The following are calculation procedures for T-LAN:

1 Calculate Voice on IP Traffic

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

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

The number of VoIP users (telephone sets) is the potential population in the system that can generate/receive traffic through the ITG node. This number may be estimated for a new Meridian 1 customer.

If the installation is for an existing Meridian 1 customer, the VoIP traffic should be based on measured route traffic from traffic report TFC002, which provides CCS for each route. A customer must provide the input about how much private network voice traffic is expected to be offered to the IP network.

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 to send or receive 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 ITG traffic (T) = Tv + Tx

4 Refer to Poisson P.01 Table to find ITG 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 (ITG ports) in Table 12 on page 94 which provides a CCS higher than T is the solution.
For P.10 blocking Grade of Service, refer to Table 13 on page 95.

5 Calculate bandwidth output. Refer to Table 5 (silence suppression enabled) or Table 6 (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, only the larger of fax traffic sent or received needs to be considered.

6 Adjust requirement for traffic peaking

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

A peakedness factor of 1.3 is the default value used to account for traffic fluctuation in the busy hour due to non-queued, Poisson random distribution of call originations.

The procedure shown here is for ITG port and T-LAN data requirement calculation. In the WAN environment, traffic parcel is defined per destination pair (route). The total node traffic should be sub-divided into destination pair traffic. The rest of calculation procedure continues to be applicable.

Example 1: ITG ports and T-LAN Engineering (silence suppression enabled)

A configuration with 120 VoIP users each generates 4 calls using 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.729 Annex AB, voice packet payload is 30 ms. The fax modem speed is 14.4 kbit/s, and payload is 16.6 ms. How many ITG ports are needed to meet P.01 blocking Grade of Service? What is the traffic in kbit/s generated by this node to T-LAN?

1 Calculate Voice on IP 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 ITG Traffic during busy hour

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

4 Refer to the Poisson P.01 table (Table 12) to find the number of ITG ports required for 1% blocking Grade of Service. For P.10 blocking Grade of Service, refer to Table 13.

804 CCS can be served by 35 ITG ports with P.01 blocking Grade of Service. Two 24 -port ITG cards are needed to serve this customer.

5 Calculate average bandwidth use on T-LAN

For voice:

720/36*30.7 =614 kbit/s

Refer to Table 5 (silence suppression enabled), data output for G.729 Annex AB and 30 ms payload is 30.7 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 T-LAN should have to handle the VoIP and fax traffic. It is recommended that the T-LAN handle ITG traffic exclusively.

Note that this example is based on the G.729 Annex AB codec with 30 ms payload size and silence suppression enabled. For relations of user selectable parameters (e.g., payload size, codec type, packet size and QoS), refer to "Set QoS" on page 108.

General LAN and WAN engineering considerations

The T-LAN traffic capacity does not limit ITG network engineering. Refer to "Set up a system with separate subnets for voice and management" on page 130 and "Single subnet option for voice and management" on page 131 Refer to standard Ethernet engineering tables for passive 10/100BaseT repeater hubs. Refer to manufacturer's specifications for intelligent 10/100BaseT layer switches.

A passive 10/100BaseT Ethernet hub is a half-duplex data transport mechanism. Both "talk" and "listen" traffic use a part of the nominal 10 Mbit/s capacity. The customer must then set up the passive 10/100BaseT Ethernet hub so that T-LAN voice traffic does not exceed 3MB/second on a 10/100BaseT Ethernet. A 10/100BaseT Ethernet switch port can operate in either half-duplex or full-duplex mode, but ITG Ethernet interfaces operate only in half-duplex mode. A switched Ethernet hub can reach throughput of 10MB/second. See your manufacturer's specifications for more information.

Because of its high capacity, 100BaseT Ethernet does not experience bottlenecks.

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 (i.e., 64 kbit/s in each direction). The same conversation on WAN (e.g, T1) requires a 64 kbit/s channel only, because a WAN channel is a full duplex channel.

When ITG cards share a segment of Ethernet in the simplex mode, the average loading on Ethernet should not exceed 30%.

When simplex/duplex Ethernet links terminate on the ports of an Ethernet switch (e.g., Baystack 450), the fully duplex Ethernet up-link to the router/WAN can be loaded to 60% on each direction of the link.

A WAN route with bandwidth of 1.536 Mbit/s or more can be loaded up to 80% (voice packets must have priority over data), a single DS0 WAN pipe (64 kbit/s) is recommended to a loading of 50%.

When the WAN route prioritizes VoIP application over data traffic, the route bandwidth can be engineered to 90% loading level, otherwise 80%.

Fax engineering considerations

Fax calculation is based on 30 bytes packet size and data rate of 64 kbit/s (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 will have to go through similar calculations.

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

Configuration of Meridian 1 routes and network translation

The objective is to maximize ITG traffic and minimize fallback routing. All ITG trunks should be busy before fallback routing occurs, except during network failure conditions.

Setting LD 86 Route List Blocks in Meridian 1

Other important objectives associated with an ITG network translations and route list blocks are:

1 make the ITG the first-choice, least-cost entry in the route list block

2 use TOD scheduling to block voice traffic to the ITG route during peak traffic periods on the IP data network when degraded quality of service causes all destination ITG nodes to be in fallback.

The proper time to implement either setting is explained below:

(1) Make the ITG the first-choice, least-cost entry in the route list block

An ITG 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 Meridian 1 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 ITG route during peak traffic periods on the IP data network

Based on site data, if fall back routing occurs frequently and consistently for a data network during specific busy hours (e.g., 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 ITG 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 ITG trunk route.

(3) Use the traditional PSTN for modem traffic

ITG does not support modem traffic except Group 3 fax. You must configure the Meridian 1 routing controls to route modem traffic over circuit-switched trunks instead of over ITG.

Use the ESN TGAR, NCOS, and facility restriction levels to keep general modem traffic off the ITG route.

Configure the IP router on the T-LAN

The ITG node telephony network, or T-LAN must be placed on its own subnet. The router should have a separate 10/100BaseT interface subnetted for the T-LAN and should not contain any other traffic. Other IP devices should not be placed on the T-LAN.

Priority routing for Voice over IP packets

Routers having the capability to turn on priority for voice packets should have this feature enabled to improve Quality of Service performance. If the Type of Service (TOS) field or Differentiated Services (DiffServ) is supported on the IP network, you can configure the decimal value of the DiffServ/TOS byte. For example, a decimal value of 36 is interpreted in TOS as “Precedence = Priority” and “Reliability = High”.

CAUTION

Do not change the DiffServe/TOS byte from the default value of 0 unless directed by the network administrator to do so.

Leader And DCHIP Card Real Time Engineering

If you will be configuring an ITG Trunk node with five cards or less, then you can safely skip this section. Real time engineering becomes important in the case of nodes with more than five cards and very large networks, i.e. one hundred or more ITG Trunk nodes.

Leader and DCHIP card standard configuration rules

1 Leader 0 with DCHIP and fully configured trunks supporting Leader 1 and all Followers. This rule covers most ITG Trunk node configurations.

2 Leader 0 with first DCHIP and fully configured trunks supporting half of the Followers, and Leader 1 with second DCHIP and fully configured trunks supporting the other half of the Followers. This rule covers D-Channel redundancy with two ITG trunk routes per node.

3 Leader 0 with first DCHIP and partially configured trunks, Leader 1 with second DCHIP and partially configured trunks supporting very large ITG Trunk nodes in very large ITG Trunk networks. This rule covers very large nodes and networks with multiple ITG trunk routes per node.

To setup an incoming voice (or fax) call, the Follower Card is responsible for communicating with the Follower Card at the far-end to set up (and tear down) the call. However, the Leader Card needs to 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 needs to be engineered to reserve enough capacity to provide this call processing functionality.

The real time capacity of the Leader Card depends on various factors:

1 host module CPU (Intel 486 or Pentium-based)

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

3 the size of the ITG network (number of Leader Cards in the network)

4 number of probe packets sent to every Leader Card at remote node, etc.

Factor (1) impacts the real time capacity significantly. Factors (3) and (4) impact the real time requirement of the software component Network Monitoring Module on the Leader Card. 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, the average holding time is 180 seconds, the number of calls per hour per port (on the Follower Cards) is 15.3.

8-Port Leader and DCHIP Card Real Time Capacity

The 8-Port ITG Trunk Card is the NTCW80 based on the Intel 486 CPU.

Table 7 shows the forecast for the number of nodes, ports and calls per hour that can be supported by the 8-Port ITG Trunk Leader/DCHIP Card when the Leader Card is not configured with any ports. Case I assumes that the call mix is 50% call origination and 50% call termination and as a result it takes approximately 200 ms per call on average for the Leader Card to assist in the call setup/tear-down process. If, for example, the network size is 25 nodes, then the Leader Card can support 10648 calls per hour (or 19166 CCS, assuming 180 second average holding time). Assuming 15.3 calls per hour per port, that translates into 695 ports, which is approximately 87 Follower Cards. If, however, the calls are 100% incoming calls (see Case II below), then the call processing assistance real time is approximately 400 ms per call and the Leader Card can support 43 Follower Cards.

Note that the Leader Card capacity that is expressed in terms of the number of calls per hour is derived from the real time measurements and is independent of customer traffic assumptions. The Leader Card capacity expressed in terms of the number of CCS and the number of ports (and the number of Follower Cards) is derived from the calls per hour value, based on the traffic assumptions of 180 second average holding time (AHT) and 15.3 calls per hour per port, respectively. If these parameters do not reflect a specific customer's traffic requirements, the capacities in terms of CCS, the number of ports, and the number of Follower Cards can be re-computed using the following procedures:

Number_of_Ports = Calls_per_hour / Customer_calls_per_hour_per_port
Number_of_Follower_Cards = Number_of_Ports / 8

Table 8 shows the forecast of the Leader Card real time capacity for the case that four or eight ports are configured to carry voice traffic with G.711 codec and 10 ms voice sample size and Table 9 shows the forecast for the case with the G.729A codec with Voice Activity Detection (VAD) and Silence Suppression, and 30 ms voice sample size. For both tables, 40% voice activity is assumed.

Table 7
8-Port ITG Leader Card RT Capacity - No voice (or fax) port configured

	Case I 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
Network Size (#nodes)	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
2	**11695**	21052	763	**95**	**5848**	10526	381	**48**
10	**11326**	20387	739	**92**	**5663**	10194	369	**46**
25	**10648**	19166	695	**87**	**5324**	9583	347	**43**
50	**9125**	16424	595	**74**	**4562**	8212	298	**37**
100	**7629**	13733	498	**62**	**3815**	6866	249	**31**
150	**7017**	12631	458	**57**	**3509**	6316	229	**29**
200	**6397**	11514	417	**52**	**3198**	5757	209	**26**
300	**5948**	10707	388	**49**	**2974**	5353	194	**24**

Table 8
8-Port ITG Leader Card RT Capacity - G.711, 10ms voice sample, 4 or 8 ports configured (Part 1 of 2)

	Case I 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
Network Size (#nodes)	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
Leader Card with 4 ports configured for G.711 with 10ms sample size								
2	**7269**	13085	474	59	**3635**	6542	237	30
10	**6900**	12420	450	56	**3450**	6210	225	28
25	**6222**	11199	406	51	**3111**	5599	203	25
50	**4698**	8457	306	38	**2349**	4229	153	19
100	**3203**	5766	209	26	**1602**	2883	104	13
150	**2591**	4664	169	21	**1296**	2332	85	11
200	**1971**	3547	129	16	**985**	1774	64	8
300	**1522**	2740	99	12	**761**	1370	50	6
Leader Card with 8 ports configured for G.711 with 10ms sample size								
2	**3462**	6231	226	28	**1731**	3115	113	14

Table 8
8-Port ITG Leader Card RT Capacity - G.711, 10ms voice sample, 4 or 8 ports configured (Part 2 of 2)

	Case I 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
Network Size (#nodes)	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
10	**3092**	5566	202	25	**1546**	2783	101	13
25	**2414**	4345	157	20	**1207**	2172	79	10
50	**891**	1603	58	7	**445**	802	29	4

Table 9
8-Port ITG Leader Card RT Capacity - G.729 Annex AB, 30ms voice sample, 4 or 8 ports configured

	Case I 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
Network Size (#nodes)	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
Leader Card with 4 ports configured for G.729 Annex AB with 30ms sample size								
2	**9415**	16948	614	77	**4708**	8474	307	38
10	**9046**	16283	590	74	**4523**	8142	295	37
25	**8368**	15062	546	68	**4184**	7531	273	34
50	**6845**	12320	446	56	**3422**	6160	223	28
100	**5349**	9629	349	44	**2675**	4814	174	22
150	**4737**	8527	309	39	**2369**	4264	155	19
200	**4117**	7410	269	34	**2058**	3705	134	17
300	**3668**	6603	239	30	**1834**	3301	120	15
Leader Card with 8 ports configured for G.729 Annex AB with 30ms sample size								
2	**7615**	13708	497	62	**3808**	6854	248	31
10	**7246**	13043	473	59	**3623**	6522	236	30
25	**6568**	11822	428	54	**3284**	5911	214	27
50	**5045**	9080	329	41	**2522**	4540	165	21
100	**3549**	6389	232	29	**1775**	3194	116	14
150	**2937**	5287	192	24	**1469**	2644	96	12
200	**2317**	4170	151	19	**1158**	2085	76	9
300	**1868**	3363	122	15	**934**	1681	61	8

24-Port ITG Leader and DCHIP Card Real Time Capacity

The 24-Port ITG Trunk Card is the NT0961 based on the Intel Pentium CPU. The 24-Port Leader card real time capacity analysis is as follows. The following assumptions are made:

1. Average Hold Time (AHT) is equal to 180 seconds, and traffic per port is equal to 28 Centi Call Seconds (CCS). This corresponds to a call rate of 15.6 calls per hour.

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 either terminate or originate on the Leader card. Voice ports are allowed on the Leader card.

4. It is also assumed that when VAD has been enabled in MAT, 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). And 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.

It has been determined via measurements that the Leader card can support 1920 IP ports, all codecs with payload sizes of 10, 20 and 30 milliseconds, and VAD status equal to “on” with 24 voice ports configured. Under the above set of assumptions, this corresponds to a total of 53,760 CCS, or 29,867 calls per hour. Note that with 24 voice ports per card, 1920 IP ports corresponds to 80 Follower cards.

It also supports 1920 IP ports, all codecs with payload sizes of 20 and 30 milliseconds, and VAD when VAD has been disabled in MAT with 24 voice ports configured. If the payload size is equal to 10 milliseconds, the number of supported IP ports, or Follower cards can be determined from Tables 10 and 11. In both tables, 50% voice activity is assumed on the voice ports.

Each Table consists of two cases. Case I assumes that the call mix is 50% call origination and 50% call termination. Case II assumes that the call mix is 0% call origination and 100% call termination. These two cases are considered because the call processing assist time for originating calls on the Leader card is negligible, while for the terminating call, this time is non-negligible.

Table 10
24-Port ITG Leader Card RT Capacity - G.711, 10 ms voice sample, VAD off

	Case I 50% Call Origination, 50% Call Termination				Case II 100% Call Termination			
#Voice Port Configured	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
0 - 18	29867	53760	1920	80	29867	53760	1920	80
20	29867	53760	1920	80	24781	44605	1593	66
22	29867	53760	1920	80	17736	31925	1140	47
24	21383	38490	1375	56	10692	19245	687	28

Table 11
24-Port ITG Leader Card RT Capacity - G.729 Annex AB, 10 ms voice sample, VAD off

	Case I 50% Call Origination, 50% Call Termination				Case II 100% Call Termination			
#Voice Port Configured	Calls/Hr	CCS	Number of ports	Number of Follower Cards	Calls/Hr	CCS	Number of ports	Number of Follower Cards
0 - 22	29867	53760	1920	80	29867	53760	1920	80
24	29867	53760	1920	80	26048	46887	1675	69

Provisioning ITG ISL TIE trunks and routes

ITG ISL TIE trunks are provisioned based on average busy hour traffic tables, using the calculated amount of traffic between ESN/ITG nodes. Table 12 shows the number of trunks required based on average busy hour CCS for a 1% blocking Grade of Service. Table 13 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, may be preferred if overflow routing is available through the PSTN, circuit-switched VPN, or ITG ISL TIE trunks.

Table 12
Trunk traffic—Poisson 1 percent 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
20	399	40	964	60	1565	80	2184	100	2816

Note: For trunk traffic greater than 4427 CCS, allow 29.5 CCS per trunk.

Table 12
Trunk traffic—Poisson 1 percent blocking Grade of Service (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
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 13
Trunk traffic—Poisson 10 percent 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
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

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

Table 13
Trunk traffic—Poisson 10 percent blocking Grade of Service (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
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.

WAN route engineering

After T-LAN traffic is calculated, determine the bandwidth requirement for the WAN. In this environment, bandwidth calculation is based on network topology and destination pair.

Before network engineering can begin, the following network data must be collected:

- Obtain a network topology and routing diagram.
- List the sites where the ITG nodes are to be installed.
- List the site pairs with ITG 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).

To illustrate this process, the following multi-node engineering example is provided.

Table 14 summarizes traffic flow of a 4-node ITG network.

Table 14
Example: Traffic flow in a 4-node ITG 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 based on a per ITG card basis. During call set up negotiation, only the type of codec available at both destinations will be selected. When no agreeable codec is available at both ends, the default codec G.711 will be used.

> ***Note:*** It is recommended that all cards in an ITG system have the same image. If multiple codec images are used in an ITG network, the calls will default to the G.711 group when the originating and destination codecs are different.

The ITG port requirement for each node is calculated by counting the traffic on a per node basis (based on Table 12 on page 94). The port requirements for the example in Table 14 are given in Table 15 on page 99.

Table 15
Example: Determine ITG card requirements

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

Assuming that the preferred codec to handle VoIP calls in this network is G729 Annex AB.

Table 16 summarizes the WAN traffic in kbit/s for each route. Note that 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 16
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.729 Annex AB with 30 ms payload, the bandwidth use 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% would give us the 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. voice call (33.7 kbit/s as compared to. 11.2 kbit/s) in this example.

The example in this section deals with nodal traffic calculation in both T-LAN and WAN. It indicates incremental bandwidth requirement to handle voice on data networks.

Assess WAN link resources

For most installations, ITG traffic will be routed over WAN links within the intranet. WAN links are the most expensive repeating expenses in the network and they often are the source of 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 obtain financial approval, provision and upgrade. For these reasons, it is important to determine the state of WAN links in the intranet before installing the ITG network.

Each voice conversation, (G.729 Annex AB 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

The starting point of this assessment is to 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 ITG traffic. Alternately use the `traceroute` tool (see “Measure intranet QoS” on page 114).

The next step is to find out 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. In order to

be consistent with the dimensioning considerations (see “ITG traffic engineering” on page 76), obtain the busy period (e.g. peak hour) utilization of the trunk. Also, because WAN links are full-duplex and that 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 that 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, say at 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 that used in this example; in the event of link failures, there needs to be spare capacity for traffic to be re-routed.

Some WAN links may actually 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 a “logical capacity” limit. The technician needs to obtain, in addition to the physical link capacity, the QoS parameters, the important ones being CIR (committed information rate) for Frame Relay, and MCR (maximum cell rate) for ATM.

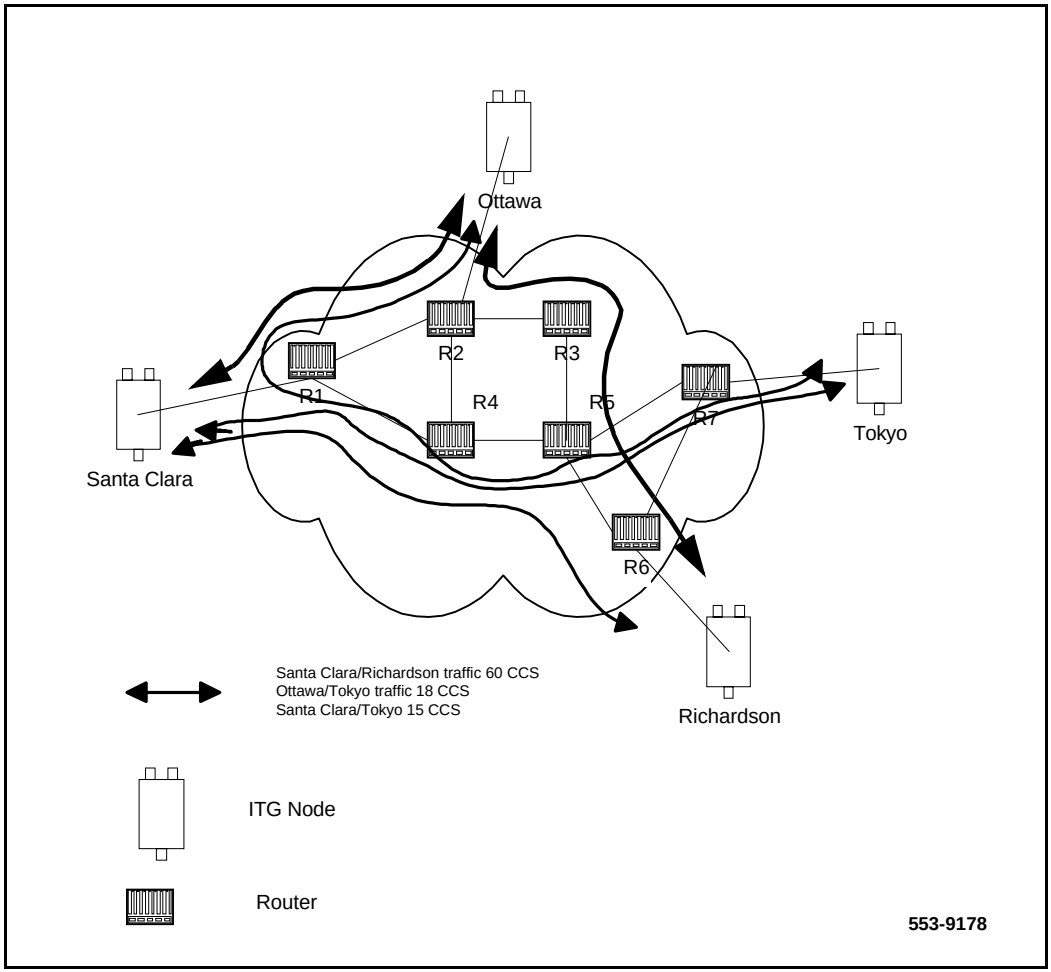
The difference between the current capacity and its allowable limit is the available capacity. For example a T1 link utilized at 48% during the peak hour, with a planning limit of 80% had an available capacity of about 492 kbit/s.

Estimate network loading caused by ITG traffic

At this point, the technician has enough information to "load" the ITG traffic on the intranet. Figure 13 illustrates how this is done on an individual link.

Suppose the intranet has a topology as shown in Figure 13, and you want to predict the amount of traffic on a specific link, R4-R5. From the “ITG 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 ITG 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.

Figure 13
Calculate network load with ITG traffic



To complete this exercise, total the traffic flow from every site pair to calculate the load on each routed and loaded to the link.

Route Link Traffic Estimation

Routing information for all source-destination pairs needs to 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
1   r6 (10.8.0.1) 1 ms  1 ms  1 ms
2   r5 (10.18.0.2) 42 ms  44 ms  38 ms
3   r4 (10.28.0.3) 78 ms  70 ms  81 ms
4   r1 (10.3.0.1) 92 ms  90 ms  101 ms
5   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 or not for each of the source-destination pairs. Use the `-g` loose source routing option[1], as shown in the following command syntax:

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

The `traceroute` program identifies the intranet links that transmit ITG traffic. For example, if traceroute of four site pairs yield the results shown in Table 17, then the load of ITG traffic per link can be computed as shown in Table 18:

Table 17
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

1. The option letter can be different depending on vendor implementation

Table 18
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

Decision: Enough capacity?

Table 19 arranges the computations so that for each link, the available link capacity can be compared against the additional ITG load. For example, on link R4-R5, there is plenty of available capacity (492 kbit/s) to accommodate the additional 24 kbit/s of ITG traffic.

Table 19
Computation of link capacity as compared to ITG load

Link		Utilization (%)		Available capacity (kbit/s)	Incremental ITG 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
Etc.							

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 you assess network resilience by conducting link and node failure analysis. By simulating failures, 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, one or more of the following options can be decided:

- Use the G.723 codec series. Compared to the default G.729 Annex AB 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 you must consider the impact of incremental ITG traffic on routers and LAN resources in the intranet. Perhaps the ITG traffic will traverse LAN segments that are saturated, or routers whose CPU utilization is high.

QoS Evaluation Process Overview

There are two main objectives when dealing with the QoS issue in an ITG network: (1) to predict the expected QoS, (2) to evaluate the QoS after integrating ITG traffic into the intranet. The process for either case is similar, one is without ITG traffic and one is with. The fine difference between them will be discussed at an appropriate place.

In the process, it is assumed that the Ping program is available on a Window 95 or NT PC, or some network management tool which can collect delay and loss data that is accessed to the T-LAN connecting to the Router going out to the Intranet:

1 Use *ping* or 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 Look up a QoS chart (Figure 5,6,7) or Table 24 to predict the QoS categories (excellent, good, fair or poor).

4 If a customer wants to manage the QoS in a more detailed fashion, he/she can re-balance the values of delay compared to loss by adjusting ITG system parameters, such as preferred codec, payload size, routing algorithm, etc. 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.

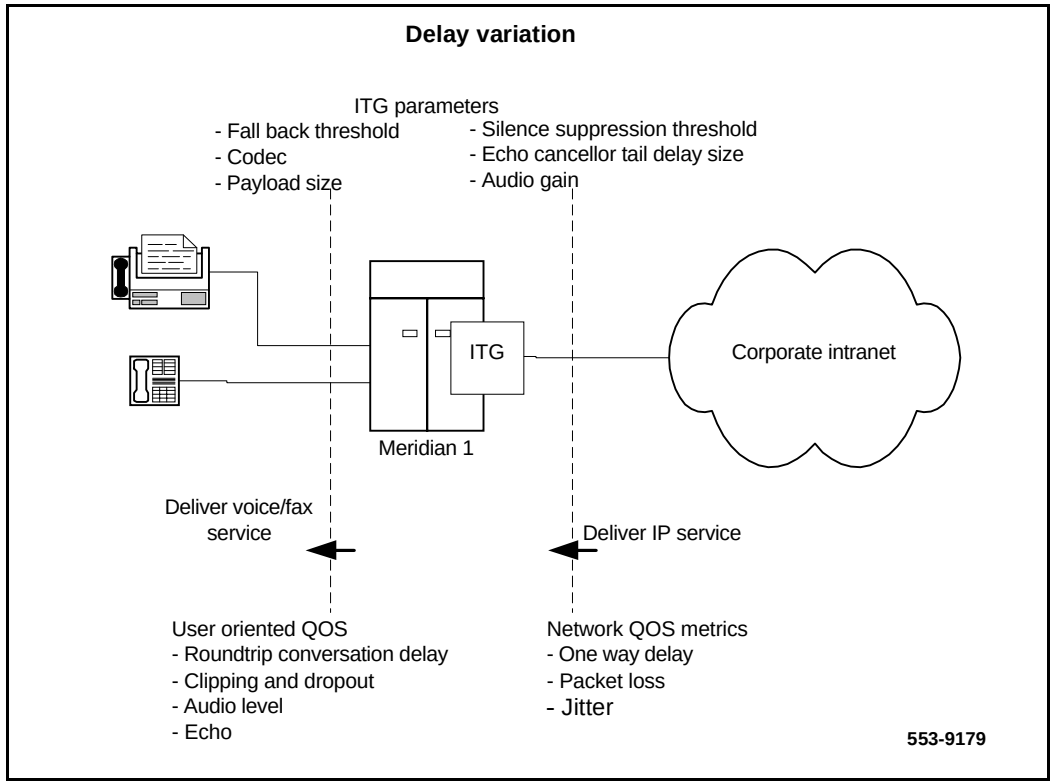
Set QoS

The users of corporate voice and data services expect these services to meet some perceived quality of service (QoS) which in turn influence 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 and ITG system, Figure 14 on page 109 shows the relationship between users and services:

From the diagram it can be seen that there are two interfaces that the technician needs to consider.

Figure 14
Relationship between users and services



- The Meridian 1 (including the ITG nodes) interfaces with the end users; voice services offered by the Meridian 1 need to meet user-oriented QoS objectives.
- The ITG 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.” The ITG translates the QoS objectives set by the end-users into IP-oriented QoS objectives. The guidelines call these objectives *intranet QoS objectives*.

The ITG node can be enabled to monitor the intranet's QoS. In this mode, two parameters, the *receive fall back threshold* and the *transmit fall back threshold*, on the ITG node then dictate the minimum *QoS level* of ITG network. Note that the fall back thresholds are set on a pair site pair basis.

The *QoS level* is a user-oriented QoS metric and takes on one of these four settings: excellent, good, fair, and poor, which indicate the quality of voice service. ITG periodically calculates the prevailing QoS level per site pair based on its measurement of

- one-way delay
- *packet loss, and*
- codec

and when the QoS level is below the fall back 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 fall back threshold levels for that particular destination, that call is not accepted by the originating ITG node; instead the call is re-routed by Meridian 1 ESN features over traditional circuit-switched voice facilities.

The following graphs (Figures 15, 16, and 17) show the operating regions in terms of *one-way delay* and *packet loss* for each codec and required QoS level as determined by ITG. 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.729A and then G.723.1 (6.4 kbp/s) and lastly G.723.1 (5.3 kbp/s). These graphs 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 10%. It is recommended that fax services be supported with the ITG operating in either the Excellent or Good QoS level. Avoid offering fax services between site pairs that can guarantee no better than a Fair or Poor QoS level.

Figure 15
QoS levels with G.729A codec

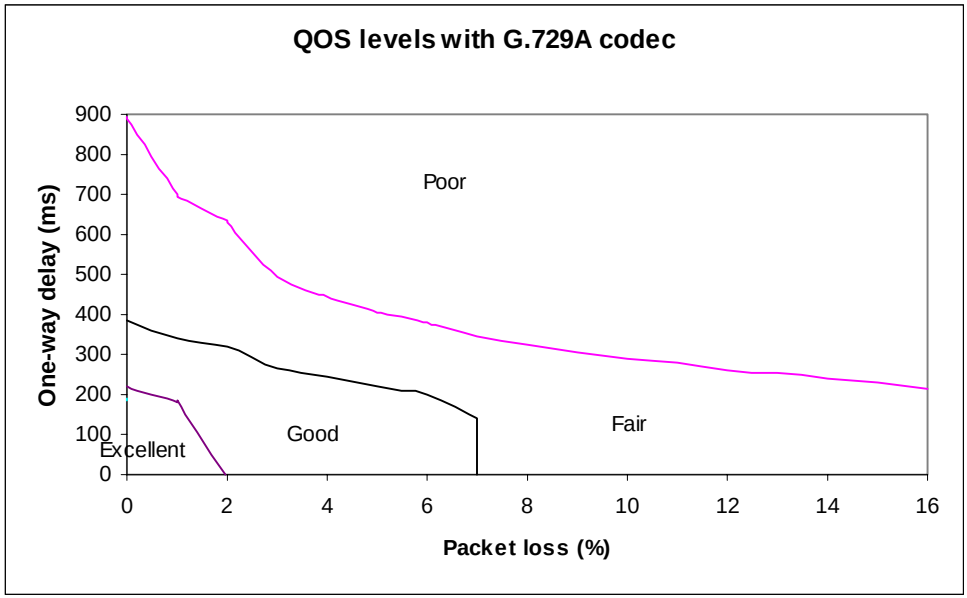


Figure 16
QoS level with G.711A/G.711U codec

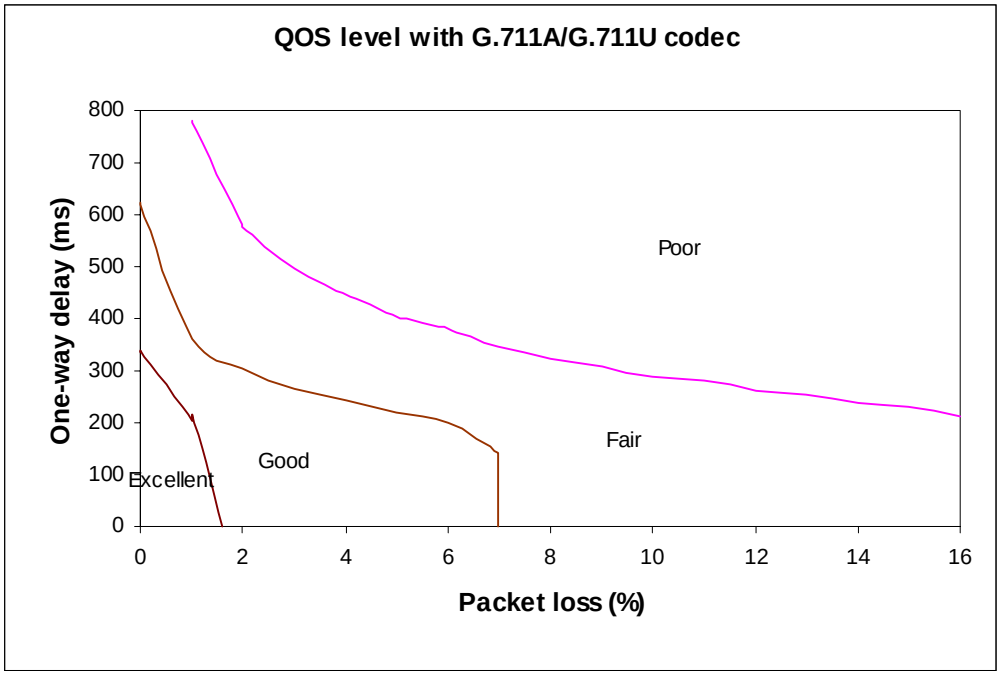
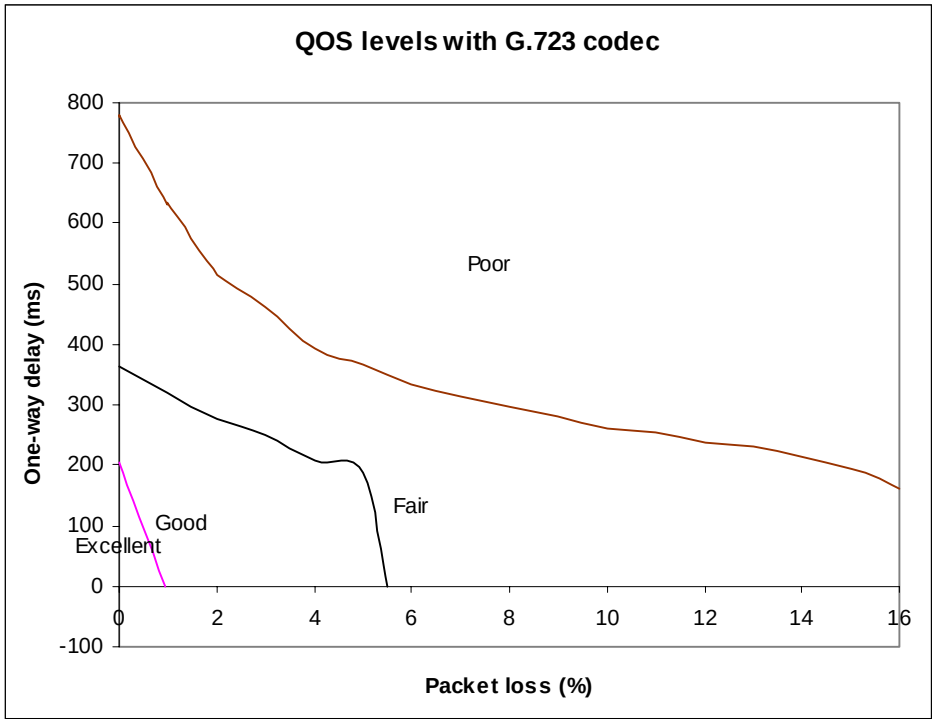


Figure 17
QoS levels with G.723



Measure intranet QoS

You can measure end-to-end delay and error characteristics of the current state of the intranet. These measurements help you set acceptable QoS standards when using the corporate intranet to transmit voice services.

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. The output of `ping` is like the following:

```
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 ITG node can experience, the `ping` host must be on a working LAN segment attached to the router intended to support the ITG node. The selection of destination host is just as important, following these same guidelines for the source host.

The size of the `ping` probe packets must be set to 60 bytes to approximate the size of probe packets sent by the ITG that are used in determining when new calls need to fall back.

Some implementations of `ping` support the `-v` option[1] for setting the TOS. The ITG ISL Trunk allows you to set the 8-bit DiffServ/TOS field to any value specified by the IP network administrator for QoS management purposes. For example, if you enter a decimal value of 36 in MAT, this is interpreted as TOS Precedence = Priority and Reliability = High. Note that if the craftsperson made `ping` measurements on an intranet that does prioritization (see "Queue management" on page 128) 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.

Notice from the `ping` output the variation of *rtt*. 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 and stores the samples in a raw data file. The file can then be to be analyzed later using spreadsheet and other statistics packages. You can check 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 ITG 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. In fact use the same `ping` host setup to measure end-to-end error, and as in making delay measurement, use the same packet size parameter.

Sampling error rate, however, requires taking multiple `ping` samples (at least 30 to be statistically significant). Thus, 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).

1. Within the 8-bit TOS field are 4 TOS bits from bits 4 to 7, which would be 0010 binary or 2 decimal

Adjust ping measurements

One-way as compared to roundtrip

The `ping` statistics are based on round trip measurements, whereas 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 ITG 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 would include components outside the intranet. The `ping` statistic for delay needs to be further modified by adding 93 ms to account for the processing and jitter buffer delay of the ITG nodes.

No adjustment needs to be made for error rates.

If the intranet measurement barely meets the round trip QoS objectives, the craftsperson needs to be aware that 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 the ITG. To determine which `ping` samples to ignore, first calculate the average *one-way delay* based on all the samples. Then add 500 ms to that. This is the maximum delay. All samples whose one-way delay exceed this maximum are considered as late packets and are 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 ITG 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 may want to know whether traffic fluctuation in their Intranet will reduce the user's QoS.

Table 20 provides a sample measurement of network delay and packet loss for the G.729A codec between various nodes.

Table 20
Sample Measurement Results for G.729A codec

Destination pair	Measured One way delay (ms)		Measured Packet loss (%)		Expected QoS level (See page 143)	
	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
Richardson/ Tokyo	305	345	2.2	2.6	Good	Fair
Ottawa/ Tokyo	260	286	2.4	2.8	Good	Fair

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 ITG will calculate mean only and not standard deviation, it will confirm the “excellent” rating (if the objective is set for excellent, it will not fallback to alternate facilities), but the customer will have up to 50% chance to experience a service level inferior to “excellent” level.

As a contrast, the site pair Santa Clara/Ottawa which has both QoS levels of mean and mean+σ falling in the excellent region. The customer will have more confidence that (better than 84% chance under the assumption of Normal distribution) during peak traffic period, the “excellent” service level is likely to be upheld.

Other measurement considerations

The `ping` statistics described above measure the intranet prior to ITG installation, which means that the measurement does not take into consideration the expected load offered by the ITG users.

If the intranet capacity is tight and the ITG traffic significant, you should consider making intranet measurements under load. Load can be applied using traffic generator tools; the amount of load should match the ITG offered traffic estimated in “ITG traffic engineering” on page 76.

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 http://www.caida.org. Some of these are delay monitoring tools that include features like timestamping, plotting, and computation of standard deviation.

Decision: does the intranet meet expected ITG QoS?

At the end of this measurement and analysis, you should have a good indicator whether the corporate intranet as it stands can deliver adequate voice and fax services. Looking at the "Expected QoS level" column in Figure 20, the craftsperson can gauge the QoS level for each site pair.

In order to offer voice and fax services over the intranet, the technician should keep the network within a "Good" or "Excellent" QoS level at the Mean+σ 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 being “Good”, the technician will need to evaluate the options and costs for upgrading the intranet. Using Appendix A, the technician can estimate the amount of *one-way delay* that needs to be reduced to raise the QoS level. “Fine-tune Network QoS” on page 119 provides guidelines for reducing *one-way delay*. Often this involves a link upgrade, a topology change, or implementation of QoS in the network.

The technician can decide 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, you need to carefully monitor the QoS level, reset expectations with the end users, and be receptive to user feedback.

Fine-tune Network QoS

Topics presented in this section deal with issues that will impact the QoS of ITG traffic. They are informative for understanding 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 ITG network engineering.

Further network analysis

This section describes actions that could 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:

- Reduce link delay
- Reduce hop count
- Adjust jitter buffer size
- Implement IP QoS mechanisms

Components of delay

End-to-end delay is contributed by many delay components; the major components of delay are described as follows.

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

This 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 given by the following formula:

Serialization delay in ms = 8*(IP packet size in bytes)/(link bandwidth in kbit/s)

Table 21 shows what the serialization delay for voice packets on a 64kbit/s and 128kbit/s link. The serialization delay on higher speed links are considered negligible.

Table 21
Serialization delay

Codec	Frame duration	Serialization delay over 64kbit/s link (ms)	Serialization delay over 128kbit/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.729 Annex AB	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

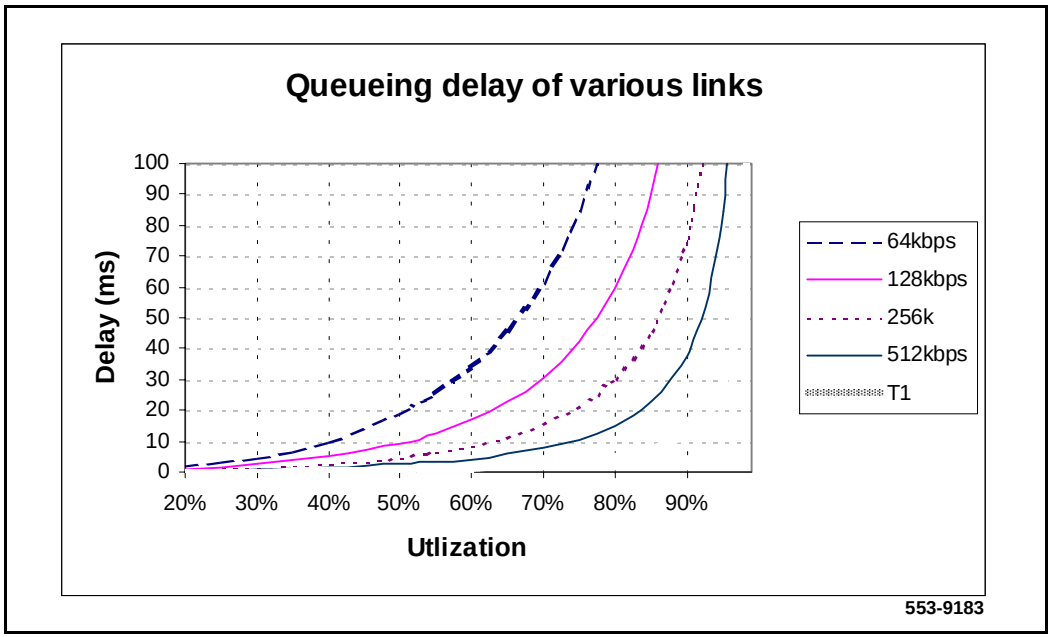
Queueing delay is the time it takes for a packet to wait in transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queueing time in ms is estimated by the formula:

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 lies between 250 and 500 bytes. Figure 18 displays the average queueing delay of the network based on a 300-byte average packet size.

Figure 18
Queuing delay of various links



As can be seen in Figure 18, queueing delays can be significant for links with bandwidth under 512 kbit/s, whereas with higher speed links they 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.

ITG system delay

The transmitting and receiving ITG nodes together contribute a processing delay of about 33 ms to end-to-end delay. This is the amount of time required for the encoder to analyze and packetize speech, and by the decoder to reconstruct and depacketize the voice packets.

There is a second component of delay which occurs on the receiving ITG 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

There are other delay components but they are generally considered very minor.

- 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 on the order of a few milliseconds.
- LAN segment delay. The transmission and processing delay of packets through a healthy LAN subnet is on the order of just one or two milliseconds.

Reduce link delay

In this and the next few sections, the guidelines examine different ways of cutting down one-way delay and packet loss in the ITG network.

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 is the link delay. Link delay can be reduced by:

- Upgrading link capacity. This reduces the serialization delay of the packet, but also 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 120 and “Queuing delay” on page 121. Before upgrading a link, you must check both routers connected to the link intended for the upgrade and ensure that router configuration guidelines are complied to.
- 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 128.

To determine which links should be considered for upgrading, first list all the intranet links used to support the ITG 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.

Lets say that a 256kbit/s link from router1 to router2 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
1  router1 (10.8.0.1) 1 ms  1 ms  1 ms
2  router2 (10.18.0.2) 42 ms  44 ms  38 ms
3  router3 (10.28.0.3) 78 ms  70 ms  81 ms
4  router4 (10.3.0.1) 92 ms  90 ms  101 ms
5  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 18 on page 121, if you upgrade this link to T1, you can shave about 19 ms 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. These are some of the ways to reduce hop count:

- Attach the T-LAN 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. You can connect colocated nodes into one larger and more powerful router.

These guidelines affect the whole intranet, as they tamper with network architecture, design and policies. To proceed with this involves considering cost, political and IP design issues, topics which are beyond the scope of this document.

Adjust jitter buffer size

The jitter buffer parameters directly affect the end-to-end delay. Lowering the voice playout settings decreases one-way delay, but the decrease comes at the cost of giving less waiting time for voice packets that arrive late. Refer to “ITG Trunk DSP profile settings” on page 135 for guidelines for re-sizing the jitter buffer.

Reduce packet errors

Packet errors in intranets are generally correlated with congestion somewhere in the network. Bottleneck links occur where the packet errors are high because packets get dropped when they arrive faster than the link can transmit them. The task of upgrading highly utilized links can remove the source of packet errors on a particular flow. Also an effort to reduce hop count gives fewer opportunities for routers and links to drop packets.

Other causes of packet errors not related to queueing delay are as follows:

- Poor link quality. The underlying circuit may have transmission problems, high line error rates, subject to frequent outages, etc. Note that the circuit may 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. Find out what the threshold CPU utilization level is, and check if any suspect router conforms to the threshold. The router may 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 may also be dropped on under-engineered or faulty LAN segments.
- Jitter buffer too small. Packets that arrive at the destination ITG, but too late to be placed in the jitter buffer are essentially loss packets as well. Refer to "Adjust jitter buffer size" on page 124.

Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation may 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 quality of service than the other.

The `traceroute` program can be used to uncover these routing anomalies. Subsequently, 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 ITG installation is large. To this end, commercial network modeling tools exist to analyze what-if scenarios of predicting the effect of topology, routing, bandwidth, etc. changes to the network. They work with an existing network management system to load current configuration, traffic and policies into tool. Network modeling tools can assist the technician to analyze and try out any of the recommendations given in this document to predict how delay and error characteristics would change.

Implement QoS in IP networks

Today's corporate intranets developed because of the need to support data services, services which for the most part a "best effort" IP delivery mechanism suffices. Standard intranets are designed to support a set of Quality of Service (QoS) objectives dictated by these data services.

When an intranet takes on a real-time service, the users of that service will impose additional QoS objectives in the intranet; some of these targets may be less stringent compared with those imposed by current services, while other targets would be more stringent. For intranets not exposed to real-time services in the past but now need to deliver ITG traffic, it is likely that the QoS objectives pertaining to delay will 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, essentially a "best-of-breed" solution. This for example would improve the quality of data services, even though most applications may not perceive a reduction of say 50ms in delay. Improving the network results in one that would be adequately engineered for voice, but over-engineered for data services.

Another approach is to consider using QoS mechanisms in the intranet, the goal of which is to provide a more cost-effective solution to engineering the intranet for non-homogenous traffic types. Unfortunately IP QoS mechanisms are still relatively recent technology, hardly implemented on intranets, and difficult to predict the consequences.

This section outlines what QoS mechanisms can work in conjunction with the ITG node, and with what new intranet-wide consequences if implemented.

Traffic mix

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

If an intranet is designed solely to deliver ITG traffic, and all traffic flows are 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 is primarily supporting data and other services. When planning to offer voice services over the intranet the technician needs to assess the following:

- Are there existing QoS mechanisms? What kind? The ITG traffic should take advantage of established mechanisms if possible.
- What is the traffic mix? If the ITG traffic is small compared to data traffic on the intranet, then IP QoS mechanisms can suffice. If ITG traffic is significant, data services might be impacted when those mechanisms are biased toward ITG 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 would appear to be congested at one time, and then followed by a period of under-utilization. There are two consequences:

- poor efficiency of WAN links, and
- ITG traffic streams are unfairly affected

ITG support for TOS field and IP QoS

You can configure the DiffServ/TOS value for Control and Voice packets, if required, to obtain better QoS over the IP data network (LAN/WAN). Do not change DiffServ/TOS from default value of 0 unless instructed by the IP network administrator.

The Type of Service (TOS) byte or Differentiated Service (DiffServ) code point determine 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.

DiffServ/TOS 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.

If the intranet provides differentiated services based on the DiffServ/TOS field, then the ITG Trunk and other traffic marked with this DiffServ/TOS value could be delivered with the goal of meeting this class of traffic’s QoS objectives.

> ***Note:*** It is not a requirement to have a router which has priority IP packet routing capability. The ITG can function without priority routing mechanisms if you design the intranet to minimize traffic congestion through the WAN backbone links and routers. Refer to “Implement QoS in IP networks” on page 126.

Queue management

From “Queuing delay” on page 121, 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. To this end, Class-Based Queueing (CBQ) can be considered for implementation on these routers, with the ITG traffic prioritized against other traffic. Classed-based queueing however may be CPU-intensive and may not scale well when applied on high-bandwidth links, hence if this is to be implemented for the first time on the intranet do so selectively. Usually CBQ is implemented at edge routers, or entry routers into the core.

The global synchronization situation described in “TCP traffic behavior” on page 127 can be countered using a buffer management scheme which discards packets randomly as the queue starts to exceed some threshold. WRED (Weighted Random Early Detection), 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, WRED should be implemented 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 ITG 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 need to 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 ITG

The following IP applications and protocols are used by ITG 2.0, and must be transmitted across the customers intranet by all IP routers and other network equipment. This information should be validated and included in the ITG network engineering guidelines.

ITG Management Protocols

ITG uses the UDP and TCP port numbers for SNMP, Telnet, and FTP, i.e. the default port numbers for these common IP applications.

ITG H.323 Voice Gateway Protocols

H.245 Call Setup Signaling Protocol uses TCP port 1720.

Realtime Transport Protocol (RTP) uses UDP port 2300-2363.

ITG QoS Network Probing Proprietary Protocol

QoS probing uses UDP port 5000.

ITG ISL Trunk card connections

10/100BaseT Ethernet ports

The ITG ISL Trunk card has two Ethernet ports. One 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, or T-LAN. A 10BaseT port on the

motherboard with a connector on the I/O panel breakout cable transmits ITG system management traffic and D-channel and connects to the Embedded LAN, or E-LAN.

RS-232 serial ports

The ITG ISL 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 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.

Set up a system with separate subnets for voice and management

It is highly recommended that the customer place the voice and management LANs on separate dedicated subnets, separated by a router.

The ITG cards have two Ethernet ports per card, so the ITG system can support two different networks for the voice interface (Telephony LAN or T-LAN) and management interface (Embedded LAN, or E-LAN) connections. The advantages of this setup are:

- to optimize Voice over IP performance on the Telephony LAN (T-LAN) segment by segregating it from Embedded LAN (E-LAN) traffic and connecting the T-LAN as close as possible to the WAN router
- to make the amount of traffic on the T-LAN more predictable for QoS engineering
- to optimize E-LAN performance, e.g., for Symposium Call Center Server (SCCS) and Call Pilot functional signaling, by segregating the E-LAN from ITG T-LAN VoIP traffic
- to enhance network access security by allowing the modem router to be placed on the E-LAN, which can be isolated from the customer's enterprise network (C-LAN) or have access to/from the C-LAN 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. The single subnet configuration eliminates the use of the Ethernet voice interface with its associated Network Activity LEDs.

Subnet configurations

ITG 2.0 systems with only 8-port cards can configure both single and dual subnets.

ITG 2.0 systems with both 8- and 24-port cards can have both single and dual subnets. The dual subnet option is recommended. Single subnets are only allowed if the E-LAN/T-LAN connection is on a 10BaseT hub or switch.

ITG 2.0 systems with only 24-port cards must configure a dual subnet.

The following restrictions apply:

- The Leader 0 and Leader 1 cards must co-reside on a single T-LAN with the Node IP Address.
- Follower cards can reside on separate T-LANs.
- All ITG cards belonging to the same node must co-reside on the same E-LAN.

Single subnet option for voice and management

Although not recommended, the "single subnet" option for voice and management can be used where the combined voice and management traffic on the E-LAN is so low that there is no impact on packetized voice QoS performance, or the customer is willing to tolerate occasional voice quality impairments caused by excessive management traffic, and there is no modem router on the ITG E-LAN because remote support access is provided by Remote Access Server (RAS) on the C-LAN or remote support access is not required, and there is no firewall router between the E-LAN and the C-LAN.

Multiple ITG nodes on the same E-LAN and T-LAN segments

There are several configurations where it can be acceptable to put multiple ITG nodes on the same dedicated E-LAN and T-LAN segments (separate subnets), or on a dedicated E-LAN/T-LAN segment (single subnet):

1 Several ITG nodes belonging to the same customer in the same Meridian 1 PBX may be configured to route calls with different CODECs depending on the digits dialed or the NCOS of the originating terminal, or to limit the maximum number of ITG calls to a particular destination node. The traffic engineering considerations on the T-LAN should determine how many different ITG nodes can be configured on the same LAN segment.

2 Layer Two (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.

You must not place other IP devices, either Nortel Networks' or other vendors' products, on the same T-LAN subnet with the ITG nodes.

Setting up the E-LAN or management subnet

The management LAN, or E-LAN, is 10BaseT Ethernet. Very little traffic is generated by the ITG node on this network. Cards generate this traffic when the cards have been reset and are looking for the active leader, and when SNMP traps are emitted due to ITG card events and errors. A standard configuration is an 8-port passive hub connecting the ITG system management Ethernet to the MAT PC through the E-LAN. If the E-LAN also carries functional signalling traffic for Symposium Call Center Server (SCCS), Small Symposium Call Center (SSCC), or Call Pilot multimedia message server, then the E-LAN can be configured on a switching hub to maximize data throughput.

Selecting public or private IP addresses

The customer must consider a number of factors to determine if the T-LAN and E-LAN 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 set up the T-LAN and E-LAN, 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 renumbering 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 T-LAN and E-LAN, but will consume limited resources.

This will have the same result as the private IP address solution, but the E-LAN will be accessible from the Internet without NAT.

T-LAN engineering

The ITG nodes must be connected to the intranet so as to minimize the number of router hops between the Meridian 1, provided 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 over IP Quality of Service. It is recommended that up to 4 cards (2 cards for Class B service) share the same 10BaseT LAN broadcast collision domain, provided that the preferred codec throughout the ITG network is set to G.729 Annex AB, G.729A, G.723 5.3K, or G.723 6.3K with 30 ms default payload size and default fax settings. (In a passive Ethernet hub, all ports on the hub share one 10Mbit/s collision domain for all connected MAC layer (Ethernet) addresses. In a switched Ethernet hub, each port has its own collision domain.) Due to the much higher

bandwidth use of the G.711 codec series, it is recommended that no more than two ITG cards share the same LAN collision domain in a G.711-only ITG network.

If you use a mixed codec ITG network or use a non-default payload size or fax settings, then you must use the LAN bandwidth consumption in Table 5 to estimate the amount of LAN bandwidth used by each card. It is recommended that you do not use the 10Mbit/s collision domain beyond 25-30% at the peak.

If the uplink from the T-LAN hub (either passive or switched) to the router is 10Mbit/s, then the maximum number of ITG cards allowed per hub is equal to the limit described in the previous paragraph. If the uplink is 100Mbit/s, then the maximum number of ITG cards allowed on the switched hub is subject to the limits described in the "Leader Card Real Time Engineering" section of this document.

You may want to consider implementing LAN resiliency. This is achieved by provisioning Leader and Follower cards on separate Ethernet hubs (but served by the same router). In this design the ITG node can provide voice services when one of the hubs fails.

The ITG node and the T-LAN router should be placed as close to the WAN backbone as possible, again to minimize the number of router hops, segregate constant bit-rate Voice over IP traffic from bursty LAN traffic, and simplify the end-to-end Quality of Service engineering for packet delay, jitter, and packet loss. If an access router separates the ITG node from the WAN router, there should be a high-speed link (e.g., Fast Ethernet, FDDI, SONET, OC-3c, ATM STS-3c) between the access router and the WAN backbone router.

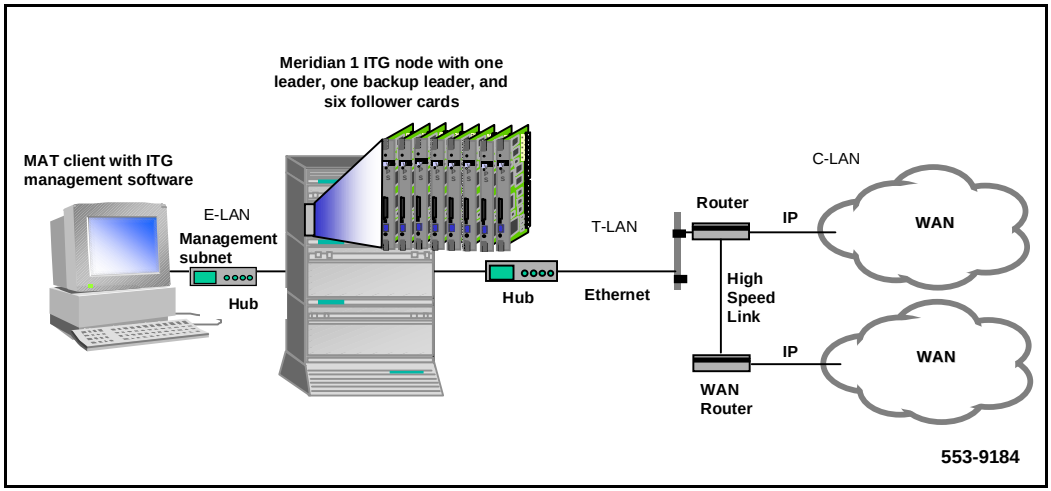
Setting the Quality of Service threshold for fallback routing

The Quality of Service thresholds for fallback routing are configured in the MAT application. A threshold is configured for the "Receive fall back threshold" as well as the "Transmit fall back threshold." The available thresholds are: "Excellent, Good, Fair, and Poor."

Basic setup of the ITG system

Figure 19 shows an example of a basic recommended ITG system setup, with separate voice and management networks. This is for illustrative purposes, and is not necessarily the setup you must use.

Figure 19
Basic setup of the ITG system



ITG Trunk DSP profile settings

Codec types

You can configure the following codecs with ITG Trunk 2.0, ITG ISDN Signaling (ISL) Trunk:

- G.711 (A and Mu law)
- G.723 (5.3 kb/s and 6.4 kb/s)
- G.729
- G.729A

You can enable/disable VAD for all of these codecs using the MAT ITG interface.

You can select from three DSP profiles on the ITG Trunk card. Profile 1 is the default setting.

- Profile 1: G.711, G.729A, Fax
- Profile 2: G.711, G.723.1, Fax
- Profile 3: G.711, G.729, Fax

The DSP coding algorithm parameter sets the preferred codec of each ITG card. The recommendation is to use Profile 1, and to set the preferred codec to G.729A with Voice Activity Detection/Silence Suppression with a payload setting of 30 ms. With this codec-payload combination the ITG can deliver a good QoS but loads less than 10 kbit/s per port on the intranet.

It is recommended that all the nodes in the ITG Trunk 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 if the ITG network results in tandem encoding for some of the users. Too much consecutive coding and encoding by G.729 Annex AB, G.723 6.3K, G.723 5.3K, or G.729A codecs can lower the end-to-end quality of service.

To maintain an acceptable QoS on speech, silence suppression can be disabled under some conditions (e.g., in tandem networking conditions when some trunk facilities have excessively low audio levels).

Fall back threshold

There are two parameters, the *receive fall back threshold*, and the *transmit fall back threshold*, which can be set on a per site pair basis.

"Set QoS" on page 108 and "Measure intranet QoS" on page 114 sections describe the process of determining the appropriate QoS level for operating the ITG network. Site pairs can have very different QoS measurements if some traffic flows are local, while other traffic flows are inter-continental. You can consider setting a higher QoS level for the local sites compared to the international sites, keeping costs of international WAN links down.

Normally you must set the fall back threshold in both directions to the same QoS level. In site pairs where one direction of flow is more important, you can set up asymmetric QoS levels.

Payload size

The ITG default payload sizes are as follows:

- 30 ms for G.729 Annex AB, G.729A, G.723.1 5.3K, and G.723.1 6.3K codecs, and 10ms for the G.711A and G.711U codecs.
- 30 bytes for fax

The payload size is adjustable to 10 ms and 20 ms for the G.711A/G.711U and G.729 Annex AB codec series. In a site pair that experience packet losses, selecting a smaller payload size improves voice and fax quality, but at the cost of a higher bandwidth use (see Table 5).

Silence suppression parameters (Voice activity detection)

Silence suppression, also known as Voice Activity Detection (VAD) is enabled by default on a new ITG node. You can enable/disable VAD using the **Enable voice activity detection** checkbox on the **MAT ITG Node Properties -- DSP Profile Codec Options** tab (See Figure 32 on page 202.) To change the current DSP VAD state to match the current VAD configuration, retransmit card properties from MAT.

When silence is detected, the ITG node sends a flag to the destination ITG 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:

- Idle noise level. This is set at a default level of -65 dBm0.
- 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 suited in most office environments. Increasing either of these two parameters lowers the amount of IP traffic generated at the expense of clipping and dropouts.

Jitter buffer parameters (Voice playout delay)

There are three parameters that control the size of the jitter buffer in the destination ITG node.

- Voice playout nominal delay. This can range from twice the payload size to 10 times, subject to a maximum of 320 ms.

- Voice playout maximum delay.
- 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 124, lowering the jitter buffer size decreases the one-way delay of voice packets; however setting the jitter buffer size too small will cause unnecessary packet discard.

If you need to discard to downsize the jitter buffer, you should first check the delay variation statistics. First obtain the one-way delay distributions originating from all source ITG sites using the measurements outlined in "Measure intranet QoS" on page 114 or "Post-installation network measurements" on page 138. 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.

Post-installation network measurements

The design process is continual, even after implementation of the ITG network and commissioning of voice services over the network. Network changes – in actual ITG 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. The design needs to be reviewed 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 to monitor, analyze, and re-design both the Meridian 1 network and the corporate intranet so that both networks continue to conform to internal quality of service standards. When operating voice-over-IP services, the customer's organization needs to incorporate additional monitoring and planing processes. They are:

- Collect, analyze, and trend ITG traffic patterns,

- Monitor and trend *one-way delay* and *packet loss*, and
- Perform changes in the ITG and intranet when planning thresholds are reached.

By instituting these new processes, the ITG network can be managed to ensure that desired QoS objectives are always met.

Set ITG QoS objectives

You need to state the design objective of the ITG network. This sets the standard for evaluating compliance to meeting users' needs. When the ITG network is first installed, the design objective expectations have been set based on the work done in “Measure intranet QoS” on page 114. Initially the QoS objective is to be set so that for each destination pair, the mean+σ of *one-way delay* and *packet loss* is below some threshold value so that calls between those site pairs are in a required QoS level. The graphs of Figures 15 to 17, with the QoS measurements, should help the technician determine what threshold levels are appropriate.

Table 22 describes examples of ITG QoS objectives:

Table 22
ITG QoS objectives

Site Pair	ITG 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, the QoS objective can be reviewed and refined, based on data collected from monitoring of intranet QoS.

Having decided on a set of QoS objectives, the technician then determines the planning threshold. The planning thresholds are then 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, you must install a delay and route monitoring tool, such as `ping` and `traceroute`, on the T - LAN of each ITG site. Each delay monitoring tool will be running continuously, injecting probe packets to each ITG site about every minute. The amount of load generated by this is not considered important. 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 114 for information about implementation of the `ping` hosts and the use of scripting.)

(See "Obtain QoS measurement tools" on page 118 for information about where to obtain other more specialized delay and route monitoring tools.)

At the end of the month, the technician can analyze each site's QoS information. Table 23 provides a sample.

Table 23
QoS monitoring

Site pair	One-way delay Mean+σ (ms)		Packet loss Mean+σ (%)		QoS		
	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
Etc.							

Declines in QoS can be observed through the comparison of QoS between last period and current period. If a route does not meet your QoS objective, you must take immediate action to improve the route's performance.

ITG network inventory and configuration

You must record the current ITG design and log all adds, moves and changes to the ITG network that occur. The following data must be kept:

- ITG site information
  - location
  - dialing plan
  - IP addressing
- Provisioning of ITG nodes - number of cards and ports
- ITG node and card parameters
  - fall back 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 fall back threshold algorithm requires a fixed ITG system delay of 93 ms, which is based on default ITG settings and its delay monitoring probe packets. The fall back mechanism does not adjust when ITG parameters are modified from their default values. Users can perceive a lower quality of service than the QoS levels at the fall back thresholds when:

- 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 ITG 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 will be noticeably higher both in terms of average and variation.

Estimate QoS level

You can use Table 24 to estimate the IP telephony 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 10ms respectively. The techniques used to determine and apply the information in this table are Nortel Networks proprietary.

Table 24
ITG QoS levels (Part 1 of 4)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A/G.711u	G.723.1
0	50-200	excellent	excellent	excellent
0	210-220	excellent	excellent	good
0	230-330	good	excellent	good
0	340-360	good	good	good
0	370-380	good	good	fair
0	390-620	fair	good	fair
0	630-780	fair	fair	fair
0	790	fair	fair	poor
1	50-180	excellent	excellent	good
1	190-200	good	excellent	good
1	210-320	good	good	good
1	330-340	good	good	fair

Note: The QoS levels are equivalent to the following MOS values: (See page 56 for more details)

- excellent 5
- good 4
- fair 3
- poor 2

Table 24
ITG QoS levels (Part 2 of 4)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A/G.711u	G.723.1
1	350-360	fair	good	fair
1	370-630	fair	fair	fair
1	640-690	fair	fair	poor
1	700-780	poor	fair	poor
2	50-270	good	good	good
2	280-300	good	good	fair
2	310-320	good	fair	fair
2	330-510	fair	fair	fair
2	520-580	fair	fair	poor
3	50-250	good	good	good
3	260	good	good	fair
3	270-460	fair	fair	fair
3	470-490	fair	fair	poor
4	50-200	good	good	good
4	210-240	good	good	fair
4	250-390	fair	fair	fair

Note: The QoS levels are equivalent to the following MOS values: (See page 56 for more details)

- excellent 5
- good 4
- fair 3
- poor 2

Table 24
ITG QoS levels (Part 3 of 4)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A/G.711u	G.723.1
4	400-440	fair	fair	poor
5	50-180	good	good	good
5	190-210	good	good	fair
5	220-360	fair	fair	fair
5	370-400	fair	fair	poor
6	50-200	good	good	fair
6	210-330	fair	fair	fair
6	340-380	fair	fair	poor
7	50-140	good	good	fair
7	150-310	fair	fair	fair
7	320-340	fair	fair	poor
8	50-290	fair	fair	fair
8	300-320	fair	fair	poor
9	50-270	fair	fair	fair
9	280-300	fair	fair	poor
10	50-260	fair	fair	fair

Note: The QoS levels are equivalent to the following MOS values: (See page 56 for more details)

- excellent 5
- good 4
- fair 3
- poor 2

Table 24
ITG QoS levels (Part 4 of 4)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A/G.711u	G.723.1
10	270-280	fair	fair	poor
11	50-250	fair	fair	fair
11	260-270	fair	fair	poor
12	50-230	fair	fair	fair
12	240-260	fair	fair	poor
13	50-230	fair	fair	fair
13	240-250	fair	fair	poor
14	50-210	fair	fair	fair
14	220-230	fair	fair	poor
15	50-190	fair	fair	fair
15	200-230	fair	fair	poor
16	50-160	fair	fair	fair
16	170-210	fair	fair	poor

Note: The QoS levels are equivalent to the following MOS values: (See page 56 for more details)

- excellent 5
- good 4
- fair 3
- poor 2

ITG MAT PC management configuration

This section provides guidelines on how to set up MAT to support the Meridian Internet Telephony Gateway (ITG) Trunk 2.0 card. The MAT application name is **ITG ISDN IP Trunks**.

MAT ITG Engineering rules

MAT ITG can manage multiple nodes with multiple ITG cards. The maximum number of ITG cards that can be configured by MAT depend on the following:

1 All MAT ITG data is stored in a single database file. The entire database is read into PC memory when you launch the program. If a large ITG network is to be managed from a single MAT server, then each MAT PC client should have more than the minimum RAM requirements of 32 Mb, and the recommended RAM is 64 Mb or more. If the data is stored on a MAT server, the application launch time will increase as the size of the ITG network grows (this also depends on the network speed).

2 In theory, a single MAT installation can support up to 500 Meridian 1s. However, MAT applications requiring real time, such as Traffic Analysis retrieval of traffic data is limited to a much smaller number of systems.

3 MAT Alarm Notification can receive a maximum of 20 SNMP traps per second based on the recommended PC configuration). In large networks, it is recommended that multiple MAT PCs be used to collect traps from ITG cards, each PC supporting one or more ITG nodes. Alarm notification scripts can be used to forward critical alarms to a central MAT PC or Network Management application.

MAT network setup guidelines

Install MAT in a standalone mode or in a network environment. For ITG Trunk 2.0 card, install MAT in a network environment, so you can manage multiple ITG nodes, provide multi-user access and maintain ITG configuration data consistency.

In the network environment, MAT stores databases on a file server. Do not use the server to access MAT as a client PC. MAT 6.6 with Windows 95 or Windows NT 4.0 clients are supported running on:

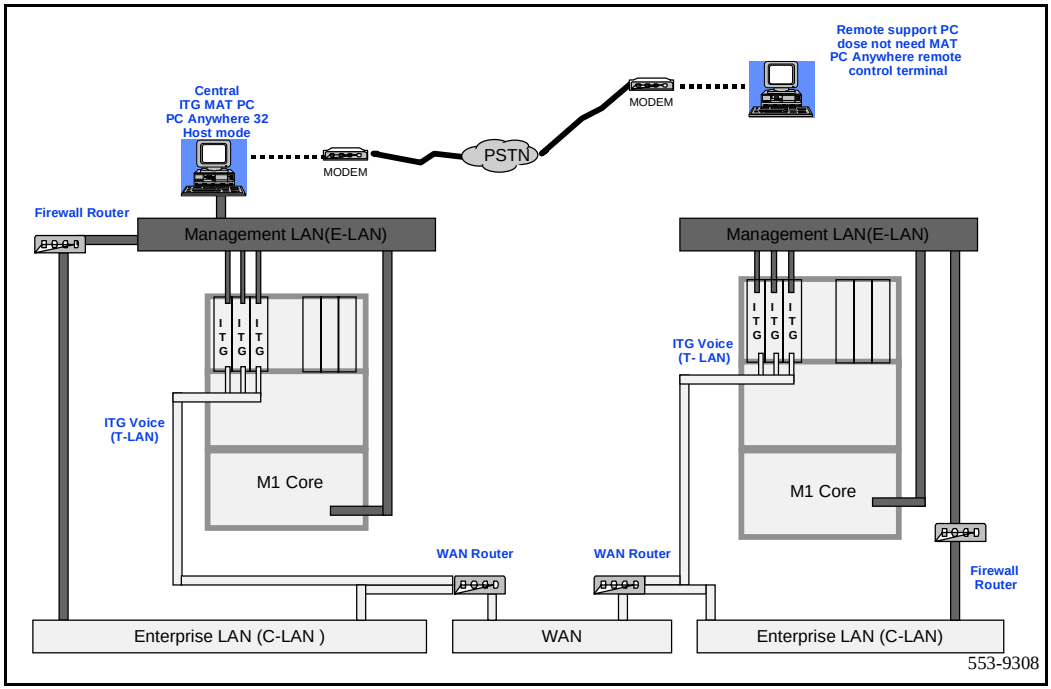
- Novell 3.12 or later server
- Windows NT server
- OTM 1.0 client requires an OTM server

MAT 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 network and a single remote support and administration MAT PC can administer a local node via the ITG Management LAN or a remote node via the WAN. The remote access capabilities are provided via a modem router that has access to any of the ITG Management LANs. The Remote MAT PC connects to the ITG Management over a PPP link and then communicates to the ITG cards the same as does a local MAT PC on the ITG Management LAN. The IP address provided by the modem router (for example, Nortel Networks Netgear RM356 Modem Router) to the remote MAT ITG PC is configured in the modem router and in the SNMP Manager's list of the ITG 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. In this case a local MAT PC on an ITG Management LAN has access to only the ITG cards on the local node. In this case, a private IP address can be used for the MAT PC since management and alarm traffic would never have to travel over any network other than the private ITG Management LAN. A modem can be used to connect the remote MAT PC to the local MAT PC with remote access software such as *PC Anywhere* running in client-server mode between the

Figure 20
Remote access with full access to the customer's LAN/WAN



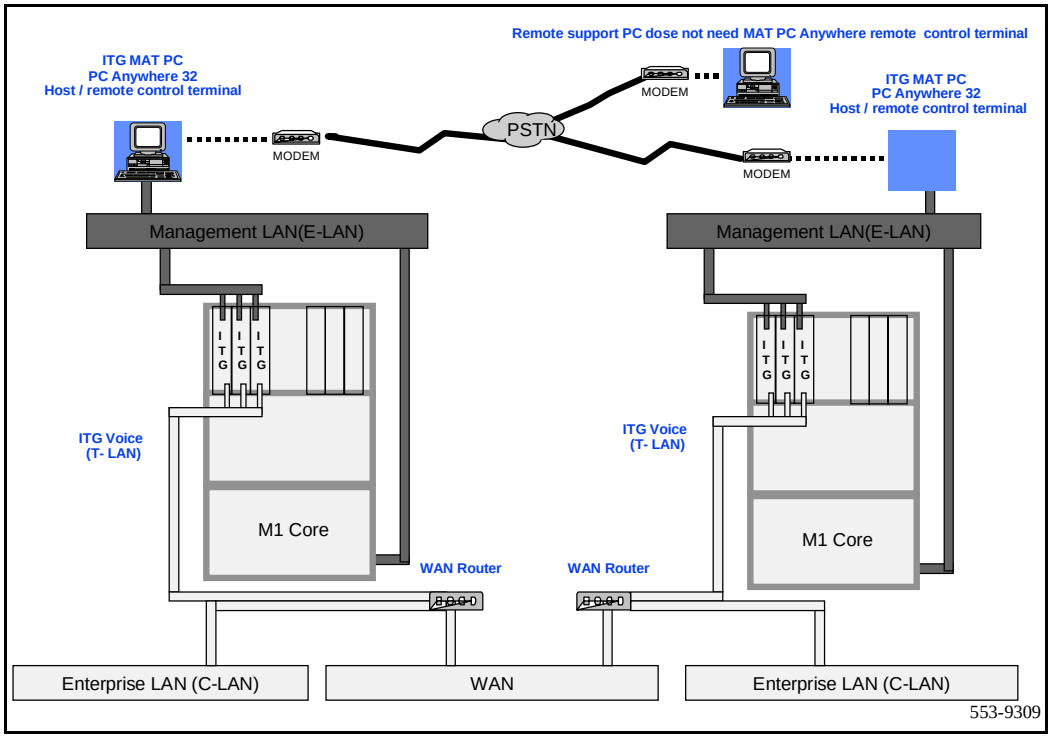
local and remote PCs. The local MAT PC is communicating with the ITG cards for management and alarm information and conveying all information back to the remote MAT PC. There are alternative solutions for remote alarm management available to the customer through third party products. The customer is referred to product bulletins for availability.

MAT PC description

The MAT PC can be attached to a LAN to provide multi-user, multi-site access. The MAT applications and database must reside on a LAN Server with each client accessing the files from the server.

Note: The server used for MAT is used as a file server only and must not be used to access MAT as a client PC.

Figure 21
Remote access with no access to the customer's LAN/WAN



A single network drive location is chosen during the MAT 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 would be recommended. Tape (or other) backup would be highly recommended.

When you install MAT client applications, it is important for the network drive to be mapped the same from each PC if a MAT user is expected to be able to login to the network with their network login ID at any MAT client PC.

A PC security device is required for every PC running MAT 6.6. A security device is not required for the PC server as it is only used to store MAT data and does not actually run any MAT applications.

Each of the MAT client PCs on the customer LAN are allowed connectivity to IP addresses of the Meridian 1;s:

1 MAT client PC in switchroom has access to the File Server on the customer network

2 Block broadcast messages from the customer LAN to the Meridian 1 private LAN.

3 Block access to the Meridian 1 private LAN from non-MAT client PCs for security reasons.

MAT PC hardware and software requirements

The list below provides the recommended minimum PC hardware and software recommended to run MAT 6.6. Other applications launched while you use MAT may require increased RAM:

- A Pentium Processor PC with:
  - — 100 MHz or faster CPU
  - — One GB or larger hard disk drive with 500 MB or more free space (includes Windows 95/NT 4.0 requirements.) Please refer to system datastore column in the hard drive requirements chart that follows:
- 32 MB or RAM (minimum)
- SVGA color monitor and interface card (800x600 resolution for graphics)
- 3-1/2 inch 1.44 MB floppy disk drive
- Windows 95 or Windows NT 4.0 with Microsoft TCP/IP installed
- Ethernet Network Interface Card
- Hayes-compatible modem is optional to connect to remote systems, required for polling configurations (9600 bps or better is recommended)
- PC COM port with 16550 UART

- Parallel printer port. You must configure a printer even through it is not required to be attached to the PC.
- Two-button Windows compatible mouse or positioning device
- CD-ROM drive

Hard drive requirements

For a single MAT PC configuration, refer to Table 25 to select the hard drive space required on the MAT PC. Consider both program and data store requirements.

For MAT client configurations (two or more MAT PCs sharing the same database), the common data is stored on a server PC that does not run MAT. Estimate the size of the required disk space on this server using the Data Store column in Table 25.

Table 25
Hard drive capacity for MAT applications

MAT application	Program store	Data store
Common services (required)	38 MB	Negligible.
ITG	1.5 MB	1.0 MB plus 0.5 MB per 1k ITG cards
Traffic Analysis	5 MB	Meridian 1 dependent: Typically 2.5 to 9 MB per month for each systems traffic data.
ESN	1 MB	Meridian 1 dependent: Allow 1 MB per customer.
Maintenance Windows	1 MB	Negligible.
Alarm Management with Alarm Notification	1.5 MB	Negligible.

Install and configure ITG ISL Trunk node

This section describes how to add a new ITG 2.0 trunk node in MAT, how to install the cards and cables, and how to configure and transmit the node properties.

Before you begin

1. Install MAT 6.6 or later, or install OTM 1.0. Make sure you install the ITG ISDN IP Trunk and Alarm Management applications.
2. Upgrade Meridian 1 X11 software to Release 25A or later. ITG requires packages 145 (ISDN) and 147 (ISL). Install additional software packages, such as Package 148 NTWK, as required for advanced ISDN features.
3. Check that required LAN and WAN networking equipment and cables are installed. For networking equipment requirements, turn to “ITG Engineering Guidelines” on page 71. The ITG Trunk card requires shielded cables.
4. ITG Trunk card (NT0961AA) DCHIP PC Card (NTWE07) and cable assemblies required for your site.
5. For Meridian 1 Large Systems, ITG ISL (NT6D80). For Meridian 1 Small Systems, ITG ISL Trunk 2.0 requires at least one available port on an SDI/DCH card (minimum vintage NTAK02BB). Be sure D-channel cards have required cables.
6. Check that the customer site has a Nortel Networks Netgear RM356 Modem Router (or equivalent) on the E-LAN. The modem router provides remote support access to ITG Trunk and other IP-enabled Nortel Networks products on the Meridian 1 site. See Appendix D: “Configure a Netgear RM356 modem router for remote access” on page 359 for more information on routers.

Installation Procedure Summary

Table 26 lists the procedures to install and configure an ITG Trunk node. You must complete all installation and configuration tasks before you transmit the configuration data to the ITG Trunk cards.

Table 26
Installation procedures (Part 1 of 2)

Step	Procedure	Page
1	**Create the ITG Trunk Installation Summary Sheet**	**page 156**
2	**Install and cable ITG trunk cards**	**page 158**
	Card installation procedure	page 158
3	**Configure ITG Trunk data on the Meridian 1**	**page 174**
	Configure the ISL D-channel on the Meridian 1 for the DCHIP card	page 174
	Configure ISDN feature in customer data block	page 178
	Configure ITG ISL trunk cards and units	page 182
	Configure dialing plans within the corporate network	page 185
	Disable the ITG Trunk cards	page 191
4	**Configure ITG Trunk data on MAT**	**page 191**
	Add an ITG Trunk node on MAT manually	page 192
	Add a node and configure general node properties	page 192
	Single vs. separate subnets for T-LAN and E-LAN	page 193
	Configure card properties	page 195
	Configure DSP profiles for the ITG Trunk node	page 199
	Configure SNMP Traps/Routing and IPs tab	page 204
	Configure Accounting server	page 205
	Set Security for MAT SNMP access	page 207
	Exit node property configuration session	page 208
	Create the ITG Trunk node dialing plan using MAT	page 208
	Retrieve the ITG Trunk node dialing plan using MAT	page 213

Table 26
Installation procedures (Part 2 of 2)

Step	Procedure	Page
5	**Transmit ITG trunk card configuration data from MAT to the ITG trunk cards**	**page 215**
	Setting the Leader 0 IP address	page 216
	Transmit the node properties, card properties and dialing plan to Leader 0	page 218
	Verify installation and configuration	page 219
	Transmit Card Properties and Dialing Plan to Leader 1 and Follower cards	page 220
6	**Set date and time for the ITG ISL Trunk node**	**page 222**
7	**Change the default ITG shell password to maintain access security**	**page 222**
8	**Check card software**	**page 225**
	Transmit new software to ITG Trunk cards	page 227
	Upgrade the DCHIP PC Card	page 229
9	**Configure MAT Alarm Management to receive SNMP traps from ITG ISL Trunk cards**	**page 231**
10	**Make test calls to the remote ITG nodes**	**page 234**

Create the ITG Trunk Installation Summary Sheet

Compile all necessary data before beginning the configuration process. For example, prepare the following information ahead of time:

- The TN, Management MAC address, and Card Density should be recorded during the ITG Trunk 2.0 hardware installation.
- D-Channel number and CHID should be recorded during the Meridian 1 configuration.
- All E-LAN and T-LAN IP addresses must be obtained from the System Administrator before beginning MAT configuration.

Create an ITG Installation Summary Sheet. This form contains important information about each card, including the fields listed in Table 27, “ITG Trunk Installation Summary Sheet,” on page 157.

Table 27
ITG Trunk Installation Summary Sheet

Site_____ System_____ Customer_____ Node Number_____
T - LAN Node IP address_____
T - LAN gateway (router)_____T - LAN subnet mask_____
E - LAN gateway (router)_____E - LAN subnet mask_____

TN	Mgmt. MAC (E-LAN)	Mgmt. IP (E-LAN)	Voice IP (T-LAN)	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				
				Follower				

Install and cable ITG trunk cards

Card installation procedure

When unpacking the hardware, use ESD precautions while handling the cards. As each card is placed in the Meridian 1 system, record the TN, management MAC address and the card density on the installation summary sheet. The management MAC address is labeled on the ITG Trunk card faceplate as the motherboard Ethernet address.

Each ITG card requires two slots in a Meridian 1 IPE shelf. Only the left slot of the card requires connection to the Meridian 1 IPE backplane and I/O panel.

At least one DCHIP card must be installed in an ITG ISL Trunk node. You must install the D-Channel (DCH) PC Card and the associated NTCW84EA DCHIP PC Card Pigtail cable on to the DCHIP card.

You can install a maximum of eight ITG cards in an IPE shelf. The ITG 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. You cannot plug in the left slot of an ITG card 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 ITG cards, install each 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 ITG card can be inserted in an odd-numbered slot.

Note 1: The ITG 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. You can insert the left slot of the ITG Trunk card in NT8D37AA slots 0, 4, 8 or 12 only. NT8D37BA or later IPE modules have no such restriction.

Note 2: When multiple ITG cards are installed, distribute them between available IPE shelves. This prevents total loss of IP trunking, in the case of localized shelf failure.

CAUTION

Wear an electrostatic discharge strap when handling ITG cards. As an additional safety measure, handle all cards by the edges and, when possible, with the loosened packaging material still around the component.

CAUTION

Never install an ITG card in an IPE shelf that has been wired for a Central Office Trunk (COT) card. Before you insert 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 ITG card, can damage the card.

CAUTION

Do not overtighten screws. They can break.

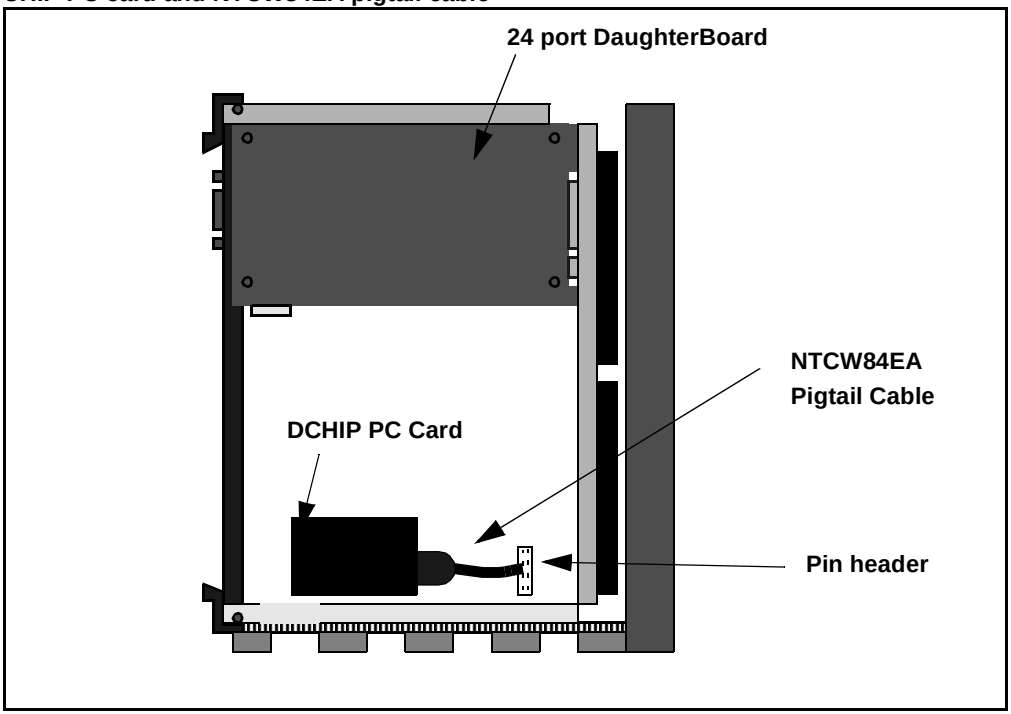
1 Identify the IPE card slots selected for the ITG card(s). Use the recorded information from the ITG Trunk Installation Summary Sheet (Figure 27 on page 157).

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 ITG Trunk card that has been selected to provide the DCHIP function. (See Figure 22 on page 160.)

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 22) 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 22
DCHIP PC card and NTCW84EA pigtail cable



5 Pull the top and bottom locking devices away from the ITG faceplate. Insert the ITG card into the card slots and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When ITG 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 2: Observe the ITG Faceplate Maintenance display to see start - up self-test results and status messages. A display of the type “F:xx” indicates a failure. Some failures indicate that you must replace the card. “F:10” temporarily appears on the display, which indicates a Security Device test failure. Since ITG 2.0 does not use Security Devices, you can ignore this error.

Refer to “ITG Trunk 2.0 faceplate maintenance display codes” on page 329 for a complete listing of the codes.

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 T-LAN 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 T-LAN Tip and Ring pairs.

For Option 11C systems, the standard I/O filter connector already supports 100BaseTX.

CAUTION

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 Filter Connector. The NT8D81BA is compatible with 10BaseT T-LAN, but if you require a 100BaseT T-LAN, you need to 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 T-LAN 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.

1 Before any of the following installation steps, 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 First remove the NT8D81AA Backplane to I/O Panel ribbon cable assembly which will be connected to the backplane side of the existing block by releasing the latching pins on the filter block and pulling the NT8D81AA cable away.

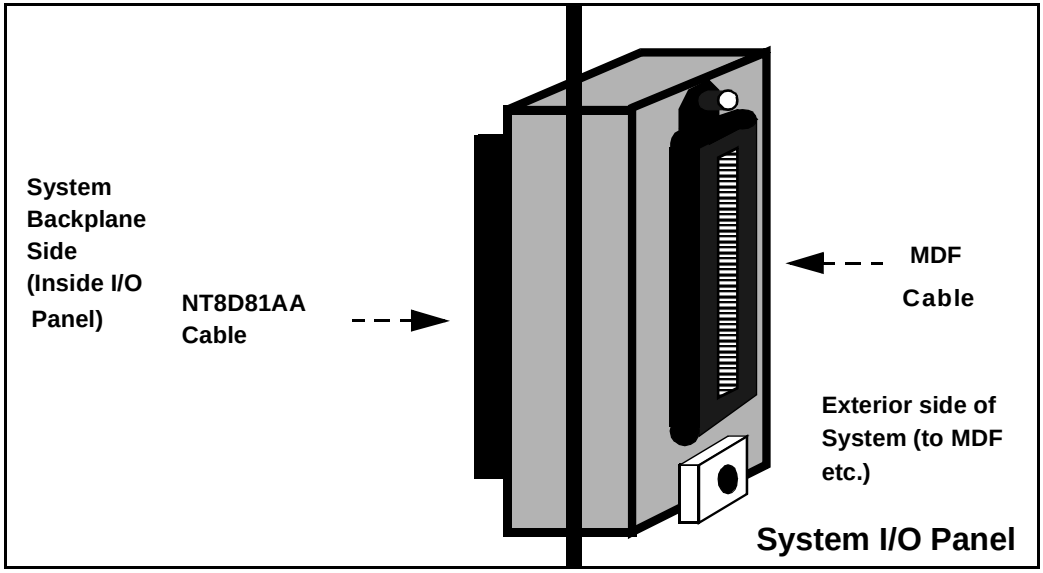
3 Next unscrew the existing filter adapter from the I/O panel. There is one screw on the lower front of the adapter and one screw on the upper back of the adapter. Remove the adapter.

4 Re-position the new NTCW84JA filter adapter in the now vacant I/O panel opening. (See Figure 22 on page 160.)

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.

Figure 23
NTCW84JA 50 pin I/O Panel Filter Connector Block



Note: Even though the ITG Trunk 2.0 card is a two-slot card, only the leftmost slot is counted for the card slot number. Example: for an ITG Trunk 2.0 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 "Cable description and NT8D81BA cable replacement" on page 333.

Install NTMF94EA and NTCW84KA cables

The ITG Trunk 2.0 card supports a one-cable solution for access to the T-LAN, E-LAN and serial E-LAN Ethernet Ports. The E-LAN supports 10BaseT operation and the T-LAN supports 10/100BaseT operation. If you use for 100BaseT operation on the T-LAN interface, you must 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 E-LAN and T-LAN interface functions include:

- the NTMF94EA E-LAN, T-LAN, and RS232 Port cable (for non-DCHIP cards)
- the NTCW84KA E-LAN, T-LAN, RS232 and DCH Ports cable (for DCHIP cards)

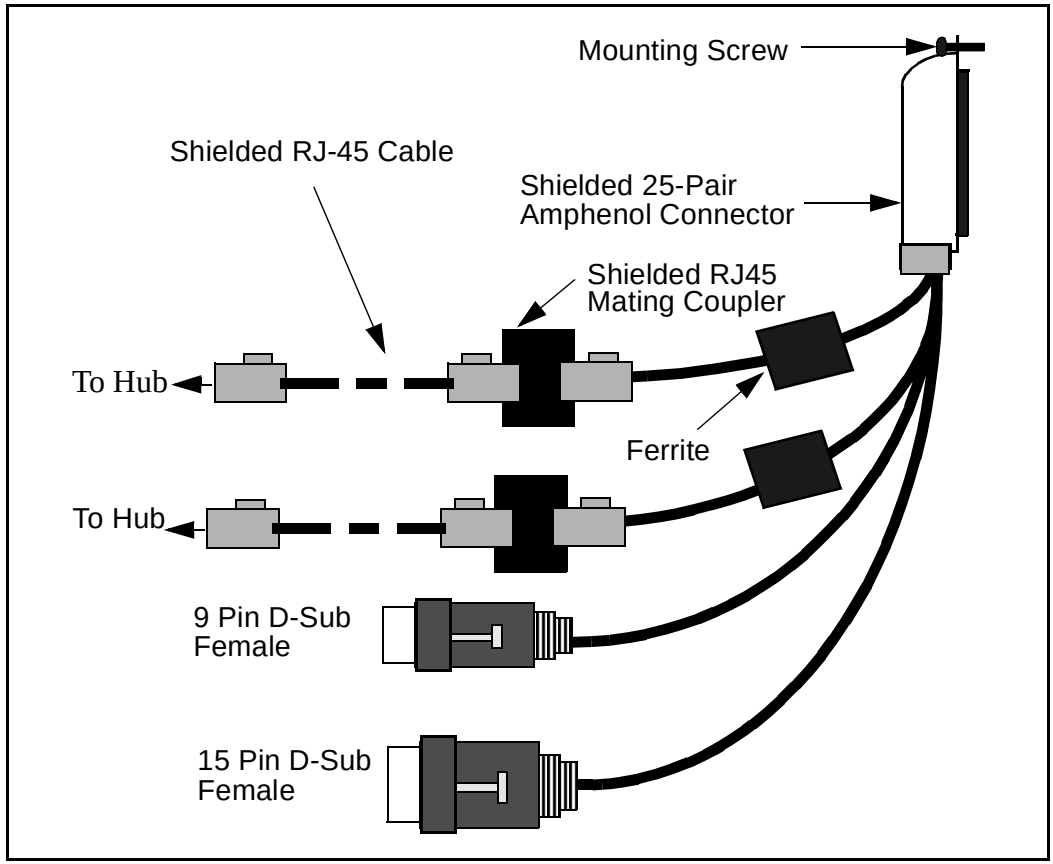
Install the NTCW84KA cable (for DCHIP cards)

1 Connect the NTCW84KA cable see to the I/O panel connector (see Figure 24).

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 Meridian 1 frame ground for EMC compliance.

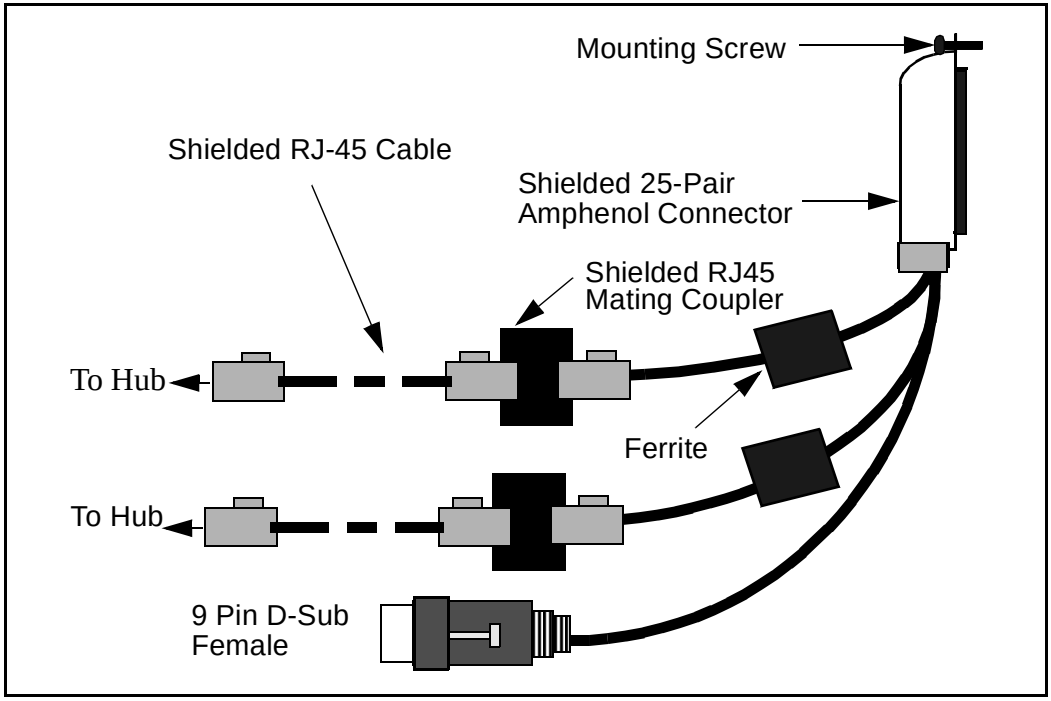
Figure 24
NTCW84KA E-LAN, T-LAN, DCH and serial cable



Install the NTMF94EA cable (for non-DCHIP cards)

1. Connect the NTMF94EA cable (see Figure 25) 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 Meridian 1 frame ground for EMC compliance.

Figure 25
NTMF943A E-LAN, T-LAN and serial port cable



Install shielded voice interface (T-LAN) cable

You must use Shielded Category 5 cable to connect to the E-LAN, T-LAN ports on the NTCW84KA cable. To conduct a ground loop test, turn to page 349 and follow the test procedure.

For DCHIP cards

Connect a shielded Category 5 LAN cable from the T-LAN hub to the RJ45 coupler on the NTCW84KA T-LAN connector.

For non-DCHIP cards

Connect a shielded Category 5 LAN cable from the T-LAN hub to the RJ45 coupler on the NTMF94EA T-LAN connector.

Note: When connecting the ITG card to the T-LAN, the link status LED on the ITG card faceplate associated with the voice interface will light green when the connection is made, and the link status LED on the hub port will also light green when connected to the ITG card.

Install shielded management interface (E-LAN) cable

For DCHIP cards

Connect a shielded Category 5 LAN cable from the E-LAN hub to the RJ45 coupler on the NTCW84KA E-LAN connector.

For non-DCHIP cards

Connect a shielded Category 5 LAN cable from the E-LAN hub to the RJ45 coupler on the NTMF94EA E-LAN connector.

Note: There are no E-LAN network status LEDs for the management interface on the ITG Trunk card. When connected to the ITG card management interface, the port status LED indicator on the E-LAN hub lights green to indicate a good connection.

D-channel cabling for the NT0961AA 24-Port ITG Trunk card

In this section, you check, and reset if necessary, MSDL switch settings, install a filter (if required for your installation) and install the cable that connects the MSDL or SDI/DCH card to the ITG Trunk 2.0 card that provides the DCH interface.

Large systems required cables and filters

- the NTCW84KA E-LAN, T-LAN, RS232 and DCH Ports cable
- the NTND26AA MSDL DCH cable

Set NT6D80 MSDL switches

1 Set the switches in the NT6D80 MSDL card as shown. See Table 28 for more information.

Table 28
NT6D80 MSDL settings for ITG ISL Trunk DCHIP

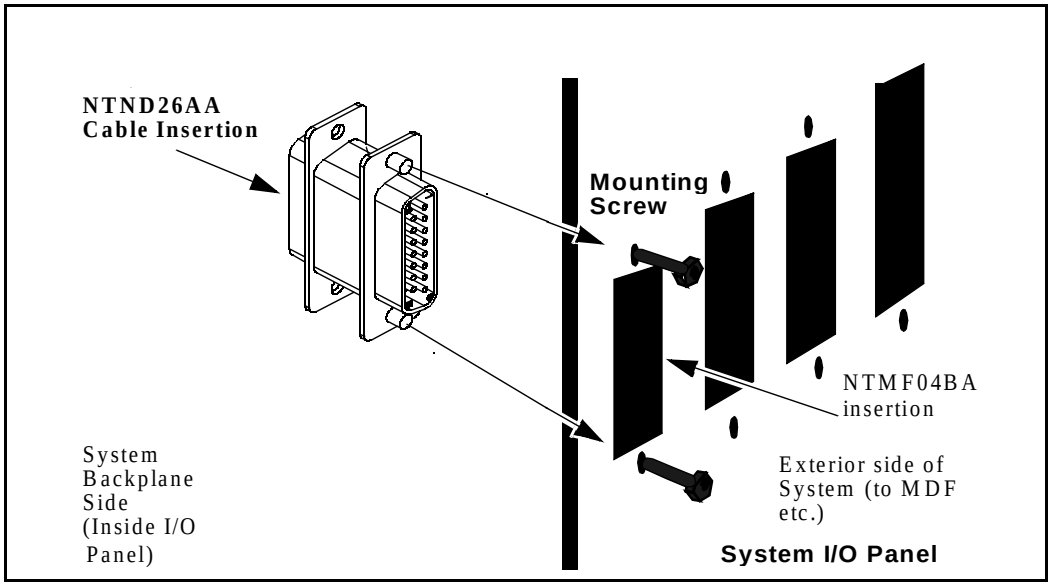
	Port 0—SW4	**Port 0—SW8**
RS-422-A DTE	all off	all on
	Port 1—SW3	**Port 1—SW7**
RS-422-A DTE	all off	all on
	Port 2—SW2	**Port 2—SW6**
RS-422-A DTE	all off	all on
	Port 3—SW1	**Port 3—SW5**
RS-422-A DTE	all off	all on

Note: The device number for the MSDL card is configured in LD17 at the prompt DNUM. You must also set the device number, using switches S9 and S10, on the MSDL card. S9 designates ones and S10 designates tens. To set 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)

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.

Figure 26
15-pin filter connector installation

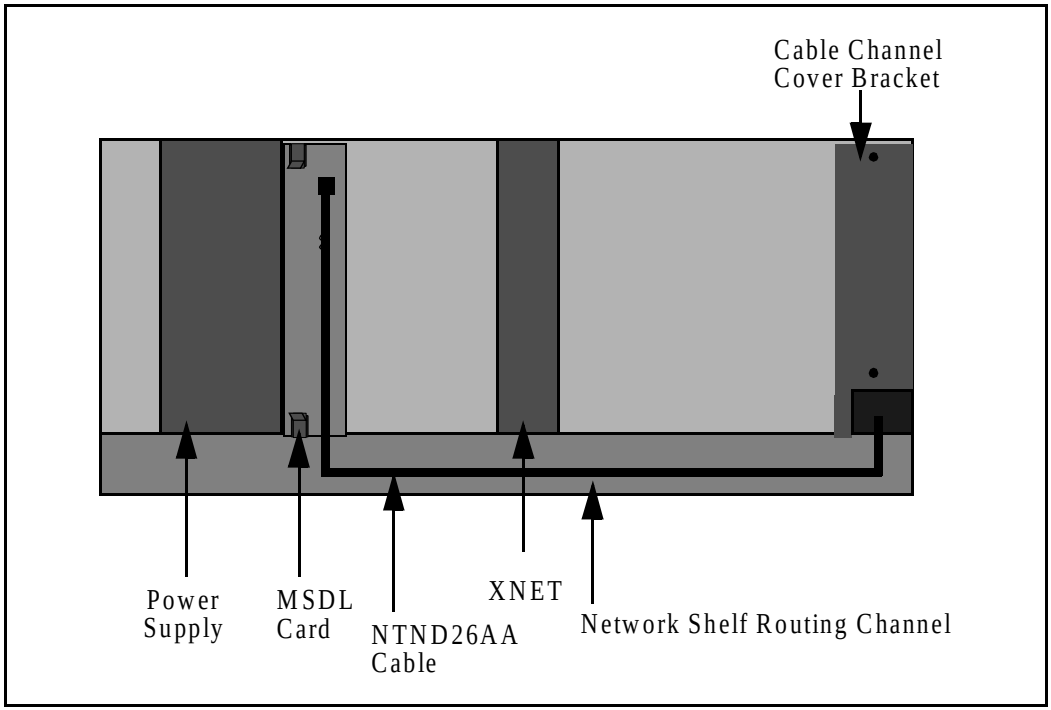


3 Obtain the correct length of the NTND26 DCHI Interface Cable Assembly to reach from the D-Channel port connector on the faceplate of the MSDL card to the outward side of the 15-pin filter connector installed in the I/O panel of the IPE Module that contains the DCHIP card. (See Figure 27)

The NTND26 DCHI Interface Cable Assembly is available in the following lengths:

- NTND26AA 6 ft.
- NTND26AB 18 ft.
- NTND26AC 35 ft.
- NTND26AD 50 ft.

Figure 27
NTND26 cable routing diagram



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.

5 Connect the DCH (P5) connector of the NTCW84KA to the outward side of the 15-pin I/O panel filter connector.

Install filter and NTND26 cable (for MSDL and DCHIP cards in different Large System equipment rows)

6 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.

7 Install the 15-pin I/O panel filter connector on the inward side of the bracket.

8 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.

9 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.

10 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.

Meridian 1 Small System cable installation (Option 11C and Option 11C Mini)

1 Set the switches and jumper plugs in the NTAK02 SDI/DCH card as shown. See Tables 29 and 30.

Table 29
NTAK02 SDI/DCH switch settings for ITG ISL Trunk DCHIP

Port 1	SW 1-1	SW 1-2
DCH	OFF	OFF
Port 3	**SW 1-3**	**SW 1-4**
DCH	OFF	OFF

Table 30
NTAK02 SDI/DCH jumper settings for ITG ISL Trunk 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 fpr Port 1 or Port 3.

Install the serial cable

1 To make a temporary connection to the ITG Trunk maintenance port from a local RS232 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 ITG 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 via 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.

Configure ITG Trunk data on the Meridian 1

You must first configure D-channels, route data blocks, and trunks through the Meridian 1 system TTY. Then, you configure the ESN data blocks to implement the network dialing plan and translations. Record the D-Channel, CHIDs, and TNs for the ITG ISL Trunks on the installation summary sheet.

Configure the ISL D-channel on the Meridian 1 for the DCHIP card

Table 31
LD 17 - Configure the ISL D-channel for the ITG 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
PORT	x	Port number for MSDL card, where: x = 0-3
DES	ITG ISL TRUNK	16 character designator is “ITG ISL TRUNK” Specific description if more than one ITG Trunk route exists.
...		
USR	ISLD	User. Dedicated Mode ISDN Signaling Link.

Table 31
LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Large Systems) (Part 2 of 3)

Prompt	Response	Description
IFC	SL1 ESGF ISGF	Interface type for D-channel: Meridian Customer Defined Network (MCDN) ESIG interface with GF platform (QSIG) 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 MAT'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.
BPS	(64000)	64000 is default, and is required for the ITG ISL Trunk DCHIP.
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)	Meridian 1 MSDL acts as User side of ISL. ITG Trunk DCHIP card acts as the Network side of ISL.

Table 31
LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Large 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.
...		

Table 32
LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Small Systems) (Part 1 of 2)

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
CTYP	DCHI	Card Type. SDI/DCH card (configure the option switches and jumper straps on the SDI/DCH for RS422 DTE mode operation.
CDNO	1-9	Card number.
PORT	1 or 3	Port Number must be 1 or 3.
USR	ISLD	User. Dedicated Mode ISDN Signaling Link.
IFC	SL1	Interface type for D-channel: Meridian Customer Defined Network (MCDN) ***Note:*** The IFC entry must match the protocol entered in MAT's ITG Node Properties, Card Configuration, Protocol pull-down menu.

Table 32
LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Small Systems) (Part 2 of 2)

Prompt	Response	Description
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 SDI/DCH card acts as User side of ISL. ITG Trunk 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.
RCAP	ND2	Network Name Display type signalling. All nodes must use same RCAP.
...		

Configure ISDN feature in customer data block

Table 33
LD 15 - Configure ISDN feature in customer data block

Prompt	Response	Description
REQ	CHG	Change customer data block.
TYPE	NET_DATA	Gate-opener for networking features.
CUST	xx	Customer number associated with this customer data block.
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. You enable or disable INAC per trunk route in LD16 in the IDSN section of the route data block.
ISDN	YES (NO)	You must enter YES to configure ITG ISL routes.
- PNI	(0) - 32700	Private Network Identifier. You must configure the PNI to 1 or other non-zero value to support Meridian Customer Defined Network (MCDN) features that use non-call-associated signaling. For example, Network Ring Again (NRAG) Network Message Services (NMS), Network ACD (NACD). Each feature needs ISDN signaling to be sent across the Meridian 1 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 node.
...	...	...

Configure ITG ISL TIE trunk routes

Note: You must configure Trunk routes as TIE routes..

Table 34
LD 16 - Configure the ITG ISL TIE Trunk route data block (Part 1 of 4)

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 associated with this route, as defined in LD 15.
ROUTE	xxx	Route Number, where: x = 0-511
DES	ITG ISL TRUNK	16-character designator is “ITG ISL TRUNK” Specific description if more than one ITG Trunk route exists.
...		
TKTP	TIE	Trunk Type. The trunk type for ITG ISL 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 ITG Trunk 2.0 fallback to circuit-switched trunks does not depend on SAT=YES.
...		
DTRK	(NO)	Digital Trunk Route. ITG ISL Trunks are analog only. They do not support circuit-switched data from MCA or ISDN BRI terminal adaptors.
ISDN	YES	Integrated Services Digital Network.

Table 34
LD 16 - Configure the ITG ISL TIE Trunk route data block (Part 2 of 4)

Prompt	Response	Description
MODE	ISLD	Mode of Operation. 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.
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. You must configure the PNI to 1 or other non-zero value to support Meridian Customer Defined Network (MCDN) features that use non-call-associated signaling. For example, Network Ring Again (NRAG) Network Message Services (NMS), Network ACD (NACD). Each feature needs ISDN signaling to be sent across the Meridian 1 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 node.
NCNA	(YES) NO	Network calling name allowed
NCRD	(NO) YES	Network Call Redirection allowed

Table 34
LD 16 - Configure the ITG ISL TIE Trunk route data block (Part 3 of 4)

Prompt	Response	Description
CTYP		Call type for outgoing call dialed with the route access code (ACOD). Set to appropriate call type for ITG Trunk node numbering plan in order to make test calls using ACOD.
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, etc. ***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, e.g. 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 LD15 to configure them at the AC2 prompt at the customer data block.
...		
ICOG	 IAO	Incoming and/or Outgoing trunk. Incoming and Outgoing.
SRCH	LIN	Linear search method. See Note 1.
SIGO	(STD) ESN5	Standard signaling arrangement ESN 5 signaling ***Note:*** Unless you are using ESN5, SIGO (outgoing signaling protocol) must be set to STD. ***Note:*** If SIGO equals ESN5: Select SL1ESN5 from the pull-down list in the Protocol field in the MAT Node Properties configuration tab. Select SL1ESN5 from the pull-down list in the Remote Capabilities field in the MAT Node Dialing plan General tab for each destination node that uses ESN5.
CNTL	YES	

Table 34
LD 16 - Configure the ITG ISL TIE Trunk route data block (Part 4 of 4)

Prompt	Response	Description
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 ITG ISL trunk cards and units

Record the first CHID for each ITG ISL Trunk card on the installation summary sheet.

Table 35
LD 14 - Configure ITG ISL 8- or 24-port trunk cards and units (Part 1 of 3)

Prompt	Response	Description
REQ	NEW XX	Add new data, where: xx = 1-8 for NTCW80 8-port ITG Trunk card xx = 1-24 for NT0961AA 24-port ITG Trunk card When using REQ = NEW XX, configure only one ITG Trunk card at a time. When using REQ = NEW XX, CHID is incremented for each of the new units created. You may need to configure partial ITG Trunk cards due to WAN traffic capacity limitations, or Leader and DCHIP card real-time capacity for very large nodes and networks.
TYPE	TIE	Trunk Type. TIE is the only supported trunk type for ITG ISL Trunks.

Table 35
LD 14 - Configure ITG ISL 8- or 24-port trunk cards and units (Part 2 of 3)

Prompt	Response	Description
TN	l s c u c u	Terminal Number for large systems, where: l = loop, s = shelf, c = card, u = unit. Terminal Number for Small Systems, where: c = card, u = unit. Always perform the NEW XX for unit 0 on the ITG ISL Trunk card.
DES		16 character descriptive designator for the ITG card. *See Note 1.*
	hhhh:hh:hh:hh:hh	For unit 0. the ITG card management MAC address.
	xxx.xxx.xxx.xxx	For units 1-23 the ITG card management IP address.
XTRK	ITG2	Extended Trunk Type: ITG Trunk card (2-slot assembly).
MAXU	XX	Maximum number of ports on this ITG card, where xx = 24 for the NT0961AA 24-port ITG Trunk card, xx= 8 for the NTCW80 8-port ITG Trunk card.
...		
CUST	xx	Customer Number, as defined in LD 15.
RTMB	0-127 1-254	Route number and Member number. Assign route member numbers to cards in the same order as the default order in the MAT ITG ISDN IP Trunks window. The trunk route member number matches the standard First CHID for the trunk unit 0 in order to facilitate administration and maintenance.

Table 35
LD 14 - Configure ITG ISL 8- or 24-port trunk cards and units (Part 3 of 3)

Prompt	Response	Description
CHID	xxx	First Channel ID for unit 0 on this ITG card, where: xxx = 1-259 for the NT0961AA 24-port ITG Trunk card 1-375 for the NTCW80 8-port ITG Trunk card Standard First CHID Configuration (24 and 8 Port): Leader 0 -- 1 Leader 1 -- 25 Follower -- 49 Follower -- 73 Follower -- 97 Follower -- 121 ... The same First CHID must be entered in MAT ITG ISDN IP Trunk Node Properties, Card Configuration, and “First CHID” field for this card. The standard First CHID matches the trunk route member number for the trunk unit 0 in order to facilitate administration and maintenance.
...		
STRI	 WNK	Start Arrangement Incoming. Wink Start is preferred for ITG Trunk.
STRO	 WNK	Start Arrangement Outgoing. Wink Start is preferred for ITG Trunk.
SUPN	YES	Answer supervision is required.
...		
CLS	 DIP	Class of Service. Dial Pulse is required for ITG ISL Trunk to avoid busying multiple Digitone receivers when ITG Trunk card faults occur.
...		

Note 1: Use the "NEW XX" command to assign DES equal to the ITG card management interface IP address. For example: 10.1.1.1. For unit 0, use CHG command to assign DES equal to the ITG card management interface MAC address, for example: is the management interface MAC address (hhhh:hh:hh:hh:hh). For example: 0060:38:01:06:C6. To find the management MAC address, see the ITG Trunk installation summary sheet. The management MAC address is labeled on the ITG 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 Overlays 86, 87, and 90 as required.

Configure the Meridian 1 ESN by creating or modifying data blocks in overlays 86, 87, and 90, as required. The Meridian 1 and MAT ITG Trunk dialing plan information must correspond.

Make the ITG the first-choice, least-cost entry in the route list block

When adding ITG tie trunks to an existing ESN, a common practice will be to create a new RLB for ESN translations that are intended to be routed by the ITG network. Insert the new ITG route ahead of the existing alternate routes for circuit-switched facilities, which are therefore shifted to the next higher entry number. Remember to increment the ISET (initial set) if Call-Back Queueing or Expensive Route Warning tone are being used.

Turn on Step Back on Congestion (SBOC) for the ITG Trunk route

For the ITG Trunk route entry in the route list block (RLB), enter RRA at the SBOC prompt to enable Fallback to alternate circuit-switched trunk route due to network QoS falling below the defined threshold for the ITG Trunk node, or when there are no ports available at the destination ITG Trunk node.

Turn off ITG route during peak traffic periods on the IP data network

Based on site data, if fall back routing occurs frequently and consistently for a data network during specific busy hours (e.g., 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 ITG 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 ITG trunk route.

ESN5 network signaling

ITG Trunk 2.0 supports ESN5 Network Signaling protocol only, in addition to standard (i.e., non-network) signaling. ITG 2.0 supports a mixed network consisting of ESN5 and standard network signaling nodes.

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 SL1 (MCDN) signaling, and do not support ESN5. You must configure an ESN5 prefix for the non-ESN5 IP telephony gateways by using the "esn5PrefixSet" command from the ITG shell CLI.

For ITG Trunk 2.0 nodes that are configured in the Node Properties to use SL1ESN5 Protocol, the ESN5 prefix configured on the ITG Trunk card is inserted in front of the called number on incoming calls from IP Telephony gateways using the H.323 V2 protocol.

For ITG Trunk 2.0 nodes that are configured in the Node Properties to use the SL1 protocol (i.e., they do not support ESN5 to their host Meridian 1), the ESN5 prefix configured on the ITG Trunk card is inserted in front of the called number on outgoing calls to ITG Trunk 2.0 nodes that are configured to use ESN5 with their host Meridian 1.

Special dial 0 ESN translations

Special dial 0 ESN translations are not supported on ITG ISL Trunk because they are not leftwise-unique.

Use ITG route as first choice for Group 3 fax

The ITG gateway supports Group 3 fax modems by means of T.38 protocol.

Use the traditional PSTN for general modem traffic

General modem traffic (e.g., V.36, V.90) cannot be supported on ITG, therefore the Meridian 1 routing controls must be configured to route modem traffic over circuit-switched trunks instead of over ITG.

Use the ESN TGAR, NCOS, and facility restriction levels to keep general modem traffic off of the ITG route. Use caution before setting TGAR=YES in the ESN block in LD86 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 ITG ISL Trunks to an existing Meridian 1 system, changes to ESN translation should be made last, after the ITG dialing plan and the entire ITG network is tested with calls dialed using the Route Access Code. In LD16, for prompt CTYP, set to appropriate call type for ITG Trunk node numbering plan in order to make test calls using ACOD. After the correct operation of the entire ITG network has been verified, ESN translations that are intended to be routed via ITG tie trunks will then be changed so as to use the new RLI.

Table 36
LD 86 - Configure Electronic Switched Network (ESN) (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number associated with this function, as defined in LD 15.
FEAT	ESN	Electronic Switched Network data block.
...		
CDP	YES	Coordinary Dialing Plan

Table 36
LD 86 - Configure Electronic Switched Network (ESN) (Part 2 of 2)

Prompt	Response	Description
...		
AC1	xx	One-or-two digit NARS/BARS Access Code 1.
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 ITG Trunk 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.
...		

Table 37
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 associated with this function, 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	0-511	Route number that references an ITG trunk route.

Table 37
LD 86 - Configure route list block with Step Back on Congestion on ISDN (Part 2 of 2)

Prompt	Response	Description
TOD		Time of Day Schedule If required, turn off ITG route during peak traffic periods on the IP data network
FRL		Facility Restriction Level Set FRL appropriately to control access to the ITG ISL Trunk route.
DMI	0	Do not use a Digit Manipulation table in the RLB entry for the ITG ISL Trunk route. For ESN translations that are not used for non-call-associated signalling, digit manipulation can be defined on the ITG ISL Trunk node dialing plan in the Digits dialed tab.
SBOC	RRA	Step Back on Congestion. Re-route all. Enter RRA at the SBOC prompt to enable Fallback to alternate circuit-switched trunk route
...		

Table 38
LD 87 - Configure the Coordinated Dialing Plan (CDP)

Prompt	Response	Description
REQ	NEW	Add new data.
FEAT	CDP	Coordinated Dialing Plan.
CUST	xx	Customer number.
TYPE	DSC TSC	Distant Steering Code. Trunk Steering Code.
...		
RLB	xx	Route List Entry created in Overlay 86.
...		

Table 39
LD 90 - Configure dialing plan

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number associated with this function, as defined in LD 15.
FEAT		Feature.
	NET	Network translation tables.
TRAN		Translator.
	AC1	Access Code 1 (NARS/BARS).
	AC2	Access Code 2 (NARS).
TSC		Type of data block.
	NPA	Numbering Plan Area Code.
	NXX	Central Office Translation.
	LOC	ESN Location Code Translation.
	SPN	Special Code Translation.
...		
RLI	xxx	Route List Index created in LD 86.

Disable the ITG Trunk cards

In order to transmit the card properties from MAT to the ITG Trunk cards, the ITG Trunks must be in the disabled state.

To disable an ITG trunk card, use the following command in LD32 or in MAT Maintenance Windows: DISI l s c u.

Wait for NPR0011 to be output. Requested pack is no longer busy and has been disabled. This indicates that the DISI command has been completed.

The status of the ITG trunk card in MAT is updated to disabled.

The cards must be enabled later after the card properties and optionally, the new card software, has been transmitted from MAT to the ITG Trunk cards.

Configure ITG Trunk data on MAT

Before you can use this procedure, you must get all the IP addresses for the new ITG Trunk node from your network administrator and add them to your installation summary sheet. Use the installation summary sheet to facilitate data entry into MAT. You will also need the node IP addresses of any existing ITG Trunk nodes in the network.

> ***Note:*** Refer the network administrator to the *Engineering Guidelines* section for information on ITG Trunk IP address requirements.

An ITG node is a collection of ITG cards in an Meridian 1 system for a selected customer.

Each node in the ITG network has a property sheet that configures the options that apply to the node's cards.

MAT stores Node Properties data. This data generates the bootptab file. You transmit the data 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 ITG Active Leader card, it is renamed "bootp.1".

Add an ITG Trunk node on MAT manually

This section uses the MAT 6.6 (or later) ITG ISDN IP Trunk application to manually add and configure an ITG Trunk node, and add ITG Trunk cards to the node. A network of multiple ITG Trunk nodes can be configured and managed from the same MAT PC. Every ITG Trunk node must first be added manually on the MAT PC, and the MAT ITG Trunk configuration data must be transmitted to the ITG Trunk node during installation.

After adding a new ITG Trunk node on the MAT PC, the dialing plans for all existing ITG Trunk nodes must be manually updated to include the destination node dial plan digits entries for the new ITG Trunk node.

There are several tabs across the top of the ITG Node Properties window. The following sections describe the windows that appear when you click on each of these tabs.

Add a node and configure general node properties

Perform the following steps to add a node:

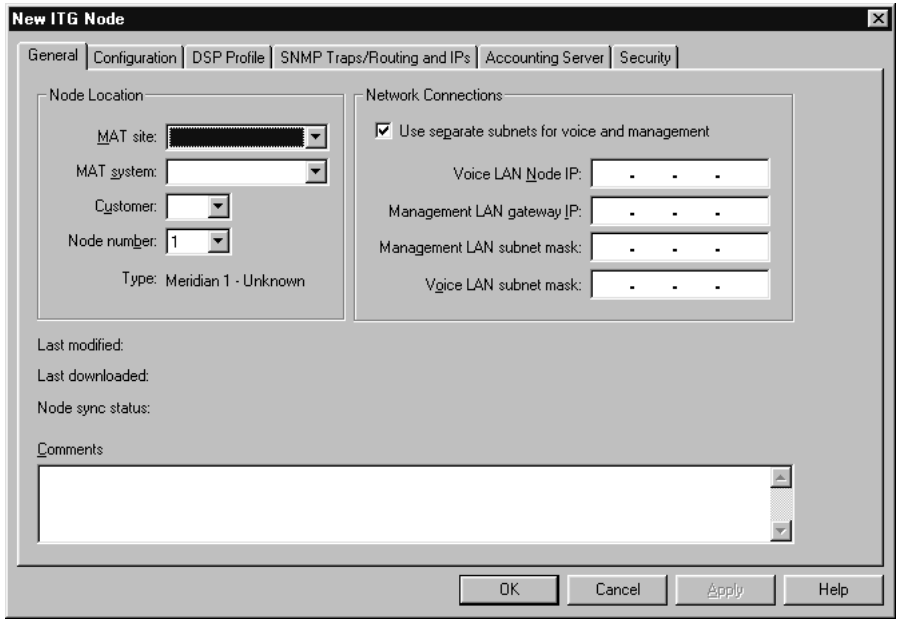
1. Launch the Meridian Administration Tools (MAT) application on the MAT PC.
2. From the MAT Navigator window, double-click the Services folder and double-click the **ITG ISDN IP Trunks** icon. The IP Telephony Gateway- ISDN IP Trunk Main window opens.
3. Select **Configuration | Node | Add** in the IP Telephony Gateway - ISDN IP Trunk Main window. The Add ITG Node window appears.
4. In the Add ITG Node window, leave the default selections **Meridian 1** and **Define the node configuration manually**. Click **OK.** The Node Properties General window appears (see Figure 28).

Set node location properties

1. Set Node Location properties: select the **MAT site**, **MAT system**, **Customer**, and **Node number** from the drop-down list boxes.

   Note: The Site name, Meridian 1 system name, and Customer must exist in the MAT Navigator before you can add a new ITG node.

Figure 28
ITG Node Properties - General tab



Single vs. separate subnets for T-LAN and E-LAN

It is *highly recommended* that you use separate subnets and separate T-LANs and E-LAN for the ITG Trunk voice and management networks. Separate subnets implies separate port groups on hubs or switches for T-LANs and E-LAN and separate IP Gateway (Router) interfaces with one subnet per router interface.

For traffic reasons, you should use separate subnets for nodes consisting of multiple 24-Port ITG Trunk cards.

Refer to the Engineering Guidelines sections “Set up a system with separate subnets for voice and management” on page 130 and “Single subnet option for voice and management” on page 131.

If you select the single subnet option, the E-LAN is used for the voice and management network, and all voice and management data goes through the 10BaseT management Ethernet interface (lnIsa0) on the motherboard of the ITG Trunk card.

Configure Network Connections

1 Decide subnet settings:

- **a** If you will be using *separate subnets* for the voice (T-LAN) and management (E-LAN) networks, accept the default setting **Use separate subnets for voice and management** check box.
- **b** If you will be using the *same subnet* for the voice and management network (E-LAN), uncheck the **Use separate subnets for voice and management** check box. The window changes.

2 If you accepted the default setting **Use separate subnets**, perform steps a-d.

- **a** Enter the **Voice LAN Node IP**
- **b** Enter the Management LAN gateway IP
- **c** Enter the Management LAN subnet mask
- **d** Enter 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 you unchecked **Use separate subnets,** perform steps a-c:

- **a** Enter the **Management LAN Node IP**
- **b** Enter the Management LAN gateway IP. The Management gateway (router) also functions as the voice gateway (router).
- **c** Enter the **Management LAN subnet mask**

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 press OK or Apply until you have completed the Configuration tab.

Configure card properties

These procedures explain how to configure the ITG ISL trunk card roles, IP addresses, TN, card density and D-Channel settings. Each ITG ISL Trunk 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. To add an ITG card to the node, perform the following steps:

1 From the **General** tab, click the **Configuration** tab. If you selected the single subnet option in the General tab, the Voice IP and Voice LAN gateway IP fields will be greyed-out.

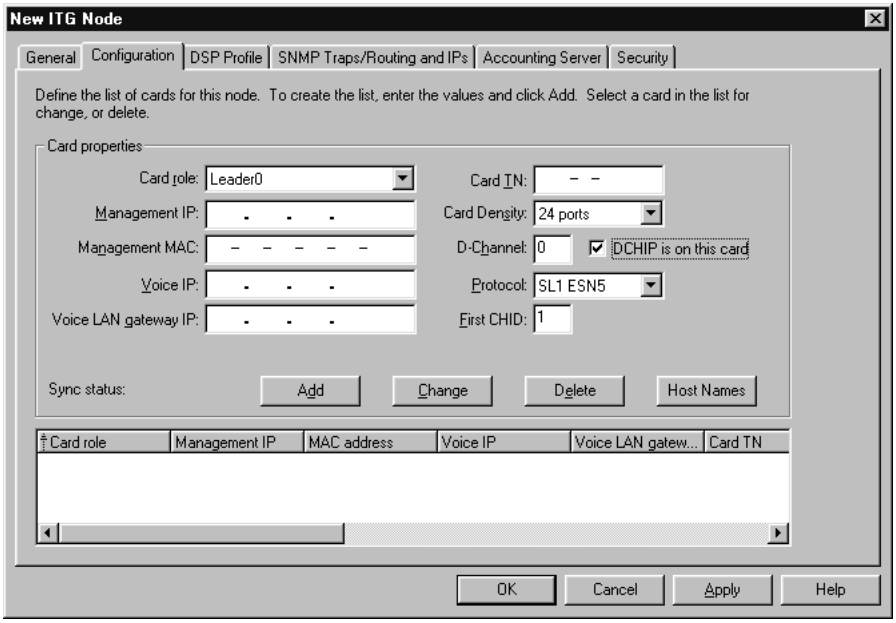
2 Select the **Card role** from the drop-down list box:

When you add the first card, select the card role **Leader 0**. When you add the second card, select the card type **Leader 1**. When you add additional cards, select the card type **Follower**. You configure the DCHIP and D-Channel information.

3 If you checked **Use separate subnets** in the **General** tab, perform steps a-d.

- **a** Enter the **Management IP** address.
- **b** Enter the Management MAC address. It is the motherboard Ethernet address. You can find it on the faceplate label of the card you are currently configuring. It is also identified as lnIsa0 on the card startup messages and by the ifShow command in the ITG shell.
- **c** Enter Voice IP address (see Notes 1 and 2).
- **d** Enter Voice LAN gateway IP address (see Notes 1 and 2).

Figure 29
Configuration tab



Note 1: 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 Voice or T-LAN subnet.

Note 2: Each Follower card can optionally have their Voice IP and Voice LAN gateway IP on a different Voice or T-LAN subnet from Leader 0 and Leader 1.

4 If you unchecked **Use separate subnets** in the **General** tab**,** perform steps a and b:

a Enter the **Management IP** address.

b Enter the Management MAC address. It is the motherboard Ethernet address. You can find it on the faceplate label of the card you are currently configuring. It is also identified as lnIsa0 on the card startup messages and by the ifShow command in the ITG shell.

The Management LAN Node IP and Management gateway IP addresses on the **General** tab and the Management IP address for Leader 0, Leader 1 and all Follower cards on the **Card Configuration** tab must be on the same Voice/Management E-LAN subnet.

5 Enter the **Card TN**. For Large Systems, 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 box: 24 ports for NT0961AA; 8 ports for NTCW80.

7 Enter the ISL **D-channel** logical device number. Its range is 0-255 for Large Systems; 0-79 for Small Systems.

8 If the card will be a DCHIP card, check 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 on Leader 0 and the second DCHIP on Leader 1. Additional DCHIPs can be put on Follower cards.

9 Select the **Protocol** for the DCHIP card from the drop-down list box. The protocol must match the protocol configured in LD16 in the route data block at the IFC prompt with respect to SL1 vs. ESGF or ISGF QSIG interface (IFC) and in LD17 at the IFC prompt under ADAN DCH. In LD 16, if SIGO is set to STD, then you must select the SL1 protocol. If SIGO is set to ESN5, then you must select SL1ESN5 protocol. In a mixed ESN5 and non-ESN5 network, you must 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 223.

The choices are SL1, SL1 ESN5, ESIG and ISIG for networks consisting of Meridian 1 large systems. For networks that include Meridian 1 small systems, the choices are SL1 or SL1 ESN5.

In addition to ITG ISL Trunk nodes, the IP telephony trunk network may contain ITG Trunk 1.0 Basic Trunk nodes or Nortel Networks IP Telephony Connection Manager. Use H323 V2 node capability for these nodes.

Once you define a DCHIP for the ITG Trunk node the protocol field is greyed-out when you select other cards in the same ITG Trunk node.

10 Enter the **First CHID** (Channel ID) for this ISL trunk card in the First CHID edit box. The First CHID range is:

- 1-259 for the NT0961AA 24-port ITG Trunk card
- 1-375 for the NTCW80 8-port ITG Trunk card

The First CHID is the ISL Channel ID of Unit 0 on this ITG Trunk card, as configured in LD 14 for the 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, you do not click OK until you add all cards to the node and complete all configuration tasks. If you click OK before you complete configuration, MAT exits the node property configuration session and displays the IP Telephony Gateway - ISDN IP Trunk Main Window. To complete the configuration tasks, double-click on the new ITG Trunk node in the list in the upper part of the Main Window.

12 Repeat steps 1-10 for Leader 1 and each Follower in the ITG Trunk node.

Configure DSP profiles for the ITG Trunk node

In this procedure, you select a DSP profile, and set Profile Options and Codec Options and, if required, modify default DiffServ/TOS values from 0. You set these profiles once for the ITG Trunk node. In a later step, you download the DSP profiles card properties to each card.

1 Click the **DSP Profile** tab (see Figure 30). The **General** tab displays a detailed description of the default DSP Profile 1

2 Change the default **DSP profile** from the drop-down list box if required. There are three DSP profiles. Each profile contains two or more codecs. All ITG 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. If you are not an expert in Voice over IP, do not modify the default DSP profile. See “ITG Trunk DSP profile settings” on page 135.

3 Click the **Profile Options** tab (see Figure 31). This tab displays the default **General** and **FAX options** values according to the selected DSP profile.

Figure 30
DSP Profile General tab

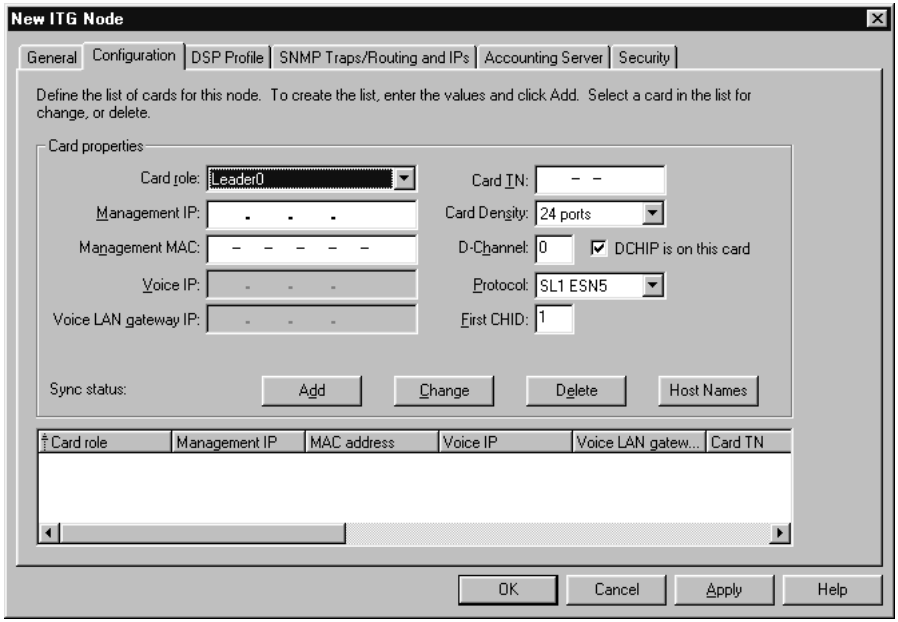
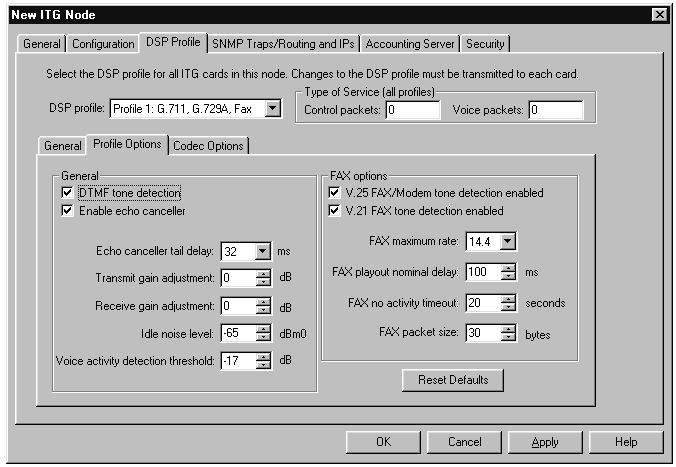


Figure 31
ITG Node Properties – DSP Profile Options tab



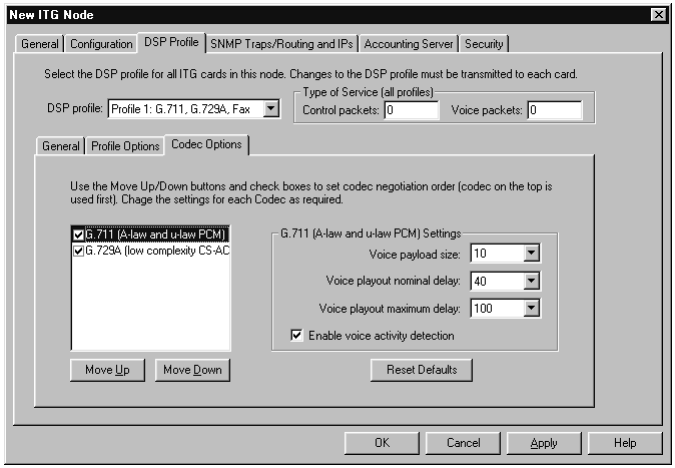
4 Change the **General** and **FAX option** parameters, if required. To revert to the default settings, click **Reset Defaults**.

CAUTION

The default DSP Profile Option settings for each codec are appropriate for most applications. If you are not an expert in Voice over IP, do not modify the Profile Options parameters. See “ITG Trunk DSP profile settings” on page 135.

5 Click the **Codec Options** tab (see Figure 32). This tab displays the default order of the preferred codec selection for outgoing calls and shows advanced codec parameters for the selected codec.

Figure 32
ITG Node Properties – DSP Profile Codec Options tab



Perform steps 6 and 7 if required. To revert to the default settings, click **Reset Defaults**.

CAUTION

The default Codec Options are appropriate for most applications. If you are not an expert in Voice over IP, do not modify the Codec Options parameters. See “ITG Trunk DSP profile settings” on page 135.

6 To turn off a codec, click on the codec and uncheck the checkbox.

7 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. ITG Trunk node requests the codec at the top of the list first on outgoing calls.

8 To enable Voice Activity Detection for silence suppression, check the appropriate box. To disable Voice Activity Detection for silence suppression, uncheck the box.

Change default DiffServ/TOS value for Control and Voice

1 Enter the **DiffServ/TOS** value for **Control** and **Voice**, 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 Type of Service (TOS) byte or Differentiated Service (DiffServ) code point determine 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.

DiffServ/TOS 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.

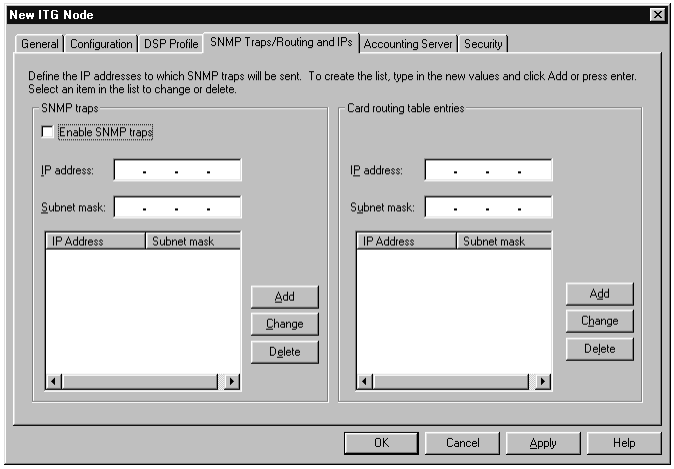
2 Click **Apply**.

Configure SNMP Traps/Routing and IPs tab

In this procedure, you define up to eight SNMP Trap destination IP addresses and subnet masks, and up to eight Card Routing Table Entry IP addresses and subnet masks. These SNMP trap and Card routing table settings become active when you transmit the card properties to the ITG trunk cards.

1 Click **SNMP Traps/Routing and IPs** tab (see Figure 33).

Figure 33
ITG Node Properties window – SNMP Trap Addresses/Routing table IPs tab



2 Check the **Enable SNMP traps** check box to enable sending of SNMP traps to the SNMP managers that appear in the list. You must enter at least one SNMP trap address if you check this option. The SNMP trap addresses determine where event and alarm messages are sent.

Refer to “Configure MAT Alarm Management to receive SNMP traps from ITG ISL Trunk cards” on page 231 to configure MAT Alarm Notification to monitor SNMP traps for ITG cards.

3 Enter the SNMP Manager IP address in the IP Address field, and enter the Subnet mask in the **Subnet mask** field. Click **Add**. The new IP address and subnet mask appears in the SNMP Manager IP address list.

Enter SNMP trap IP addresses for MAT PCs on local and remote subnets and any other SNMP Management PCs for Alarm monitoring. All MAT PCs must have the Alarm Notification feature.

- The MAT PC on the local subnet or E-LAN.
- MAT PC on a remote subnet on the customer's IP network.
- Remote support MAT PC PPP IP address (on the E-LAN) configured in the Nortel Networks Netgear RM356 Modem Router, or equivalent
- Any SNMP managers for remote alarm monitoring

In the next step, you add the SNMP trap IP addresses for remote subnets in the Card Routing Table entries IP address field.

4 Configure the **Card routing table entries:**

5 Enter 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, you transmit this information to each ITG card.

The ITG card uses the addresses in the routing table entries to route management packets over the Management Gateway (router) on the E-LAN. Without routing table entries, the ITG card routes management traffic over the voice LAN gateway. Sending management traffic over the voice LAN can affect voice quality.

6 Click **Apply**.

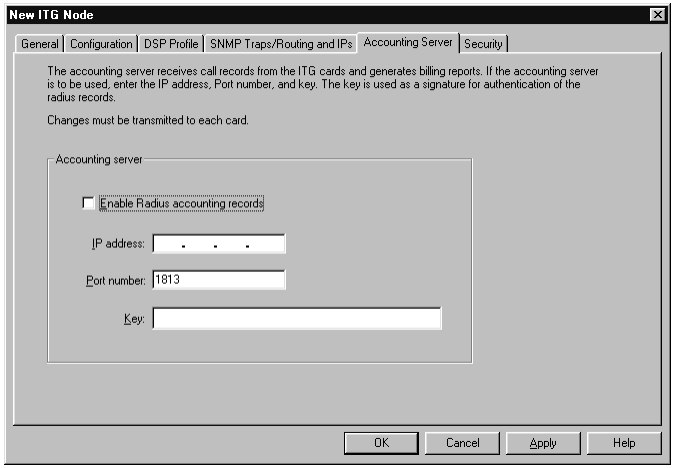
Configure Accounting server

If you do not have a Radius Accounting Server, skip this step. A Radius Accounting Server collects call records from the ITG ISL trunk cards and generates billing reports.

1 Click the **Accounting Server** tab (see Figure 34).

2 Click the **Enable Radius accounting records** checkbox.

Figure 34
ITG Node Properties window - Accounting Server tab



3 Enter the Radius accounting server IP address. Add the same Accounting Server IP address configured in the Card Routing Table entries as discussed in “Configure SNMP Traps/Routing and IPs tab” on page 204.

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 alphanumeric characters.

6 Click **Apply**.

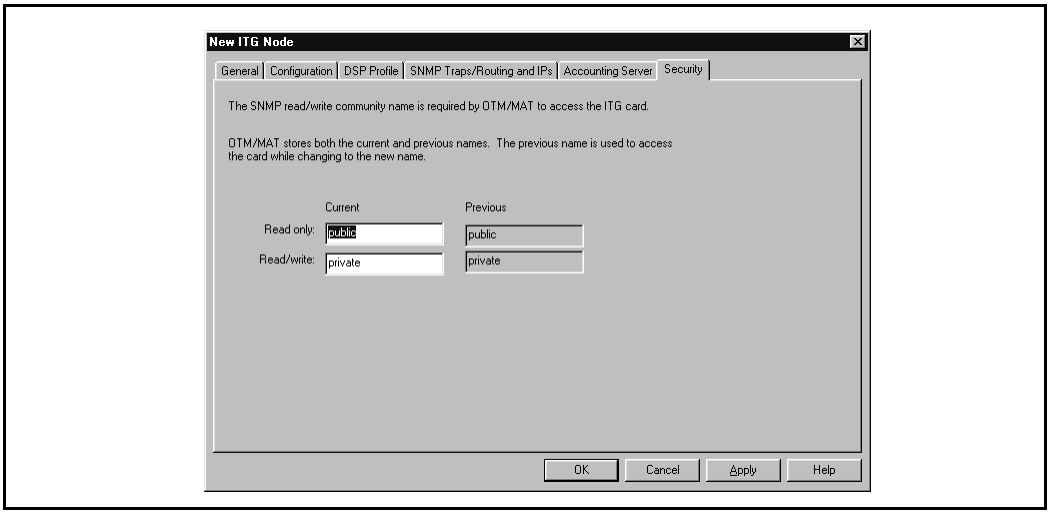
Set Security for MAT SNMP access

This procedure explains how to change the SNMP community names. which you change to provide better security for the ITG node. MAT uses the community name password to refresh the ITG Trunk node and card status, and to control the transmitting and retrieving of files for database synchronization.

Note: If you forget the community names, connect a TTY to the ITG card maintenance port. Restart the card. The card displays the community name on the tty during startup.

1 Click the **Security** tab (see Figure 35).

Figure 35
ITG Node Properties window - Security tab



2 Change the default Read only and Read/Write default community names. MAT uses the previous read/write community name to transmit the card properties. The first time you transmit data after changing the password, MAT uses the Previous read/write password. MAT uses the changed password for all following data transmissions.

Exit node property configuration session

The procedure to add an ITG Trunk node on MAT manually is complete. Press OK to save the node and card properties configuration and exit. MAT displays the IP Telephony Gateway - ISDN IP Trunk Main window. If you plan to manage a network of ITG ISL Trunk nodes from this MAT PC, add the remaining ITG ISL Trunk nodes before you configure the dialing plan for the new ITG Trunk nodes on MAT.

Create the ITG Trunk node dialing plan using MAT

In this procedure, you configure the ITG Trunk node dialing plan in MAT. Use this procedure to create the dialing plan for the first node in the network. This procedure will also work to create a dialing plan for a new node in a very small network. If you are adding a new node to a large existing network, it is more efficient to retrieve the ITG Trunk node dialing plan from an existing node. See “Retrieve the ITG Trunk node dialing plan using MAT” on page 213.

A dialing plan consists of a number of ITG Trunk destination nodes and one or more dialing plan entries for each destination node. You select a destination node, define the destination node protocol capability, decide if you want to enable Quality of Service (QoS) monitoring for this destination node, and enter one or more ESN dialing plan entries for each destination node. You repeat this procedure for all destination nodes in the ITG Trunk network.

The dialing plan information you enter in MAT must match the ESN data entered in the Meridian 1 overlays (LD15, LD16, LD86, LD87 and LD90). You must keep the dialing plan entries consistent between the Meridian 1 and the ITG Trunk node. Transmit the dialing plan from MAT ITG to the ITG Trunk node during installation, card replacement, when ITG Trunk nodes are added to the network, or whenever you change the dialing plan on MAT ITG.

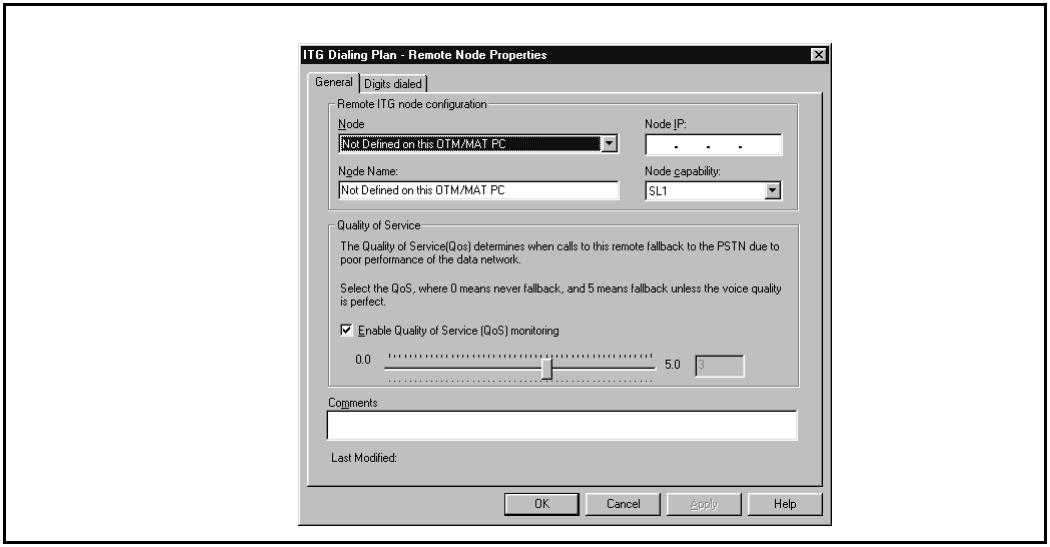
Each ITG Trunk node shares one dialing plan for all cards in the node. The ITG Trunk node dialing plan translates the dialed digits in the Meridian 1 ISDN Signaling Call Setup message, according to ESN translation type, into the Node IP addresses of the ITG Trunk destination nodes.

Configure General tab

1 In the IP Telephony Gateway - ISDN IP Trunk Main window, select the new ITG Trunk node for which you want to build a dialing plan. Select menu **Configuration | Node | Dialing Plan**. The ITG Dialing Plan window appears

2 In the ITG Dialing Plan window, select menu **Configuration | Add remote node.** The ITG Dialing Plan - Remote Node Properties window appears and displays the General tab (see Figure 36.) The default Node drop-down list reads “Not defined on this MAT PC.” and the Node IP address field is blank. When you click the drop-down list, you see a list of all the other ITG ISL Trunk nodes configured on this MAT PC. You do not see the ITG ISL Trunk node for which you are creating the dialing plan.

Figure 36
ITG Dialing Plan - Remote Node Properties window (General tab)



3 Select the destination **Node** to be added from the list. MAT provides the ITG Trunk **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 ITG ISL Trunk node. The protocol must match the protocol configured in LD16 in the route data block at the IFC prompt with respect to SL1 vs. ESGF or ISGF QSIG interface (IFC) and in LD17 at the IFC prompt under ADAN DCH. In LD 16, if SIGO is set to STD, then you must select the SL1 node capability. If SIGO is set to ESN5, then you must select SL1ESN5 node capability. In a mixed ESN5 and non-ESN5 network, you must 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 223.

The choices are SL1, SL1 ESN5, ESIG and ISIG for networks consisting of Meridian 1 large systems. For networks that include Meridian 1 small systems, the choices are SL1 or SL1 ESN5.

In addition to ITG ISL Trunk nodes, the IP telephony trunk network may contain ITG Trunk 1.0 Basic Trunk nodes or Nortel Networks IP Telephony Connection Manager. Use H323 V2 node capability for these nodes.

Quality of service

The default setting enables Quality of Service monitoring. QoS monitoring allows new calls to fall back to alternate circuit switched trunk routes when the IP network Quality of Service falls below the configured threshold. If you change the default setting and disable QoS monitoring, then the ITG trunk node attempts to complete new calls over the IP network regardless of the IP network QoS. You can still have alternate routes but ITG Trunk only uses them if the D-Channel connection to the local ITG Trunk node fails, or 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 56 and Table 24, “ITG QoS levels,” on page 143 for more details on Quality of Service levels and MOS values.

Configure Digits dialed tab

In this tab, you configure one or more ESN translations for the current destination node. Figure 37 describes the Dialed Digits tab fields.

1 Click on the **Digits dialed** tab.

MAT displays the **Digits dialed** tab.

2 Select the ESN translation type from the **Dial Plan** drop-down list. You must add every ESN translation configured for this destination node in the Meridian 1 ESN (LD86, LD87 and LD96) one at a time.

3 Enter the Called Number digits for the ESN translation type in the **Dial Plan Digits** field (see Figure 34, number 2).

Note: The digits must be leftwise unique within the ESN translation types that correspond to given pair of NPI and TON values. Every Meridian 1 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.

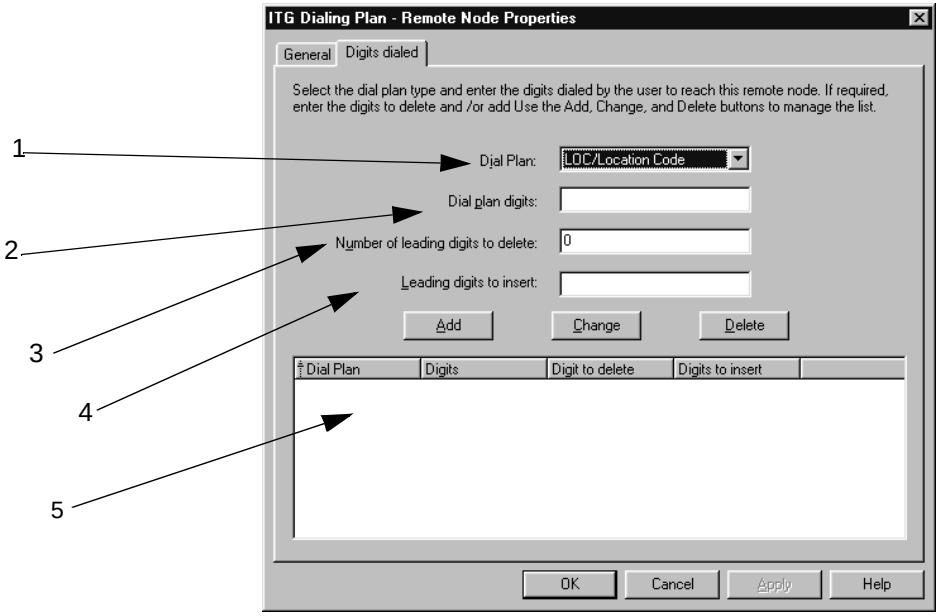
Note 1: The digit manipulation defined in the Digits dialed tab of the ITG Dialing Plan - Remote Node Properties window does not apply to the Destination Number of the Facility messages for non-call-associated signalling for MCDN features. These features include: NRAG, NMS, NACD, and NAS.

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**.

Figure 37
ITG Dialing Plan - Remote Node Properties window - Digits dialed tab



1. **Dial Plan** - Click on 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 Meridian 1 after digit absorption, insertion and manipulation by Meridian 1.

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 ITG 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.

7 Repeat steps 7 through 11 until you have added all the ESN translation Dial Plan digits for this destination node.

8 Click **OK**.

The Dialing Plan window is displayed with the added dialing plan entries.

9 Repeat steps 2 through 13 until you have added dialing plan entries for all the destination nodes in the drop down list and all destination nodes Not Defined on this MAT PC.

Retrieve the ITG Trunk node dialing plan using MAT

If you are adding a new node to a large existing network, it is more efficient to retrieve the ITG Trunk node dialing plan from an existing node. Make the necessary modifications before transmitting the dialing plan to the new node.

1 In the IP Telephony Gateway - ISDN IP Trunk Main Window, select an existing ITG Trunk node which has a dialing plan similar to one you are creating for the new ITG Trunk node.

2 Make sure that MAT can monitor the card state of Leader 0 in the existing node from which you are retrieving the dialing plan. 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 which you 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 will appear asking you to enter the new node's community name.

10 Click **Start Retrieve** and monitor progress in the Retrieve control field. Make sure the dialing plan is retrieved successfully and added to the MAT database.

11 Click **Close** to close the ITG Retrieve Options window and return to the IP Telephony Gateway - ISDN IP Trunk Main 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 on an dialing plan entry to inspect its property sheet. To save modifications, click **Apply** and then **OK**.

From the **View** menu, you have the option of viewing by **Digits dialed** or **Remote Nodes**.

Transmit ITG trunk card configuration data from MAT to the ITG trunk cards

ITG Trunk nodes and cards are configured in the MAT ITG ISDN IP Trunk application and then transmitted to the ITG cards. The configuration data is converted by MAT to text files. The ITG cards then get the configuration files from MAT using a File Transfer Protocol (FTP) server on MAT.

Before you can transmit configuration data

Perform the following procedures in any order before transmitting configuration data:

- Install the ITG Trunk cards in the Meridian 1 IPE modules or cabinets and cable them to the T-LAN and E-LAN Ethernet hubs, Ethernet switches, and IP routers.
- Configure the ITG Trunk data in the Meridian 1. Disable the ITG Trunk cards in LD32.
- Configure the ITG Trunk data on MAT.
- Connect a local RS232 terminal to the serial maintenance port to set the Leader 0 IP address. Under certain conditions, the local terminal is required to configure IP routing table entries in the Leader 1 card and each of the Follower cards.
- Connect the MAT PC to the local E-LAN subnet or to a remote subnet across the LAN/WAN from a remote subnet.

Setting the Leader 0 IP address

Configure the IP address of the Leader 0 ITG card, using the ITG shell command line interface.

1 To access the ITG shell, connect a MAT PC to the RS232 serial maintenance port on the faceplate of the ITG Leader 0 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 MAT 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 E-LAN, T-LAN, RS232 Ports cable for non-DCHIP cards, to create a more permanent connection to the ITG 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 MAT ITG PC: 9600 baud, 8 bits, no parity bit, one stop bit.

When a new ITG Trunk card starts up and displays "T:20" on the 4-character display, the ITG card will begin sending bootp requests on the E-LAN. A series of dots appears on the TTY.

3 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>

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 Management IP address of Leader 0 on the E-LAN,
- where “yyy.yyy.yyy.yyy” is the Management Gateway (Router) IP address on the E-LAN. If the MAT PC will be connected locally to the LAN, and there is no management LAN gateway, then the Gateway IP address is “0.0.0.0”.
- and where “zzz.zzz.zzz.zzz” is the subnet mask for the management IP address of Leader 0 on the E-LAN.

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 management 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, you must 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 *Appendix D*.

5 Press **Enter**.

6 Press the reset button on the faceplate to reboot the Leader 0 ITG Trunk card.

After the reboot is completed, the Leader 0 card will be in a state of "backup leader". The faceplate display will show "BLDR." It cannot yet be in a state of "active leader", until you have successfully transmitted the node properties from MAT to the Leader 0 card.

Transmit the node properties, card properties and dialing plan to Leader 0

Verify that the ITG Trunk cards are disabled in LD32 in the Meridian 1 before transmitting card properties.

Note: It is necessary to disable ITG Trunk cards whenever transmitting card properties or new software.

Use the MAT Maintenance Windows, the MAT System Passthru terminal, or use a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1. Use the overlay 32 DISI command to disable the ITG cards when idle. In the MAT IP Telephony Gateway - ISDN IP Trunk main window, select **View | Refresh** and verify that the card status is showing "Disabled". If the card status is showing "unequipped," configure the card in LD14.

1 From the **MAT Navigator** window, double-click the **ITG ISDN IP Trunks** icon from the **Services** folder. The IP Telephony Gateway - ISDN IP Trunk Main window opens.

2 Select the ITG Trunk node for which you want to transmit properties 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 Main 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 ITG 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 ITG card.

Verify installation and configuration

To verify installation and configuration:

Check 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 you have a MAT PC on the local E-LAN subnet, it should now be in communication with all cards in the ITG Trunk node.

Observe ITG ISL trunk status in MAT

1 From the MAT IP Telephony Gateway - ISDNIP Trunk Main window, select menu **View | Refresh**, and verify that the card status is showing “enabled” or “disabled” (depending on the card status in the Meridian 1). If any cards show “not responding”, verify:

a the management interface cable connection to the E-LAN

b the voice interface cable connection to the T-LAN

c the management MAC addresses that were entered previously on the “Configuration” tab of the Node Properties, while adding the ITG node on MAT.

d IP addresses

Note: If you are installing ITG ISL Trunk Node from a MAT PC on a remote subnet, and you cannot communicate with the Leader 1 and the follower cards 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 back to the remote MAT PC through the default IP route that points to the voice gateway (router) on the T-LAN.

To establish communication with Leader 1 and the Follower cards from a MAT PC on a remote subnet, you must connect a local terminal to the maintenance port on the faceplate of the Leader 1 and Follower cards and use the ITG shell command 'routeAdd' on Leader 1 and each Follower card to add a new IP route for the remote MAT PC subnet that points to the Management Gateway (router) IP address. Repeat this step every time a card is reset until the card properties (containing 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 MAT PC, and
yyy.yyy.yyy.yyy is the IP address of the management gateway on the E-LAN.

Press **Enter**.

2 Verify that the TN, management interface MAC addresses, and IP addresses are configured correctly for each ITG card. Select any card in the ITG node in the MAT ITG ISDN IP Trunk main window, and select menu **Configuration | Node | Properties** from the drop-down menus. Compare the values displayed on the "General" tab and the "Card Configuration" tab with those on the ITG Trunk 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.

Transmit Card Properties and Dialing Plan to Leader 1 and Follower cards

Verify that the ITG Trunk cards are disabled in the Meridian 1 before transmitting card properties.

Note: Disable ITG Trunk cards when transmitting card properties or new software.

Use the MAT Maintenance Windows, the MAT System Passthru terminal, or use a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1. Wait for the NPR0011 message, which indicates that all units on each card are disabled.Use the overlay 32 DISI command to disable the ITG cards when idle. In the IP Telephony Gateway - ISDN IP Trunk Main window, select **View | Refresh** and verify that the card status is showing "Disabled". If the card status shows "unequipped," configure the card in LD14.

1 Select the ITG Trunk node for which you want to transmit properties 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 Main window, select menu **Configuration | Synchronize | Transmit**.

4 Leave 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 ITG ISL Trunk cards, which are identified by TNs.

7 When the transmission is complete, click the **Close** button.

8 Use the overlay 32 ENLC command to enable the ITG cards in the node.

9 In the IP Telephony Gateway - ISDN IP Trunk Main window, select **View | Refresh**. The card status should now show "Enabled."

10 Verify the TN, management interface MAC address, IP addresses, and D-Channel for each ITG card. Compare the configuration data with the data on the ITG Installation Summary Sheet.

Once the Card Properties and Dialing Plan have been successfully transmitted, the new Card Properties and Dialing Plan are automatically applied to each card. The ITG node is now ready to make test calls provided that the ITG ISL Trunks and the ESN data have been configured on the Meridian 1.

Set date and time for the ITG ISL Trunk node

Set the date and time on the ITG ISL Trunk 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.

1. Select the ITG ISL Trunk node for which you want to set date and time from the list in the upper part of the IP Telephony Gateway - ISDN IP Trunk Main window.
2. Double-click on Leader 0 from the list in the lower part of the Main window. The ITG Card Properties Maintenance tab appears.
3. Click on 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 ITG ISL Trunk node.

Change the default ITG shell password to maintain access security

You must change the default user name and password when installing the ITG Trunk node to maintain access security. The ITG user name and password protects maintenance port access, Telnet, and FTP access to the ITG card over the LAN.

1. Select the new ITG Trunk node in the upper part of the IP Telephony Gateway - ISDN IP Trunk Main window.
2. For each card in the node, right-click on the card and select **Telnet to ITG Card** from the right-click menu.
3. The Telnet window appears with the VxWorks prompt:
4. When prompted to login, enter the default username and password as:

   VxWorks login: **itgadmin**
   Password: **itgadmin**

   ITG>

5 Use the command **shellPasswordSet** to change the default user name and password for Telnet to ITG shell and FTP to the ITG card file system. The default user name is **itgadmin** and the default password is **itgadmin**.

You will be prompted for the following information:

Enter current username: **itgadmin**
Enter current password: **itgadmin**
Enter new username: **newname**
Enter new password: **newpwd**
Enter new password again to confirm: **newpwd**

6 Record the new user name and password and transmit to authorized network security personnel.

7 Repeat procedure for all cards in the node.

If the entire sequence of commands is successfully entered, you get the system response with 'value = 0 = 0x0'. The new user name and password are now stored in the non-volatile RAM on the ITG card, and will be 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 279.

Change default ESN5 prefix for non-ESN5 IP telephony gateways

You must 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, you need to change the default ESN5 prefix to work with the established NCOS plan in the customer's network. Turn to "ESN5 network signaling" on page 186. You must perform this procedure on every card in the node.

1 Select the new ITG Trunk node in the upper part of the IP Telephony Gateway - ISDN IP Trunk Main window.

2 For each card in the node, right-click on the card and select **Telnet to ITG Card** from the right-click menu.

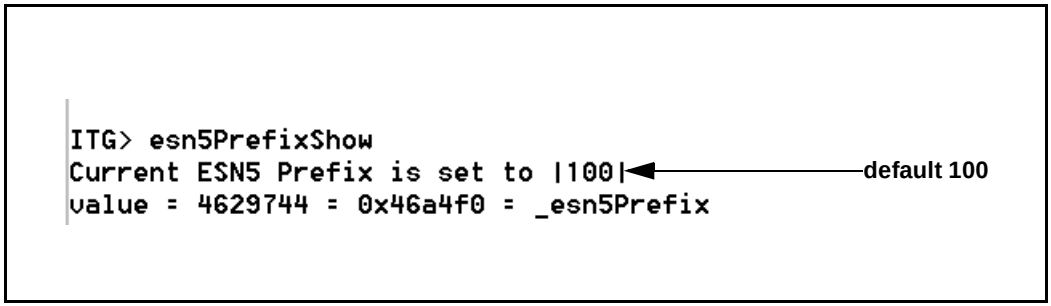
The Telnet window appears with the VxWorks prompt:

3 When prompted to login, enter the default (or user-modified) login and password:

4 VxWorks login: **itgadmin**
Password: **itgadmin**

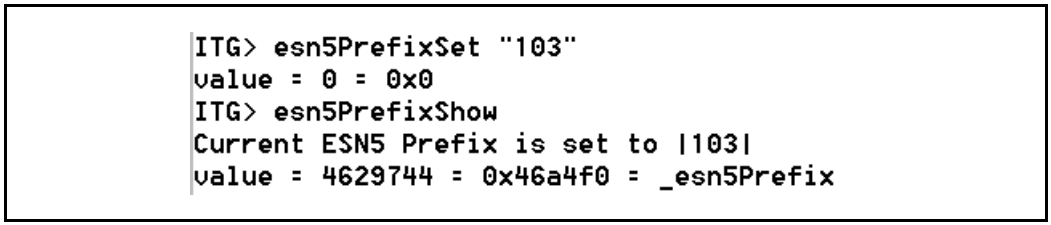
ITG> **esn5PrefixShow**

Figure 38
esn5PrefixShow



5 At the ITG prompt, enter >esn5PrefixSet “1xx” where xx = the NCOS value as shown in the example in Figure 39,. In the figure, the default value was changed from NCOS 00 to 03..

Figure 39
esn5PrefixSet



Check card software

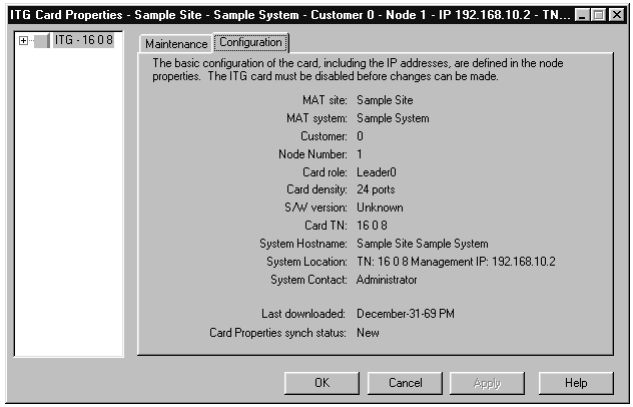
In this procedure, you check the software version of the cards in a new node. All cards must have same version. To ensure proper ITG ISL trunk network operation, Nortel Networks recommends that all network nodes have the same software version. Verify the software release from each card is the latest recommended software release for ITG ISL Trunk by connecting to a Nortel Networks website that contains the latest software versions for the NT0961 24-port card the NTCW80 eight-port card.

1 From the IP Telephony Gateway - ISDN IP Trunk Main window, click on the new node.

2 For each card in the node, starting with Leader 0, double-click on the card entry in the lower half of the window. The Card Properties window appears.

3 Click **Configuration** tab and record **S/W version**, **card density** and **TN** for each card in the new node (see Figure 40).

Figure 40
Properties configuration tab



6 The website URL to check the latest recommended ITG software release is:

http://www.nortelnetworks.com/itg

The browser prompts you to enter a user name and password.

The default user name is **usa**

The default password is **usa**

The software delivery main window appears.

7 Click **Download Software.** Compare the ITG card Properties software version to the version listed in the **Release** column.

a If versions match, software upgrade is not required. Turn to "Configure MAT Alarm Management to receive SNMP traps from ITG ISL Trunk cards" on page 231.

b If versions are different, go to step 6.

8 Fill in the **Name, Phone number** and **Company** fields. Click the **Download Current Release** button. The ITG Software Download Request Form window appears.

9 Download software packages and associated release notes:

a For 24-port cards, download the **Software Package** for **Release** ITG 2.24.xx

b For 8-port cards, download the **Software Package** for **Release** ITG 2.8.xx

10 When your browser prompts you, select Download. Record the file name and location of downloaded software on your MAT PC.

Now you are ready to transmit the new card software from MAT to the ITG ISL Trunk cards.

Transmit new software to ITG Trunk cards

Verify that the ITG Trunk cards are disabled in the Meridian 1 before transmitting new card software.

> ***Note:*** Disable ITG Trunk cards when transmitting card properties or new software.

Use the MAT Maintenance Windows, the MAT System Passthru terminal, or use a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1. Use the overlay 32 DISI command to disable the ITG cards when idle. NPROG indicates that all units on the card have been disabled. In the MAT IP Telephony Gateway - ISDN IP Trunk main window, select **View | Refresh** and verify that the card status is showing "Disabled". If the card status shows "unequipped," configure the card in LD14.

1 Open MAT. Click on **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 Main window.

3 Select node or cards for software transmission according to card density:

- **a** If all cards in the node have same card density (24-port or 8-port), you upgrade all the cards together by transmitting to the selected node. Click new node in upper half of the IP Telephony Gateway - ISDN IP Trunk Main window.
- **b** If you have a mix of 24-port and 8-port cards in the same ITG ISL Trunk node, then select all cards of the same density in the lower half of the Main Window. Hold down the **Ctrl** key while you make individual card selections.

4 Select menu **Configuration/Synchronize/Transmit**. The **ITG - Transmit Options** dialog box appears.

5 a. If you are transmitting new software to a node containing cards of the same density:

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 ITG card. Monitor the progress of the card software transmission in the Transmit Control window. ITG indicates success or failure of card software transmission by card TN. Scroll to verify that 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.

b. If you are transmitting new software to a node containing a mix of card densities:

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 8-port).

Click **Start Transmit**. The software is transmitted to each card in turn and burned into the flash ROM on the ITG card. Monitor the progress of the card software transmission in the Transmit Control window. ITG indicates success or failure of card software transmission by card TN. Scroll to verify that transmission was successful for all card TNs. The 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 ITG card that received transmitted software, so that the new software can begin operation. Start the rebooting with Leader 0, then Leader 1, and finally the follower cards.

Double-click on card in the lower part of the IP Telephony Gateway - ISDN IP Trunk Main window. The Card Properties Maintenance tab appears. Click **Reset** to reboot the card. Click **OK.**

Note: You also can 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 Main window, select the new node. Select menu **View/Refresh/Selected** or press F5.

8 After all ITG cards have been reset and have successfully rebooted, the **Card state** column shows disabled: active for Leader 0; disabled: standby for Leader 1; 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 overlay 32 ENLC command to re-enable the ITG cards.

The software upgrade procedure is complete.

Upgrade the DCHIP PC 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 Main window, right-click on 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 Trunk 2.0 card in LD32 (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.

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 will FTP the DCHIP PC Card from the Active Leader card. Since the FTP server on the ITG card is password protected, the user is prompted for the login/password fields. If correct, the upgrade of the DCHIP PC Card begins.

Once the upgrade is complete, the DCHIP card will reboot automatically.

Configure MAT Alarm Management to receive SNMP traps from ITG ISL Trunk cards

You must have the MAT Alarm Management option enabled to perform these procedures. For the procedure to activate SNMP trap generation on the ITG Trunk node, see “Configure SNMP Traps/Routing and IPs tab” on page 204. Enter the IP address of the MAT PC as described in the procedure referenced above.

1. In the MAT Navigator window select **Utilities | Alarm Notification**. The "MAT 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. .

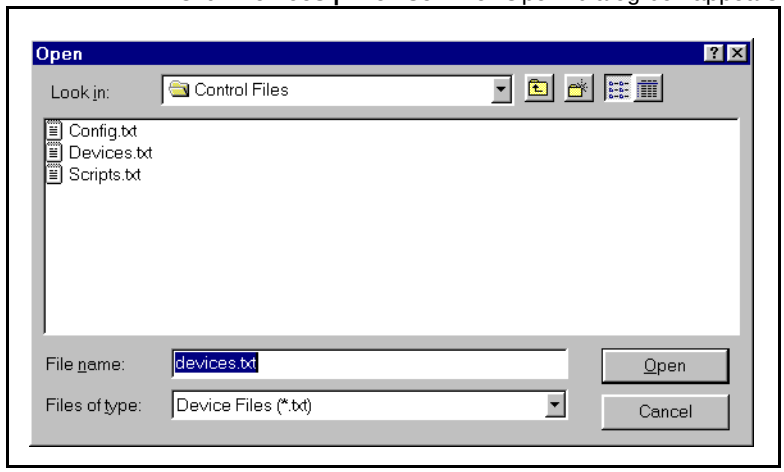


Figure 41
Open Devices.txt window

5 Select the "Devices.txt" file from the "Control Files" folder and click **Open**. The "Devices.txt" file opens. :

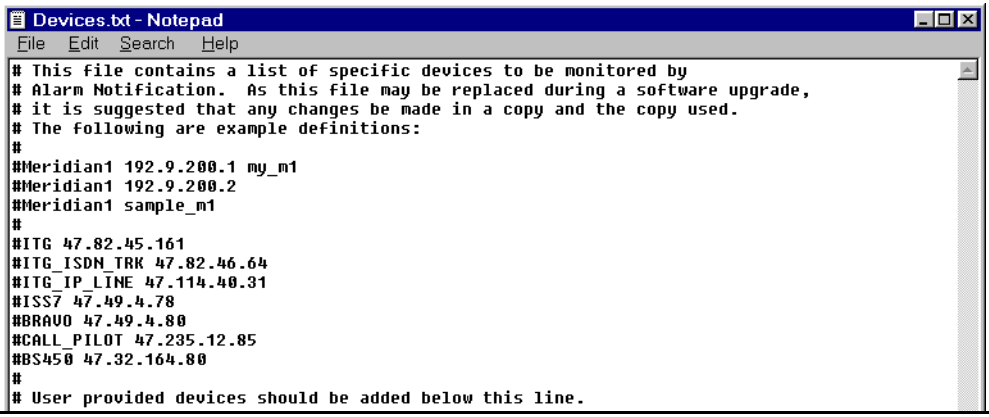
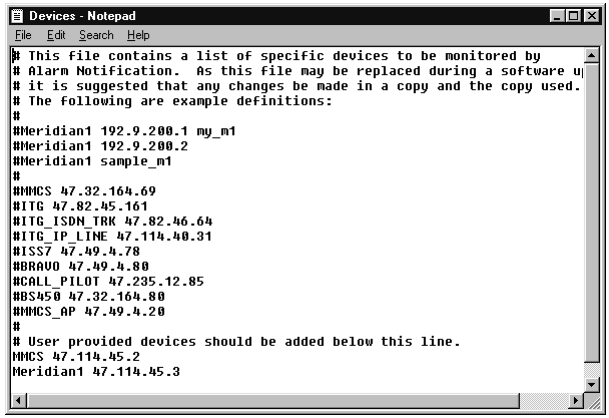


Figure 42
Devices.txt file



6 For each ITG Trunk card in each monitored ITG Trunk node, add a line consisting of three fields separated by spaces. 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 ITG devices with “#”.

Table 40
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 Meridian 1 site where the ITG Trunk node is located.		

7 Click **File | Save**.

8 In the Alarm Notification Run Options window, click **OK**.

MAT Alarm Notification must be restarted whenever Control Files are changed.

9 If MAT Alarm Notification is running (i.e., the red traffic light is showing on the tool bar), first stop it by clicking on the red traffic light on the tool bar. Restart it by clicking on the green traffic light.

10 If MAT Alarm Notification is not running (i.e., 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 ITG card and appears in the MAT Alarm Notification browser window. Verify the device name identifies the correct ITG card.

The procedure is complete.

Make test calls to the remote ITG nodes

Make test calls to check that:

- the ITG system can process calls from each node to a remote node,
- the ITG trunk cards are enabled,
- the Quality of Service, as defined within the Dialing Plan window, is acceptable.

Check the ITG operational report. If Fallback to PSTN occurs, examine the IP data network for problems. Also, check the ITG cards' dialing plan table and verify that the remote ITG node is powered up, configured, and enabled.

Upgrade an ITG Trunk 1.0 node to support ISDN signaling trunks

ITG Trunk 1.0 customers can upgrade their systems to ITG 2.0 to include ISDN Signaling Link (ISL) capabilities. An upgraded ITG Trunk 2.0 node can support 8-port and 24-port ITG Trunk cards in the same node. You must upgrade all eight-port cards in a node to ITG ISL software. ITG Trunk 2.0 also supports interworking between ITG ISL Trunk nodes and ITG 1.0 (Basic Trunk) nodes in the same network.

Upgrade procedure summary

1. If required, select at least one 8-port trunk card to support DCHIP functionality. In some cases, a new 24-port card will support DCHIP functionality.
2. Install DCHIP PC Card and pigtail cable in the selected 8-port trunk card.
3. Remove all ITG Trunk 1.0 software and configuration files from the 8-port cards.
4. Install new ITG ISL Trunk software on the 8-port cards.
5. Remove ITG 1.0 configuration data from Meridian 1.
6. Configure the upgraded cards as if you were performing a new ITG 2.0 24-port installation.

   Note: When a node includes 8-port and 24-port cards, you must upgrade all 8-port cards to the 2.0 software. the standard configuration is to have the 24-port card support the DCHIP functionality.

Before you begin

The list below is numbered for convenience. The steps can be accomplished in any order.

1 Upgrade to MAT 6.6 or later. Make sure you install all the ITG and Alarm Management applications.

2 Upgrade Meridian 1 X11 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 1, “Software packages for Meridian 1 ITG ISL Trunk,” on page 22 lists required software packages.

3 Download the ITG 8-port upgrade software from the website. The website URL to check the latest recommended ITG software release is:

http://www.nortelnetworks.com/itg

The browser prompts you to enter a user name and password.

The default user name is **usa**

The default password is **usa**

The filename that you want to download is called “ITG28xx.mms” where “ITG2” indicates the ISL trunk software, “8” indicates it is the upgrade software for an 8-port card, and “xx” is the software revision level.

WARNING

It is critical that you install *only* the 8-port software on the 8-port cards. If you install the 24-port software, the 8-port card will become unusable and must be returned to Nortel Networks for repair.

4 If you are adding 24-port cards to the 8-port node as part of the upgrade, check that the required LAN networking equipment and cables are installed. For networking equipment requirements, turn to “ITG Engineering Guidelines” on page 71. Leader 0 and Leader 1 must be on the same subnet T-LAN.

5 If you are upgrading an 8-port ITG Trunk Card to support DCHIP functionality, you need one hardware upgrade kit (NTZC47AA for large systems, and NTZC47BA for small systems). 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 8-port trunk card. At the ITG> prompt, enter

itgCardShow

Write down the IP address and other card data.

7 If required for an 8-port 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 Check that the customer site has a Nortel Networks Netgear RM356 Modem Router (or equivalent) on the E-LAN. The modem router provides remote support access to ITG Trunk and other IP-enabled Nortel Networks products on the Meridian 1 site.

9 Identify the TNs of the ITG Trunk 1.0 cards that you will be upgrading. Open MAT ITG M1 IP Trunk main window. The TNs are listed.

Install the DCHIP hardware upgrade kit

In this procedure, you upgrade an ITG Trunk 1.0 node by installing at least one eight-port DCHIP hardware upgrade kit.

Note: Skip this step if the DCHIP functionality is provided by a 24-port ITG Trunk 2.0 card.

1 Disable all 8-port ITG trunk cards in the node that you are upgrading. Disable the cards in LD32 (DISI l s c for large systems, DISI c for Option 11). Wait for the NPR0011 message, which indicates that all units on each card are disabled.

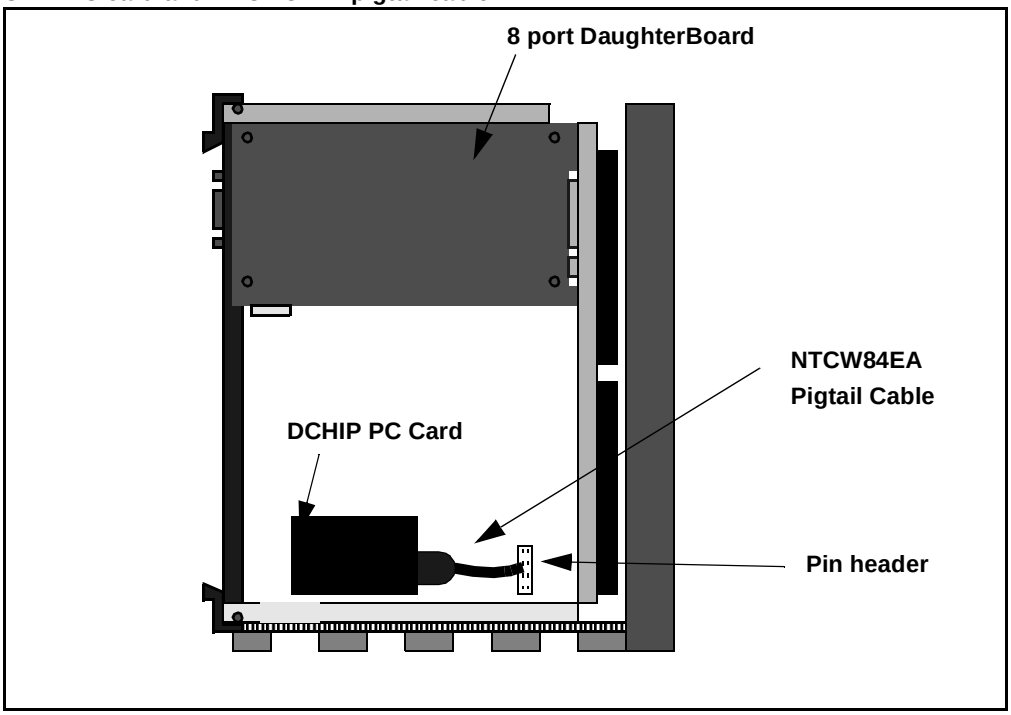
Note: Whenever you work on the card, be sure you are wearing an anti-static wrist strap.

2 Select the card in which you are going to install the DCHIP hardware upgrade kit. Disconnect T-LAN cable from faceplate (NTCW80AA only) and label the cables for reconnection. Remove card from 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 43.)

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 43). 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 43
DCHIP PC card and NTCW84EA pigtail cable



5 Pull the top and bottom locking devices away from the ITG faceplate. Insert the ITG card into the card slots and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

Install the DCHIP I/O Panel breakout cable from the upgrade kit

The breakout cable provides one D-channel connector.

If you are installing the DCHIP upgrade kit for the NTCW80AA 8-port ITG Trunk card, use the NTCW84MA I/O Panel breakout cable.

If you are installing the DCHIP upgrade kit for the NTCW80CA 8-port ITG Trunk card, use the NTCW84LA I/O Panel breakout cable.

1 For the large system, locate the I/O connector that corresponds to the leftmost card slot of the ITG 8.0 port that is undergoing the hardware upgrade.

2 Disconnect existing ELAN 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 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 169 to install the DCHIP connector and MSDL cable.

Upgrade the 8-port ITG basic trunk software to ITG ISL trunk software

You use the MAT ITG Basic Trunk application to perform this procedure. Once you have upgraded to MAT 6.6 or later, all the configuration data for the ITG Trunk node will have been converted.

Step 1 - Remove ITG 1.0 configuration files

In this step, you remove the ITG 1.0 Trunk configuration files from the TABLE, BOOTP and CONFIG directories of every card in the node you are upgrading.

1 From the MAT 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.** MAT 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 Management IP address of Leader 0 on the E-LAN,
- where "yyy.yyy.yyy.yyy" is the Management Gateway (Router) IP address on the E-LAN. If the MAT PC will be connected locally to the LAN, and there is no management LAN gateway, then the Gateway IP address is "0.0.0.0".
- and where "zzz.zzz.zzz.zzz" is the subnet mask for the management IP address of Leader 0 on the E-LAN.

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 management 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, you must 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 *Appendix D*.

3 Press **Enter**.

4 The ITG shell outputs value = 0 = 0 x 0 to indicate successful completion of the **setLeader** command. If the ITG shell outputs **command not found**, check the spelling of the command. If the ITG shell outputs a value of -1, contact Nortel Networks customer technical support.

5 Return to the MAT 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: You enter **clearLeader** command even when you remove configuration files from Follower cards.

Step 2 - Transmit ITG Trunk 2.0 software to the 8-port cards

1 Launch MAT/OTM 1.1. Double-click on **ITG M1 IP Trk** in the Services folder

1 In the **IP Telephony Gateway** window, select Leader 0 from the ITG trunk node you are upgrading.

2 Select menu **Configuration | Synchronize | Transmit**. The ITG-Transmit Options window appears.

3 Make sure to set the radio button to **Transmit to selected nodes**. Check the **Card Software** check box only.

4 Locate the ITG28xx.mms software file on the MAT PC. If you know the path to the ITG28xx.mms software file software, type the path information in the **Software** field. Or click the Browse button to find and select the file and 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.

5 Click the **Start Transmit** button.

Monitor progress in the **Transmit control** window. Confirm that the card software is transmitted successfully to all the 8-port ITG Trunk cards. The window identifies the cards by their TNs.

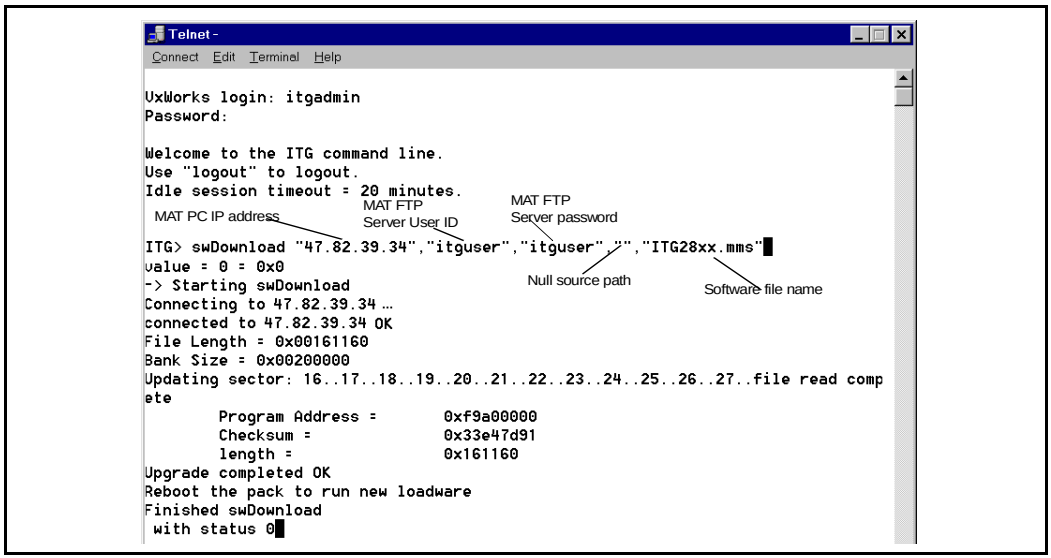
If the message in the control window indicates the software transmit is unsuccessful, do not press Cancel. Leave the Transmit Control window open displaying the location of the software file on MAT.

If you can Telnet to the card from MAT, but MAT shows the card status as Not Responding, MAT ITG SNMP MIB is incompatible with the ITG 8-port software version. In this case, the software upgrade must be executed from the ITG shell CLI of each 8-port card in the node (see step a and Figure 44).

a. ITG> swDownload "IP address of MAT PC","itguser","itguser","","ITG28xx.mms" where xx indicates the latest version of the ITG Trunk 2.0 software for the 8-port card.

Note: Be sure to hit the space bar after you type in swDownload and enter the quotation marks, commas exactly as described in the step above and shown in Figure 44.

Figure 44
Software download example



6 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 reset button if card is showing responding. Close the Card Properties and go on 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> cardReset

c. Press the reset button on the card faceplate.

The card faceplate shows T.20 in the maintenance display window.

7 At this point, the cards have ITG 2.0 ISDN functionality and are in the state of new 8-port cards that need to be configured. Turn to “Configure ITG Trunk data on the Meridian 1” on page 174.

8 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**

9 Configure the ITG Trunk data on the MAT 6.6 ITG ISDN IP Trunk application. See “Configure ITG Trunk data on MAT” on page 191.

10 Transmit configuration data to the upgraded ITG Trunk cards using normal ITG Trunk 2.0 installation procedures.

11 Upgrade Meridian 1 to release 25 software.

Remove ITG 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 MAT ITG ISDN IP Trunks application for ITG trunks or, in LD21, request an LTN of existing basic ITG tie trunk route. The LTN gives you a list of every single unit. You can see 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 you use the G.729 codec, there may only be four units on the card.

b Load LD14 and out the cards one at a time. The way to do this is to say OUT x, where x = 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 you have outed all the trunks on the LTN of your basic ITG trunk TIE route, then you can out the route data block.

2 Out route data block for ITG basic trunks. Load LD16.REQ = OUT. It prompts you for the customer number and route number and hit enter. The route data block is then deleted.

Configure the Meridian 1 ITG ISL Trunk data: upgrade considerations

If you are going to leave the 8-port cards in the same cardslots, use the same card TNs and route number when you build your new ITG ISL Trunk Route.

If you want to re-use the same ESN route list blocks and the ESN translation tables, then you will use the same route number when you build the new ITG ISL TIE route and the RLB entries will still be correct.

You must remember to make certain changes to the RLB entry in LD86. For the ITG ISL TIE Trunk Route, configure SBOC = RRA to enable fallback routing to circuit-switched trunks.

In ITG 2.0, the digit manipulation tables are not required to reinsert AC1 or AC2. Therefore, change the DMIs accordingly.

Verify customer data block (see Table 33, “LD 15 - Configure ISDN feature in customer data block,” on page 178). See “LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Large Systems)” on page 174 or “LD 17 - Configure the ISL D-channel for the ITG DCHIP card (Small Systems)” on page 176, as appropriate.

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 Table 34, “LD 16 - Configure the ITG ISL TIE Trunk route data block,” on page 179

Note: Any references to the ITG trunk route number in ESN route list blocks will still be valid after you are finished.

2 Go to LD14 and add ISL trunks to the new ISL route. See Table 35, “LD 14 - Configure ITG ISL 8- or 24-port trunk cards and units,” on page 182 for complete information.

3 In LD14, at prompt, **REQ**, enter **new 8**.

Note: Do this configuration on a card-by-card basis.

4 At prompt, **XTRK**, specify **itg2.**

5 In LD14, at prompt, **MAXU**, enter **8**.

6 Look at the MAT dialing plan. Go to LD90 and determine which RLBs are used for ITG translations that are used for ITG destinations. Print NPA, Nxx or LOC.

7 In LD86, remove digit manipulation and print out RLBs. Do not use ESN digit manipulation tables for the ITG ISL Trunks.

Note: You need to determine which RLBs are used for the ITG trunks. You need to know which ESN translations are using the ITG RLB.

8 Inspect entries in RLB.

9 Find the entry that refers to ITG basic trunk route.

10 Under those entries, find the DMI and make a note of it.

11 Remove the DMIs that were previously used for ITG basic trunks.

Verify ROM-BIOS version

When you reset the card, the ITG card displays a series of start-up messages on the local TTY. Verify that the ROM-BIOS is 1.1 or greater. If not, contact Nortel Networks technical support.

Upgrade Troubleshooting

This section provides two procedures to correct MAT upgrade problems.

MAT cannot refresh view (Card not responding)

If MAT cannot see card status through refresh, but you can Telnet to the card from MAT, your MAT version is incompatible with the 8-port card software.

How to upgrade software using the ITG shell

Use this procedure if MAT displays a Card status of Not Responding.

1. Prepare the MAT 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 MAT ITG ISDN IP Trunk** application Configuration menu.
3. Check the box for Card Software. Browse for the software image file on the MAT PC. When you find the software image file, open it from the Browser so the path and file name appear in the MAT 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 card.

OA&M using MAT applications

This chapter explains how to perform ITG Trunk 2.0 Operation, Administration and Maintenance (OA&M) tasks using MAT Navigator, Maintenance windows and system terminal passthru, the MAT Alarm Notification application, and MAT ITG ISDN IP Trunks application.

You perform most OA&M tasks from MAT. A few OA&M tasks must be performed through the ITG shell (See “OA&M using the ITG shell CLI and overlays” on page 275.) If MAT is temporarily unavailable, you can perform many OA&M tasks from the ITG shell as an alternative method.

MAT OA&M procedure summary

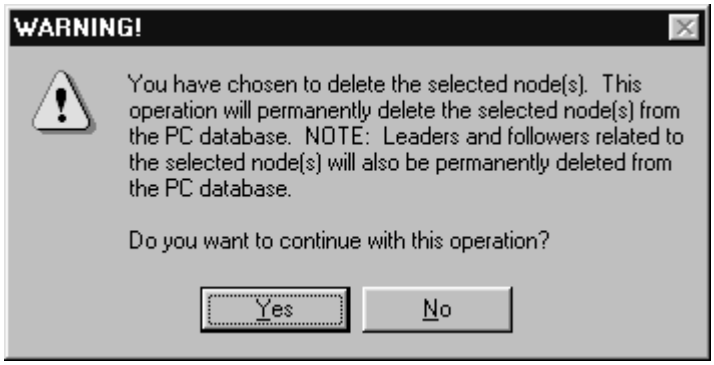
- "Alarm Notification" on page 269

Delete a node

To delete an ITG node, perform the following steps:

1. Double-click the **ITG ISDN IP Trunk** icon from the Services folder in the MAT Navigator window.
2. Right-click on 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 46 appears. Click "Yes" to confirm the deletion of the ITG node. The ITG node and all related ITG cards are deleted.

Figure 45
Delete Node dialog box



To delete a card, perform the following steps:

1. Select the ITG ISDN IP Trunk icon from the Services folder in the MAT Navigator window.
2. Right click on the node and select menu **Node | Properties.**
3. The ITG Node Properties window appears.
4. Select the Card Configuration tab.
5. Select the ITG card to delete from the list.

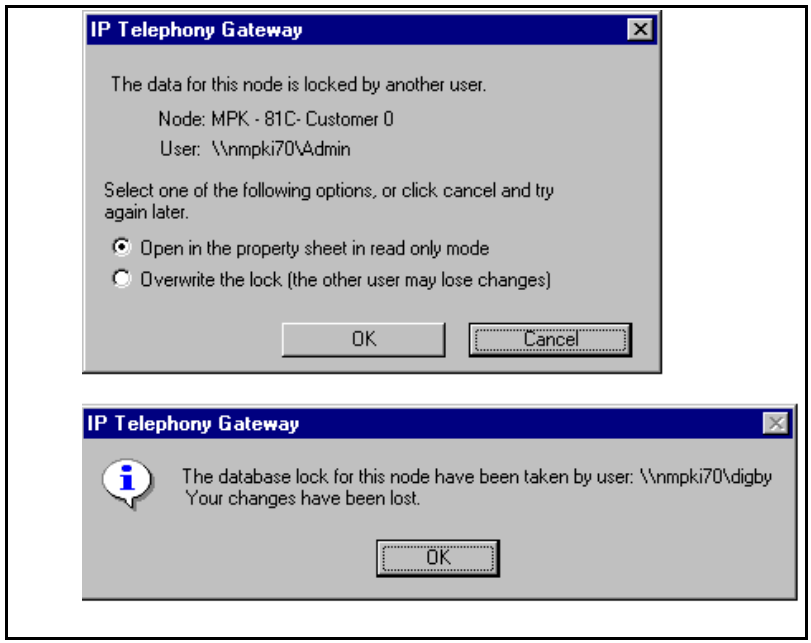
6 Click the “Delete” button.

7 Click “OK”.

Database locking

All node and card properties are stored in a single MAT database. When you open Node or Card Properties, 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 as you, the second user is given the option of overriding the lock. If the second user decides to override the lock and you have made changes and then clicked “OK” or “Apply”, you are provided with a message that says that their changes have been lost (see the second dialog box in Figure 46 on page 249). This message only appears if changes have been made. If you try to open a property sheet in the node after rebooting the PC, the first dialog box in Figure 46 appears. In this example, a property sheet was open when the MAT PC crashed.

Figure 46
Database lock message



ITG Card Properties

To display the property sheet of an ITG card, double click on an ITG card in the ITG Main window.

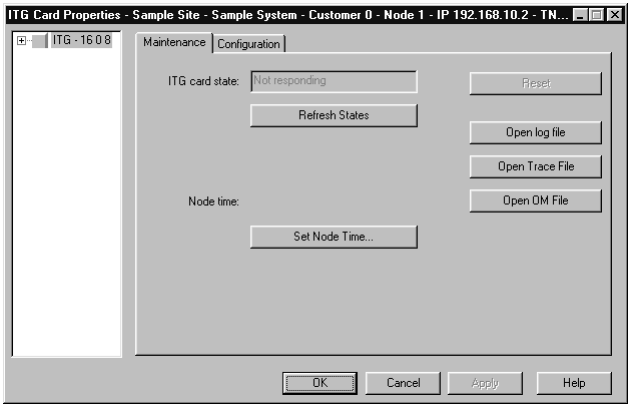
The property sheet has a tree control on the left-hand side of the window. You can control the ITG card or any of the DSPs. Different property sheets appear for ITG cards, DSPs, and D-channels by clicking on the required item in the tree. ITG determines the number of DSPs at run time when the property sheet opens. If the card is not responding, the number of DSPs is unknown and no DSPs are displayed. The D-channel only appears in the tree control 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 you click on these tabs.

ITG Card Properties – Maintenance window

Click on the Maintenance tab to perform maintenance operations (see Figure 47). Click on the appropriate button in the Maintenance window to perform the required operation.

Figure 47
ITG Card Properties-Maintenance tab



The following comments apply to the operations in the ITG Properties Maintenance window:

- To perform Enable, Disable, and Perform operations, use the MAT Maintenance Windows or System Terminal applications.
- The “Reset” button is disabled when the ITG 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 “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 (must turn trace turn 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. MAT sets the Leader card’s time. The Leader sets the time on all other cards.

Set date and time for the ITG ISL Trunk node

Set the date and time on the ITG ISL Trunk 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.

1 Select the ITG ISL Trunk node for which you want to set time and date from the list in the upper part of the window.

2 Double-click on Leader 0 from the list in the lower part of the window.

The ITG Card Properties Maintenance tab appears.

3 Click on the **Set Node Time** button. The Set Node Time dialog box appears.

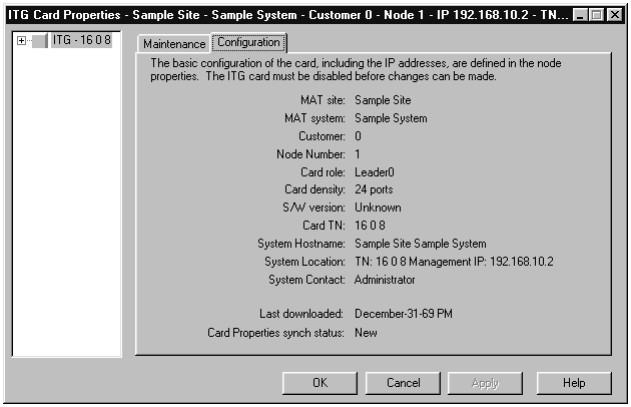
4 Set the correct date and time.

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.

ITG Card Properties – Configuration window

The Configuration window for the ITG card contains the information shown in Figure 48. 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 48
ITG Card Properties Configuration tab



Note: For more information about maintenance commands, see “Maintenance” on page 295.

DSP maintenance window

Note: If the ITG card is not responding, no DSP icons appear in the tree on the left-hand side of the ITG Card Properties window.

Click on 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 on the Self Test button to perform a self test on the DSP. The command is sent to the ITG 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 ITG card has D-channel hardware, the tree on the left hand side of the window contains the D-channel. Click on the D-channel and the D-channel Maintenance window appears. This window allows you to perform D-channel maintenance operations. The commands are sent to the card through SNMP.

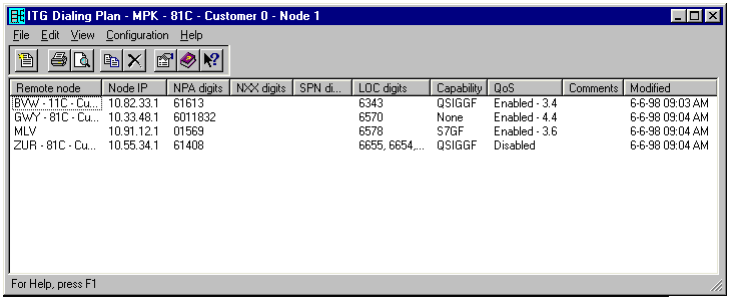
Note: The menu items are not context-sensitive. For example, you can try to enable an enabled D-channel.

Add Dialing Plan entries

The dialing plan provides translation between the dialed digits and the IP address of the remote ITG node. Right click on any card in the node and select menu **Node | Node Dialing Plan**. The ITG Dialing Plan window appears (see Figure 49).

There is one dialing plan for each ITG node in the network; it is transmitted to each card. When the dialing plan is changed, dial plan synchronization status is set to “Changed” for each card in the node. The card does not have to be disabled.

Figure 49
Dialing Plan - Remote Node view



You can view the dialing plan data sorted by digits dialed. select menu **View | Digits Dialed**. To return to the remote node view, select menu **View | Remote Nodes**.

The following comments apply to the ITG Dialing Plan windows:

- The Node name is derived from the Node Properties if the node is defined on this MAT PC. If not, the Node name entered in the property sheet is displayed.
- If there are many digit strings in a column, the first five appear in the list followed by dots. To see all strings, you must open the property sheet.
- The Quality of Service column has the following two parts:

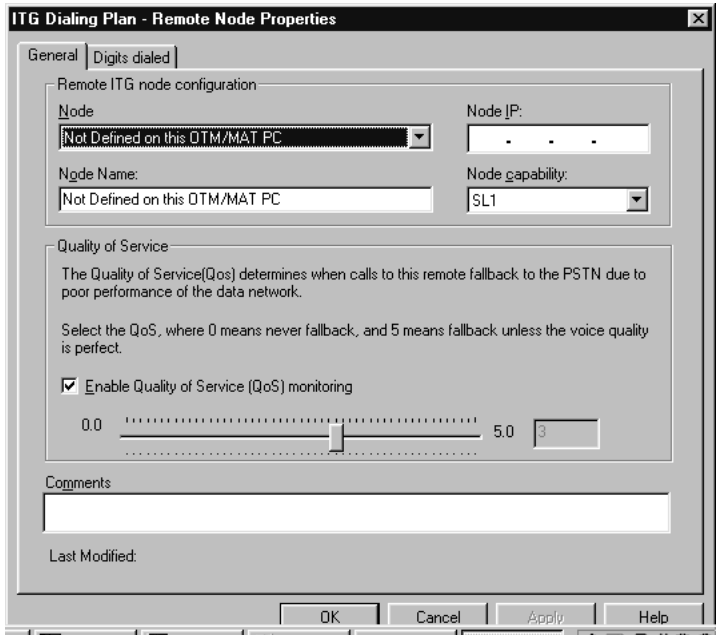
— Enable / Disable status

— QoS value

Dialing Plan Entry Properties – General window

In the ITG Dialing Plan window select menu **Configuration | Add**. The property sheet shown in Figure 50 appears. Use this property sheet to add or change an entry in the dialing plan.

Figure 50
ITG Dialing Plan – Remote Node Properties General window



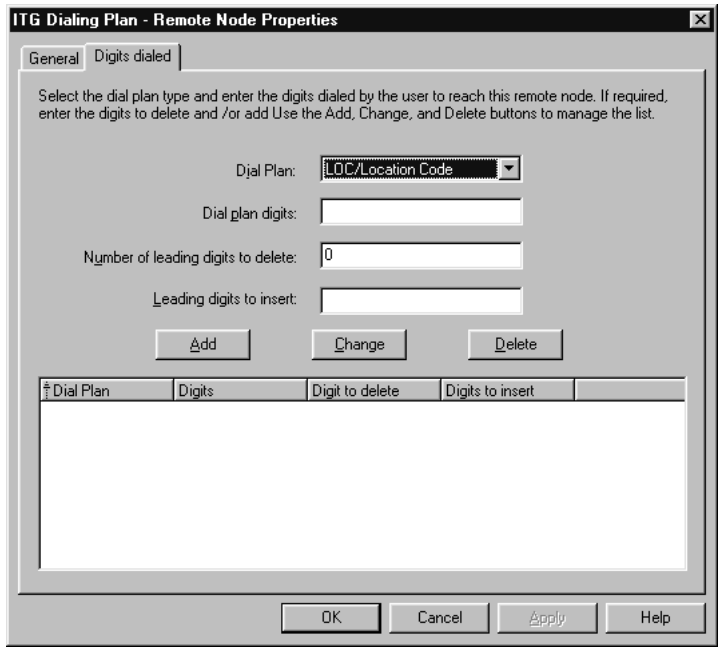
The following comments apply to the fields in the ITG Dialing Plan – Remote Node Properties General window:

- The list of nodes in the Node drop list is derived from the list of nodes in the Main ITG window. When you select a node, the Node IP address is inserted as read only. If you change a Node IP address through the Node Properties, the address is automatically updated in the dialing plans. You must, however, transmit the dialing plan to each ITG card for the change to begin. When you select “Not defined on this MAT PC”, the Node IP edit box is empty, and you must define the Node IP. When you delete the node in the Main ITG window, the node is set to “Not defined on this PC” and the IP address is not changed.
- The Node name is optional, unless you select the “Not defined on this PC” option. If you select this option, you must enter the Node name.
- The Node capability drop-down list contains H.323 V2, ESGF, FTUP, V1UP, and V2UP. The default is H.323 V2.
- The Quality of Service is a slider bar and read-only edit box with spin buttons. You can use either control. Changes in the slider are dynamically reflected in the edit box. These controls are disabled if the QoS monitoring option is not checked.

Dialing Plan Entry Properties – Digits Dialed window

Click on the “Digits dialed” tab. In this window, define the digit sequence(s) for dialing remote nodes (see Figure 51).

Figure 51
ITG Dialing Plan - Remote Node Properties window - Digits Dialed tab



The following comments apply to the "ITG Dialing Plan – Remote Node Properties Digits dialed" window:

- The standard copy, cut and paste functions are available through keyboard shortcuts or a menu.
- There is a maximum of 20 digits in a string.
- The NXX and LOC digit strings must be "leftwise distinct" within its user dialing plan type (NXX or LOC) across all remote nodes in this node dialing plan. The SPN and NPA must be distinct across all remote nodes in this node dialing plan. For example, 011 and 0112 are not leftwise distinct; 011 and 012 are leftwise distinct.
- The maximum number of strings is limited only by hard disk space.
- Scroll bars appear if necessary.
- 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 41 shows the mapping between the NPI / TON fields and the resulting ITG dialing plan tables which are searched.

Table 41
Mapping of dialing plan with TON and NPI

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

Table 41
Mapping of dialing plan with TON and NPI

NPI	TON	Dialing Plan
Private	CDP	DSC TSC
Private	Unknown	SPN DSC TSC LOC
Unknown	Unknown	SPN DSC TSC LOC

Transmit configuration data

MAT converts the ITG node and card configuration data to text files, and transmits the files to the ITG cards using FTP. The text files are the following:

- Node properties: **bootptab.txt** (only transmitted to the Active Leader)
- Dialing plan: **dialplan** (transmitted to every card)
- Card properties: **CONFIG.INI** (transmitted to every card)

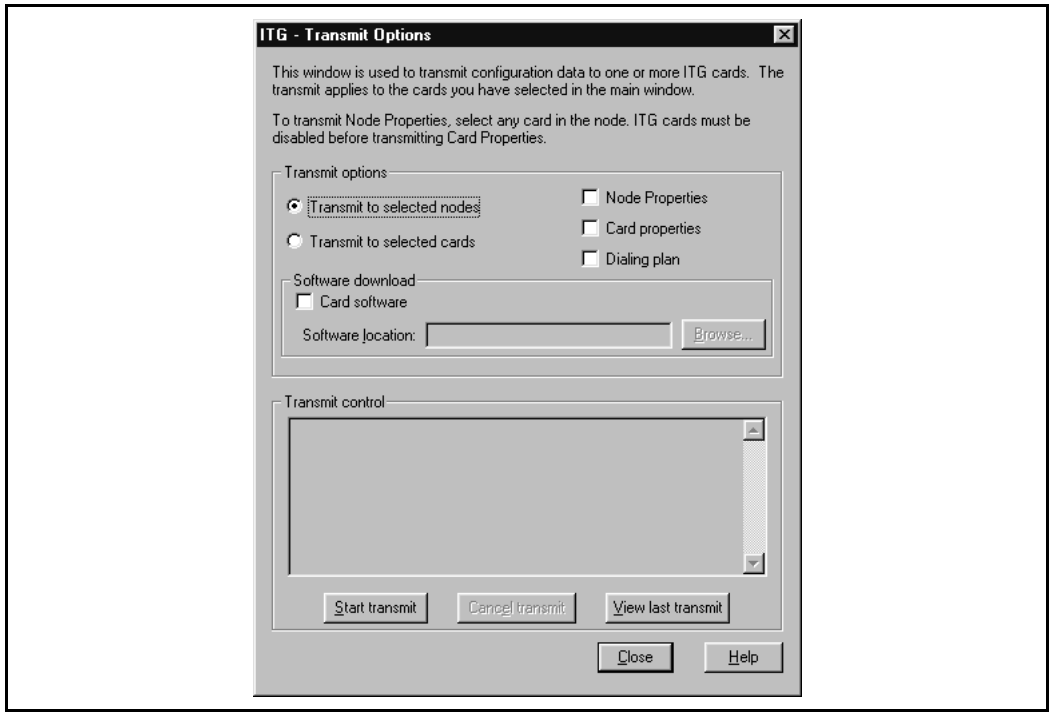
The bootp table is downloaded to the Leader card and copied to the Backup Leader. All other ITG cards in the node use bootp to retrieve their bootup data from this table. MAT downloads the config.ini file to each card. It also downloads the dialplan file to each card.

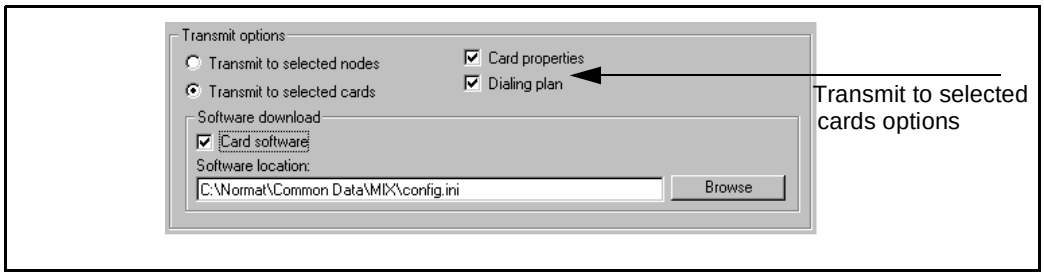
The ITG Main window displays the synchronization status of each of these fields. Changes to the first two tabs (General and Card Configuration) in the Node Properties sheet affect the Node Synchronization Status. Changes to the other tabs (DSP Profile, SNMP Trap / Routing table IPs, Accounting Server, and Security) in the Node Properties sheet affect the Card Synchronization Status. You must transmit these changes 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 52). This window allows you to transmit multiple files to one or more ITG cards.

To transmit configuration data, select cards in the ITG Main window, select a transmit option, and click on "Start transmit". MAT transfers the data to the appropriate cards using FTP.

Figure 52
ITG Transmit Options window





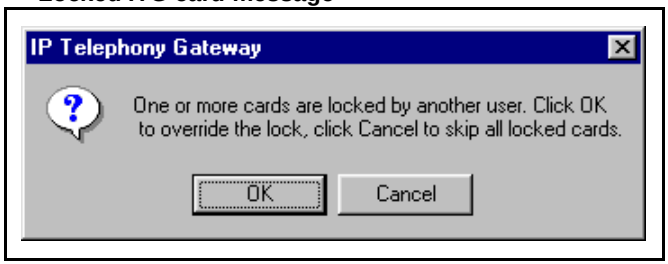
The following comments apply to the ITG Transmit Options window:

- To transmit Node properties, select any card in the node.
- You must disable ITG cards before transmitting Card Properties.
- You can enable while transmitting all other data. However, you must reset the card before the new card software begins working.
- To transmit to selected nodes, you must select one card in each node.
- Transmit control shows the status of the operation and any errors which occur (for example, if a card is not responding).
- The “Cancel transmit” button is disabled until you begin a transmission. When a transmission begins, the “Close” button is disabled. You must cancel the active transmission before the window can close.
- The “View last transmit” button displays the results of the last transmission in the list box. When a transmission is started, the list clears and the “View last transmit” button is disabled.
- If there are no cards selected, the Synchronization menus are disabled.
- Transmission of card properties fails if the card is not disabled.

When transmitting to an ITG card which is locked by another user, the second user is provided with the option to override the lock (see Figure 53). 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 53
Locked ITG card message



Add an ITG ISL Trunk node on MAT by retrieving an existing node

After you have manually configured and installed an ITG node, you can add that node to another MAT PC by retrieving the configuration data from the existing ITG node.

You can use this **optional** procedure:

- to combine existing ITG ISL Trunk nodes on the network that were originally configured from different MAT PCs onto one MAT PC to manage the ITG ISL Trunk network from a single point of view.
- to restore the ITG ISL Trunk configuration database to a MAT PC whose hard drive had failed. (You can also restore the MAT ITG nodes from the MAT Disaster Recovery Backup.)
- to temporarily create a copy of the ITG ISL Trunk node configuration on for maintenance and diagnostic purposes. For example, you can create a copy of an ITG ISL Trunk node database on a MAT PC located at a remote technical support center.

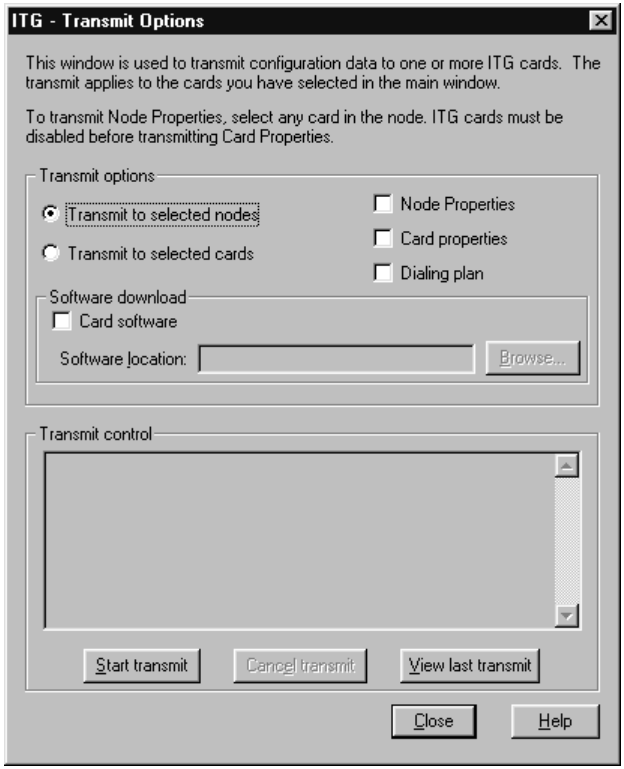
The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the MAT Navigator before you can add a new ITG node. Multiple ITG ISL trunk nodes can be added in the MAT ITG ISDN IP Trunks application per Meridian 1 customer.

> ***Note:*** If you use multiple MAT PCs to manage the same ITG network, and the PCs are not using file-sharing, caution must be taken to synchronize the different copies of the ITG database. You can use the MAT ITG menu **Configuration | Synchronize | Retrieve** function to synchronize the MAT ITG database with the ITG node's database.

Retrieve and add an ITG ISL Trunk 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 menu **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.

Figure 54
Retrieve ITG node window



4 In the **Retrieve ITG node** window, select the **MAT Site**, and **Meridian 1 System** fields. Select the **Meridian 1 Customer** number.

Note: The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the MAT Navigator before you can add a new ITG node.

5 Enter the management IP address field for Leader 0 or Leader 1 on the existing node.

6 Enter the SNMP read/write community name. The default is “private”.

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 from the View menu, and check that the cards in the new node are responding.

Retrieve and add an ITG ISL Trunk Node for maintenance and diagnostic purposes

Use this procedure to create a “dummy” ITG node for retrieving and viewing the real ITG node configuration, without over - writing the existing ITG configuration data for an existing node in the MAT ITG database. Retrieving the real ITG node configuration to the “dummy” node is useful in the following cases:

- Isolating ITG node configuration faults
- Determining which copy of the database is correct, so that you can determine the required direction of database synchronization:
  - transmit MAT ITG to ITG node, or
  - retrieve ITG node to MAT ITG node.

You can add the dummy node manually or by retrieving the ITG node configuration data from an existing node.

The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the MAT Navigator before you can add a new ITG node.

The following is the recommended method to create the “dummy” ITG node.

1. In MAT 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.

When you need to view the data of a real ITG node, select the “dummy” node and change the management 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, you retrieve the card properties and dialing plan from each card in the selected nodes. MAT compares the retrieved data with the card properties and dialing plan currently stored in the MAT database. MAT 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 card properties or dialing plan from the selected card. Double-click on the temporary node to view the 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 node in MAT.

Retrieve ITG configuration information from the ITG node

You can use this optional procedure when you:

- add an ITG node on MAT by retrieving an existing node
- know that the ITG node configuration on the ITG card is different from the MAT ITG database (e.g., during maintenance and fault isolation procedures).
- have multiple MAT PCs with multiple instances of the database (administration).

Use the MAT ITG menu **Configuration | Synchronize | Retrieve** command to retrieve the ITG configuration information from the ITG node.

1. Launch MAT 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 ITG configuration data that you need to retrieve:

   Note 1: Select **Node Properties**, **Card Properties**, and **Dialing Plan** if the MAT ITG data is out of date and you intend to synchronize all MAT ITG node data with the data from the ITG cards on the node.

   Note 2: Select **Card Properties** to add a node on MAT 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 you are attempting to isolate a problem on a particular card. Use the “dummy” node for this purpose.

5. Select **Prompt user for community name** if required.
6. Click the **Start retrieve** button.

Monitor the status of the retrieval in the **Retrieve control** box. The retrieved **Node Properties**, **Card Properties**, and **Dialing Plan** will over-write the existing MAT ITG configuration data for the respective node or card.

When you retrieve a dialing plan table, MAT ITG compares it against the existing node dialing plan and discards it if it is identical. If it is different, you are asked to confirm before it over-writes the existing node dialing plan on MAT ITG.

The “Retrieving the ITG configuration information from the ITG node” procedure is complete.

Schedule and generate and view ITG OM reports

Operational Measurement (OM) reports are a collection of OM data from all ITG cards defined on the MAT PC or server. You can generate a report on request or schedule the report to generate at a selected time. Each time a report is generated, the application retrieves the latest OM data from each ITG card defined in MAT. This data is then added to a comma separated file on the MAT 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).

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 55).
- **b** To generate a report immediately, click Generate OM Report now to prepare a report immediately. MAT 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 . Fill in the fields to schedule the report and define the times and information. Schedule report generation at least one time a day. Click OK.

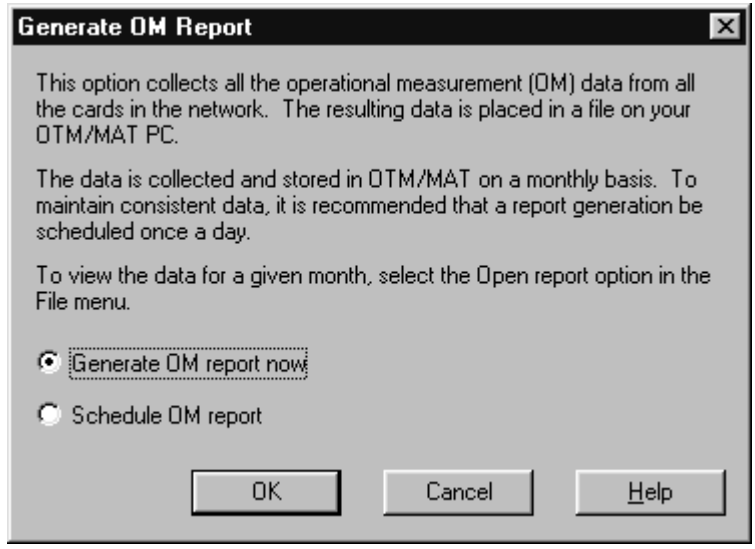
2 To open and view a report:

- **a** Select File | Report | Open. The Open OM Report dialog box appears.
- **b** Double-click on an OM report. The report appears in Microsoft Excel. If you do not have Excel, use an application that recognizes .csv (comma-separated) files to view the report.

Backup and restore operations

The ITG card supports backup and restore procedures for critical configuration data. If you replace a failed ITG card with a spare, the dialing plan tables, DSP configuration, passwords, and other configuration data will be restored from the MAT PC.

Figure 55
Generate OM Report



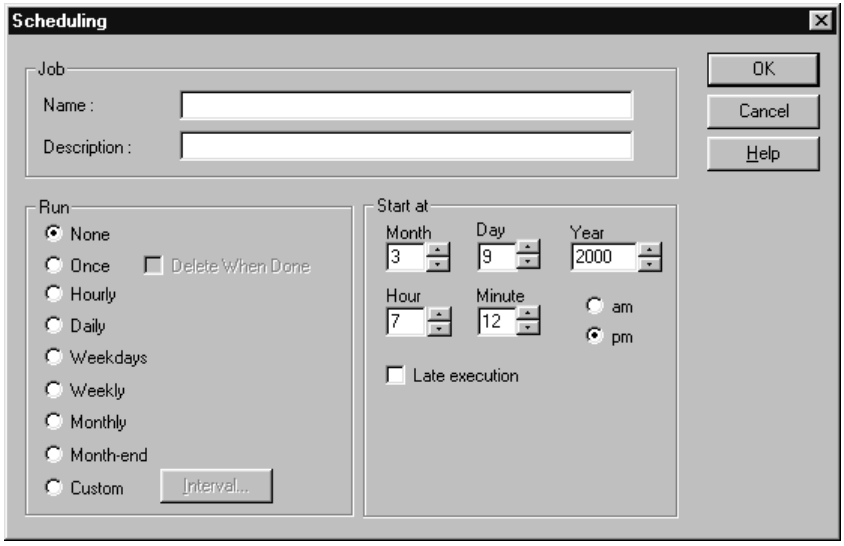
The Meridian Administration Tools (MAT) application has a backup and restore procedure for all data downloaded to and from the ITG card. If MAT is not available, you can use the ITG shell command line interface to retrieve the configuration files from an FTP server or from a PC card.

ITG data is stored in an Access database file on the MAT PC or server, or in the OM files. These files are only backed up when you select the “Disaster recovery” option. This option backs up all MAT data and can only be used to restore all data.

Alarm Notification

The ITG uses the MAT Alarm Notification application. This application receives SNMP traps from any device connected to the network. When received, traps appear in an event browser. You can write scripts to generate notification messages to pagers, e-mail, and SNMP network management systems. You must configure the ITG card to send SNMP traps to the MAT PC and the local modem router on the E - LAN.

Figure 56
OM Report scheduling window



Note: For more information about Alarm Notification, please refer to the *MAT Alarm and Event Management User Guide*.

Meridian 1 system commands - LD 32

You can perform the following Meridian 1 system administration commands:

- "Disable the indicated ITG card" on page 272.

  Note 1: The ITG card must be disabled before card properties can be transmitted from the MAT ITG application to the card.

  Note 2: The card reset button is only available in the MAT ITG application when the card is disabled.

  Note 3: Disabling the ITG card in overlay 32 does not disable the active leader or backup leader functions.

- "Disable the indicated ITG card when idle" on page 273.

Note: This will temporarily prevent the ITG node from seizing the port from incoming calls.

- "Disable an indicated ITG port" on page 273.
- "Enable an indicated ITG card" on page 273.
- "Enable an indicated ITG port" on page 273.
- "Display ITG card ID information" on page 274.

  Note 1: This command displays the PEC (Product Engineering Code) for the card. The ITG PEC is NT0961AA.

  Note 2: The ITG card information displays the same ITG card serial number that is displayed from the ITG shell using the **serialNumShow**.

- "Display ITG card status" on page 274.
- "Display ITG card port status" on page 274.

A summary list of ITG Meridian 1 system commands is shown in Table 42 on page 271.

Table 42 shows a summary of the Meridian 1 system administration commands available in overlay 32.

Table 42
Overlay 32 - ITG 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: you should use the DISI command to disable the ITG card instead of the DISC command. The disablement of the ITG card is indicated by the NPR011 message.

Table 42
Overlay 32 - ITG maintenance commands

Command	Function
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
STAT l s c	Print the Meridian 1 software status of the indicated card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 software status of the indicated unit, where: l = loop, s = shelf, c = card, u = unit

Disable the indicated ITG card

To disable the indicated ITG card in LD 32, use the following command:

DISC l s c	Disable the indicated ITG card, where: l = loop, s = shelf, c = card

Disable the indicated ITG card when idle

To disable the indicated ITG card when idle in LD 32, use the following command:

DISI l s c	Disable the indicated ITG card when idle, where: l = loop, s = shelf, c = card

Disable an indicated ITG port

To disable a indicated ITG 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 ITG card

To enable a indicated ITG card in LD 32, use the following command:

ENLC l s c	Enable the indicated ITG card, where: l = loop, s = shelf, c = card

Enable an indicated ITG port

To enable a indicated ITG 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 ITG card ID information

To display the ITG card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the ITG card, where: l = loop, s = shelf, c = card

Display ITG card status

To display the status of a indicated ITG card in LD 32, use the following command:

STAT l s c	Display the status of the indicated ITG card, where: l = loop, s = shelf, c = card

Display ITG card port status

To display the status of a port on the ITG 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

This chapter explains how to perform ITG Trunk 2.0 Operation, Administration and Maintenance (OA&M) tasks using the ITG shell Command Line Interface (CLI). You access the ITG shell directly through a serial port connection, or remotely through Telnet from the MAT PC or any Telnet client host.

ITG Shell OA&M procedure summary

You can perform the following OA&M tasks from the ITG shell:

- "IP configuration commands" on page 288.
- "Download the ITG error log" on page 289.

Access the ITG shell through a maintenance port or Telnet

You can access the ITG shell administration and maintenance commands in two ways:

You can log in through a direct cable connection between the ITG faceplate maintenance port and the MAT PC.

You can access the ITG shell from the MAT PC. Refer to "Telnet to an ITG card through the MAT PC" on page 277 for details.

Connect a PC to card maintenance port

1 To access the ITG shell, connect a PC to the RS232 serial maintenance port through DIN-8 connector on the faceplate of the ITG Leader 0 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 MAT PC.

Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB - 9 connector of the NTCW84KA E-LAN, T-LAN, DCH, and Maintenance Port cable (for DCHIP cards), or the NTMF94EA E-LAN, T-LAN, Maintenance Port cable (for non-DCHIP cards, to create a more permanent connection to the ITG Trunk card serial maintenance port.

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**

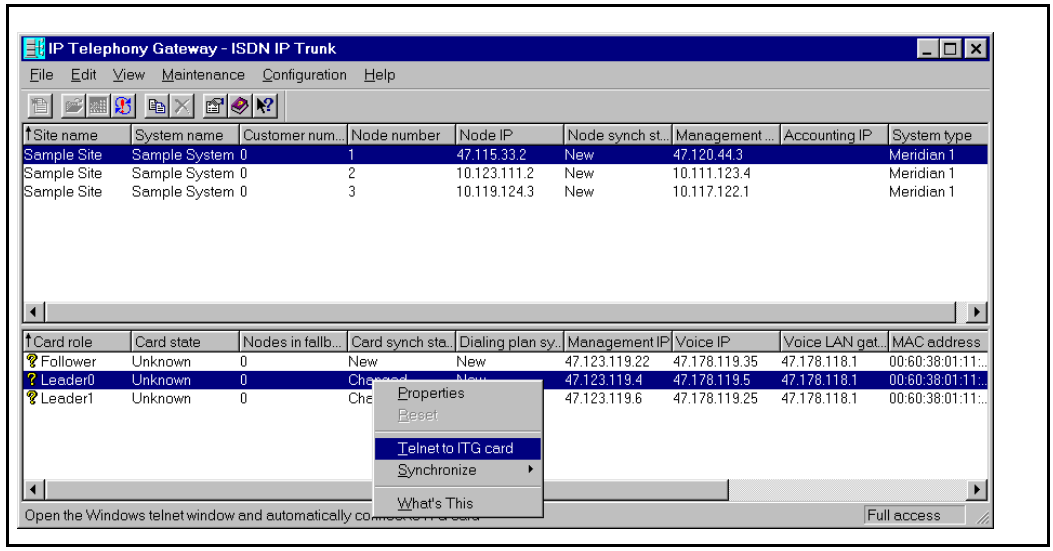
ITG>

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 ITG card through the MAT PC

1. In the "MAT 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 57). The PC opens a Telnet window and automatically connects to the ITG card by using the card management IP address.

Figure 57
Select card and open Telnet session



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.

4 You can increase the Telnet terminal buffer size to capture multiple screens of data from the ITG card:

From the Telnet “Terminal” menu, select “Preferences”. Set the Buffer Size to a larger value, e.g. 1000, and click “OK”. You will have to set the Telnet buffer size only on occasion, because Telnet preferences are automatically saved.

5 To prevent the loss of diagnostic data from the ITG card if the Telnet session terminates unexpectedly, you must enable logging of Telnet sessions on your MAT PC:

From the Telnet “Terminal” menu, select “Start Logging”, and use the “Browse” dialog to indicate the appropriate folder and file name for Telnet log file for the current Telnet session. You can open the Telnet log file using a text editor, such as Windows 9x Notepad, or a word processor for large log files.

Change the default ITG shell password to maintain access security

You must schedule routine changes of user names and passwords to maintain access security. The ITG user name and password protects maintenance port, FTP, and Telnet access to the ITG card over the LAN.

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 ITG card file system. The default user name is **itgadmin** and the default password is **itgadmin**.

You will be prompted for the current user name:

Enter current username: **itgadmin**
Enter current password: **itgadmin**
Enter new username: **newname**
Enter new password: **newpwd**
Enter new password again to confirm: **newpwd**

If the complete sequence of commands is correctly entered, you get the system response with 'value = 0 = 0x0'. The new user name and password are now stored in the non-volatile RAM on the ITG card, and will be retained when the card is reset, powered off, or on.

Reset the default ITG shell password

If you lose the ITG shell password, you can reset the ITG shell user name and password to the default: itgadmin. This procedure requires physical access to the ITG card. You cannot perform this procedure through Telnet.

1 Connect a terminal to the ITG card maintenance port.

2 Press the reset button on the ITG card observe the sequence of start up messages from the card.

3 Look for the prompt to enter the BIOS ROM. You have approximately 2-3 seconds to enter xxx when this prompt appears. If you see the prompt "vxWorks login:" you have lost the BIOS ROM prompt, and you must reset the card 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.

4 Press the reset button on the card again.

The ITG Trunk card starts up and displays "T:20" on the 4-character display, the ITG card will begin sending bootp requests on the E-LAN. 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 management interface on Leader 0,
- where "yyy.yyy.yyy.yyy" is the Gateway IP address for the management interface on Leader 0. If the MAT ITG PC will be connected directly to the LAN, and there is no management LAN gateway, then the Gateway IP address is "0.0.0.0".
- and where "zzz.zzz.zzz.zzz" is the subnet mask for the management 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 278.

8 Configure all the ITG cards in the same node with the same password. Repeat this procedure for other cards in the node.

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 MAT PC to the ITG card:

ITG>**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, enter the following command to display the number of DSPs on the ITG card: **DSPNumShow**

Display ITG Node Properties

ITG> enter the following command to display information about an ITG node: **IPInfoShow**

The following ITG node information appears on the TTY:

- IP addresses for the management and voice subnets
- default router for the management and voice subnets
- subnet mask for the management and voice subnets
- SNMP manager

Enter the following command to display information about an ITG card: **itgCardShow**

The following commands give additional information about an ITG card:

- ldrResTableShow
- ifShow
- dongleIDShow
- serialNumShow
- firmwareVersionShow
- swVersionShow
- emodelSim

Transfer files through the command line interface

Perform one of the following commands at the ITG shell command line to:

- transfer a file from the ITG card to an FTP host, or
- transfer a file from an FTP host to the ITG card

The correct command depends on the type of file being transferred.

These commands are from the point of view of the ITG card. Commands with "Get" as part of the command name refer to file transfer from the FTP host to the ITG card. Commands with "Put" as part of the command name refer to file transfer from the ITG card to the FTP host:

For security reasons, there is no generic FTP client on the ITG card. You cannot perform a DIR or PWD (print working directory) command on the FTP host.

The "bootptab.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 MAT ITG dialing plan information. The "config1.ini" file (transferred by the "configFileGet" command) contains card properties and SNMP information. The "bootptab.1" file only goes to the active Leader card, while the "dptable.1" and "config1.ini" files go to every ITG card.

Software update and file transfer commands

These commands are separated into different categories as described below.

These commands are case-sensitive. The parameters following the command must each be enclosed in quotation marks. There must be a comma and no spaces between the parameters.

Refer to the *Maintenance* section 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 ITG card, or another ITG card in the same node.

Software upgrade

Use this command in the procedure “Transmit new software to ITG Trunk cards” on page 227.

- swDownload *"hostname","username","password", "directory path","filename"*

Generic file transfer:

Use these commands 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 ITG 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 ITG card. To avoid damaging the configuration files and ITG card, only use the ’hostFileGet’ command under the direction of Nortel Networks 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 means, the MAT ITG 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 MAT 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 ITG card software from the command line interface

Use this procedure when the preferred method, described in “Transmit new software to ITG Trunk cards” on page 227, is not available.

> ***Note:*** If the MAT PC is remotely connected to the ITG node through PPP link through the dialup modem router, then use this procedure to upgrade the ITG card from an FTP host. This makes sure that the software file is transmitted intact before it is copied to the flash ROM device.

This procedure updates the ITG card software with the binary file received from an FTP host or ITG card with IP address *hostname*. The ITG card FTP client performs a get which downloads the file to the ITG flash device. A

checksum is calculated to check correct delivery. When the new software version is correctly downloaded, you must reboot the ITG card with cardReset to run the new software.

1 Download the MAT ITG software from the World Wide Web (WWW) to a PC hard drive. Open a browser on a PC and connect to WWW address: **http://www.nortelnetworks.com/itg**

When connected to the site, enter the user name and password.

The default user name is **usa**

The default password is **usa**

2 Select the latest recommended software version and select the location on the MAT ITG PC hard drive where it is to be downloaded. Record the MAT ITG PC hard drive location for use later in the procedure.

Alternatively, you can order the latest ITG software on a PC card.

Upgrade ITG card software by PC card

The PC card can be received from Nortel Networks containing the latest ITG card software version. You can update the ITG card software version on the PC card by copying the file from your PC hard disk to the PC card, which is inserted in a PCMCIA slot on your PC.

1 Insert the PC card containing the software into the A: drive of the ITG card, located on the faceplate of the card.

2 From the ITG shell, monitor the successful insertion of the PC card. There will be a message that indicates that the card has been successful recognized and installed.

3 Use the **swDownload** command to copy the software from the PC card to the ITG card flash ROM device, using the FTP client and the FTP host on the card. The host name parameter in this command is the management interface IP address of the ITG card. The user name and password are the same as 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, you must reboot the ITG card to use it. Use the cardReset command or press the reset button on the card faceplate.

Upgrade ITG card software via an FTP host

1 The latest ITG card software, which was obtained from the Nortel Networks web page, must be made available to an FTP host. This can be an FTP host on the PC. As a special case, the FTP host can be the ITG card.

Alternatively, you can use an FTP client running on the PC to put the ITG card software file on an ITG host available by the ITG card on the network.

For example, any ITG card on the same node can serve as the FTP host. The file can be put onto the C: drive of the ITG card serving as the FTP host.

2 Use the **swDownload** command to copy the software from the PC card to the ITG 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 ITG 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 ITG 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, you must reboot the ITG card to use it. Use the cardReset command or press the reset button on the card faceplate.

Backup and restore from the ITG command line interface

This procedure can be used when the preferred method, using the MAT ITG PC, is not available. This whole procedure must be performed when a configuration file has been changed.

You must first use the ‘Put’ commands to back up the ITG card configuration files. You can later restore the files using the ’Get’ commands.

However, you can use the "DPAddrTGet" file to restore the Dialing Plan file from another ITG card in the same node.

Backup from the ITG command line interface

1. Identify an appropriate FTP host and get 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 ITG card of the ITG 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 ITG 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.

Restore from the ITG command line interface

To restore configuration when the MAT ITG PC is not available to retransmit the ITG configuration data, use the appropriate ’Put’ commands:

1. Use the **BootPFileGet** command with the appropriate parameters, to restore the Node Properties file from the FTP host to the ITG card.
2. Login to the ITG shell for each 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 ITG card in the node that has a valid copy of the Dialing Plan, to each card. Each card requires a valid copy of the Dialing Plan.

3 Log in to the ITG shell for each card that requires a Card Properties restore and use the **configFilePut** command with the appropriate parameters, to restore the card properties files.

Note that the keycode for each card is located in the specific card properties file. Card properties files are not interchangeable.

Recover the SNMP community names

Use this procedure when MAT ITG cannot display the updated status or to transmit or retrieve data to or from an ITG card because of an invalid community name in MAT ITG. This procedure can be used if the MAT PC has crashed, and had to be restored from scratch.

The SNMP community names can be read from the ITG card in two ways:

- Reset the card and monitor the start up messages.
- Use the configFilePut command to backup the Card Properties file to an FTP host and subsequently use a text editor to open the Card Properties file and read the community name.

  Alternatively, use the SNMP client on the MAT PC to connect to the FTP host on the ITG card and 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 configuration commands

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.

- setLeader

Enter this command to clear the leader information in NVRAM and set the boot method to use bootp, making the card a follower:

- clearLeader

Enter this command to print the values of the IP parameters that exist in NVRAM.

- NVRIPShow

Download the ITG error log

The ITG 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 ITG error log:

- currLogFilePut
- prevLogFilePut

Meridian 1 system commands - LD 32

You can perform the following Meridian 1 system administration commands:

- "Disable the indicated ITG card" on page 291.

  Note 1: The ITG card must be disabled before card properties can be transmitted from the MAT ITG application to the card.

  Note 2: The card reset button is only available in the MAT ITG application when the card is disabled.

  Note 3: Disabling the ITG card in overlay 32 does not disable the active leader or backup leader functions.

- "Disable the indicated ITG card when idle" on page 291.

  Note: This will temporarily prevent the ITG node from seizing the port from incoming calls.

- "Disable an indicated ITG port" on page 291.
- "Enable an indicated ITG card" on page 292.
- "Enable an indicated ITG port" on page 292.
- "Display ITG card ID information" on page 292.

  Note 1: This command displays the PEC (Product Engineering Code) for the card. The ITG PEC is NT0961AA.

  Note 2: The ITG card information displays the same ITG card serial number that is displayed from the ITG shell using the **serialNumShow**.

- "Display ITG card status" on page 292.

- "Display ITG card port status" on page 293.

Table 43 shows a summary of the Meridian 1 system administration commands available in overlay 32.

Table 43
Overlay 32 - ITG 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: you should use the DISI command to disable the ITG card instead of the DISC command. The disablement of the ITG 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 43
Overlay 32 - ITG maintenance commands

Command	Function
STAT l s c	Print the Meridian 1 software status of the indicated card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 software status of the indicated unit, where: l = loop, s = shelf, c = card, u = unit

Disable the indicated ITG card

To disable the indicated ITG card in LD 32, use the following command:

DISC l s c	Disable the indicated ITG card, where: l = loop, s = shelf, c = card

Disable the indicated ITG card when idle

To disable the indicated ITG card when idle in LD 32, use the following command:

DISI l s c	Disable the indicated ITG card when idle, where: l = loop, s = shelf, c = card

Disable an indicated ITG port

To disable a indicated ITG 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 ITG card

To enable a indicated ITG card in LD 32, use the following command:

ENLC l s c	Enable the indicated ITG card, where: l = loop, s = shelf, c = card

Enable an indicated ITG port

To enable a indicated ITG 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 ITG card ID information

To display the ITG card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the ITG card, where: l = loop, s = shelf, c = card

Display ITG card status

To display the status of a indicated ITG card in LD 32, use the following command:

STAT l s c	Display the status of the indicated ITG card, where: l = loop, s = shelf, c = card

Display ITG card port status

To display the status of a port on the ITG 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.

Maintenance

This chapter describes the maintenance, debug, and software upgrade procedures available for the ITG card.

This chapter includes the following sections:

- **ITG Trunk 2.0 faceplate maintenance display codes** – provides a list of the Maintenance codes displayed to the technician on the diagnostic status of the ITG card.
- **System level maintenance** – shows how to maintain the ITG card using Meridian 1 overlays, or a MAT PC.
- **ITG shell command set** – shows how to maintain the ITG card using the ITG's card command line interface.
- **ITG card self-tests** – describes how to perform diagnostic tests on the ITG card to check correct operation.
- **Upgrades** – explains the different upgrade options available for the ITG application.
- **Replace an ITG card** – provides step-by-step procedures for replacing an ITG card
- **Backup and restore procedures** – shows how to backup the application data.
- **Fault clearance procedures** – describes potential system faults and how to correct them.

ITG Trunk 2.0 alarms

This section describes the alarms, messages and codes output by the ITG Trunk 2.0 card. All ITG Trunk 2.0 alarms shown in Table 44 on page 297 can be emitted as SNMP traps. SNMP is the method ITG Trunk 2.0 uses to send alarms to an alarm monitoring center.

ITG 2.0 displays and logs alarm information in the following ways:

1 Displayed on the ITG card console through the ITG shell in a Telnet session or on a terminal connected to the local maintenance port.

2 Logged in the error log files on the /C: drive of the ITG card.

3 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” correspond to last three digits of the alarm ITG04xx listed in Table 44.

4 You can access the current error log file through MAT ITG card properties by clicking on the “Open Log File” button on the “Maintenance” tab of ITG card properties.

If enabled in MAT ITG Node Properties **SNMP Trap/Routing table IPs** tab, SNMP sends appropriate traps to MAT Alarm Management or another specific SNMP manager when an error or event occurs. The ITG Trunk card also puts the system error message into the error log file on the /C: drive of the ITG 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 ITG 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 44 on page 297 lists ITG SNMP alarms by severity.

Table 44
ITG Trunk 2.0 alarms (Part 1 of 6)

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 other than a known power-on event or a user-invoked card reset, the causes of recurring bootup must be investigated. Contact Nortel Networks 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 ITG Trunk node failure or network QoS configuration errors.
ITG0102	Ethernet voice port restored to normal operation.	Indicates recovery from ITG0402.
ITG0103	Ethernet management port 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 ITG node engineering issues that require analysis by a technician.		
ITG0200	Voice Ethernet buffer exceeded. Packet(s) discarded.	Indicates T-LAN interface hardware problems or excessive T-LAN traffic.

Table 44
ITG Trunk 2.0 alarms (Part 2 of 6)

Alarm	Description	Fault Clearing Action
ITG0201	Management Ethernet buffer exceeded. Packet(s) discarded.	Indicates E-LAN interface hardware problems or excessive E-LAN 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 ITG Trunk 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 ITG card” on page 321)
ITG0206	Invalid A07 message received. Message discarded. A07 is a message signaling interface between Meridian 1 and the ITG Trunk 2.0 card.	Verify that the card type is correctly configured in Meridian 1. Print TNB in LD20. Ensure that the card is configured as a TIE Trunk with XTRK=ITG2.
ITG0207	Unknown H.323 message received. Message discarded.	Indicates unsupported H.323 gateway is misconfigured to send messages to ITG Trunk 2.0. 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).	

Table 44
ITG Trunk 2.0 alarms (Part 3 of 6)

Alarm	Description	Fault Clearing Action
ITG0250	Invalid X12 message received. Message discarded.	Verify that the card type is correctly configured in Meridian 1. Print TNB in LD20. Ensure that the card is configured as a TIE Trunk with XTRK=ITG2.
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. Talkpath 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 ITG Trunk 2.0 card requires manual intervention. For example, you can upgrade to an enhanced software version or replace the ITG Trunk 2.0 card.		
ITG0300	Memory allocation failure. Check configuration. Indicates a dynamic memory allocation problem.	If this occurs frequently, contact Nortel Networks technical support.
ITG0301	DSP channel not responding. DSP channel is disabled. Card sends message to Meridian 1 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	Meridian 1 messaging error threshold exceeded. Too many invalid A07 or X12 messages.	

Table 44
ITG Trunk 2.0 alarms (Part 4 of 6)

Alarm	Description	Fault Clearing Action
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.	
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 ITG 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. T - LAN problem or cable removed.	
ITG0403	Ethernet management port failure. E - LAN problem or cable removed.	

Table 44
ITG Trunk 2.0 alarms (Part 5 of 6)

Alarm	Description	Fault Clearing Action
ITG0404	Cannot open address translation file. File does not exist or is corrupted.	
ITG0406	Start-up 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).	
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.	

Table 44
ITG Trunk 2.0 alarms (Part 6 of 6)

Alarm	Description	Fault Clearing Action
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.	
ITG0450	D-channel loss of signal. Associated channels busied out.	
ITG0451	D-channel hardware failure. Associated channels busied out.	
ITG0452	Meridian 1 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 ITG card can be performed using the following:

- Meridian 1 overlays
- MAT PC
- The command line interface of the ITG card

Access the ITG card

Telnet access

You can connect to the ITG 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 continuing serial session disables the serial connection for the period of the Telnet session. The serial session continues when the telnet session ends.

Serial access

You can connect to the ITG 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.

ITG card overlay commands

System level maintenance of the ITG card is performed using Overlay 32 or Overlay 36. (See Tables 45 and 46.)

Table 45
Supported Overlay 32 commands (Part 1 of 2)

Command	Function
DISC l s c	Disable the indicated card, where: l = loop, s = shelf, and c = card.
DISI l s c	Disable the indicated 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 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.
IDC l s c	Print the Card ID information for the specific card, where: l = loop, s = shelf, and c = card.

Table 45
Supported Overlay 32 commands (Part 2 of 2)

Command	Function
STAT l s c	Print the Meridian 1 software status of the indicated card, where: l = loop, s = shelf, and c = card.
STAT l s c u	Print the Meridian 1 software status of the indicated unit, where: l = loop, s = shelf, c = card, and u = unit.
Note 1: For Option 11C and Option 11C Mini, the TN address < l s c > should be replaced by < s c > and the < l s c u > address by < s c u >.	

Table 46
Supported Overlay 36 commands

Command	Function
DISC l s c	Disable the indicated 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 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.
STAT l s c	Print the Meridian 1 software status of the indicated 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 Option 11C and Option 11C Mini, the TN address < l s c > should be replaced by < s c > and the < l s c u > address by < s c u >.	

Information equivalent to that provided by the STAT command can be accessed from the command line on the card.

Identify ITG routes and cards in the Meridian 1

In LD 16, the Route Data Block, use the “DES” prompt to identify the IP Telephony Gateway route.

ITG card management interface MAC address and IP address

In LD 14, use the “DES” prompt to identify the management interface MAC address and IP address.

Print the ITG route and trunk designators in the Meridian 1

In LD 21, enter the “LTM” (List Trunk Members) in response to the “REQ” prompt to list the ITG route designator’s and the individual ITG trunk designators’ MAC addresses and IP addresses. When cards are added, deleted, or changed, the trunk designators must be updated.

MAT maintenance commands

When changing DSP parameters in MAT, disable the ITG card’s ports before downloading the new parameters. Modifications to node parameters require the affected cards to be rebooted. You can modify a Dialing Plan without rebooting or disabling the cards.

Multi-purpose Serial Data Link (MSDL) commands

All Meridian 1 MSDL commands are supported. Use Overlay 96 to enter MSDL commands. Table 47 lists some of the more important commands.

Table 47
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 MAT or an SNMP manager. A buffer containing received traps is also available through the command line interface, if no SNMP / Alarm manager exists.

Error traps

Table 48 shows the error events that cause the SNMP agent to issue a trap.

Table 48
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 will be 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 49 shows other events that cause the SNMP agent to issue a trap.

Table 49
SNMP trap causing events (Part 1 of 2)

Command	Function
Card Disabled	The card has been disabled by the Meridian 1.
Card Enabled	The card has been enabled by the Meridian 1.
Channel Enabled	A given channel has been enabled by the Meridian 1.

Table 49
SNMP trap causing events (Part 2 of 2)

Command	Function
D-channel Released	The D-channel link has been released.
Alternate Routing	QoS prevents calls from being completed. Cause value “Temporary failure” is sent to Meridian 1 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 they 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 one single LOG file.

ITG shell command set

ITG shell commands are designed to supplement overlay commands, and to introduce new features specific to the ITG platform. To access ITG shell commands, connect a MAT PC or a TTY to the RS-232 Maintenance port on the ITG card faceplate. Alternatively, connect the MAT PC or a TTY to the Serial I/O Panel port to create a more permanent connection to the ITG 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 50-55.

Table 50
General purpose commands (Part 1 of 3)

Command	Description
cardReset	Perform a warm reboot of the ITG card. The card has to be in the OOS state to be able 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 H323 session information for each channel.
itgMemShow	Show memory usage.
ifShow	Show detailed network interface information, including MAC and IP addresses.
IPInfoShow	This command will return the following IP information: • IP addresses (for both management and voice networks) • default router (for both management and voice networks) • subnet masks (for both management and voice networks) • SNMP manager
cardStateShow	card state (that is Unequipped, Disabled, Enabled).
serialNumShow	Print out card serial number and PEC. This command displays the same ITG card serial number that is displayed from the Meridian 1 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 nodes that are in fallback to the conventional voice circuit-switched network.

Table 50
General purpose commands (Part 2 of 3)

Command	Description
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.
displayClear	Clear the maintenance display on the faceplate of the ITG 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 T-LAN.
tLANDuplexSet	Set the duplex mode of the T-LAN.
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 hosts. The host matching the destination address in the packets will respond to the request. If a response is not returned, the sender will time out. This command is useful to determine if other hosts or ITG cards are properly communicating with the sender card. The <numPackets> parameter specifies how many packets to send; if it is not included, pings runs until it is stopped by Ctrl-C (which also exists the ITG shell). Example: ITG> ping "47.82.33.123", 10
trap_gen	SNMP test alarm (one of each type) generation.

Table 50
General purpose commands (Part 3 of 3)

Command	Description
clearLED	Clear the LED display.
esn5PrefixSet	Set the esn5Prefix, default is “100”:esn5Prefix<“char string”>
esn5PrefixShow	Display the esn5Prefix character string.
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", "Subnetmask", "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 they are entered with this command, as the ToS and subnetmask 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”, "Subnetmask", <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 51
File transfer commands (Part 1 of 3)

Command	Description
swDownload hostname, username, password, directory path, filename	Update the software on the ITG card with the binary file received from an FTP server corresponding to the *hostname* IP address. The ITG card FTP client performs a get which downloads the file to the ITG flash bank. A checksum is calculated to check correct delivery. Once the new software version is successfully downloaded, the ITG 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 ITG card itself or another ITG card when a PC card in the A: drive of the ITG 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 ITG card with the address table file on the indicated host, account, and path. The ITG 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 ITG card with the config.ini file on the indicated host, account, and path. The configFileGet task on the ITG 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 ITG card with the bootptab file on the indicated host, account, and path. The bootpFileGet task on the ITG host starts an FTP session with the given parameters and downloads the file to the flash file system.
Example:	ITG> bootpFileGet “ngals042”, “anonymous”, “guest”, “/bootpDir”, “bootptab”

Table 51
File transfer commands (Part 2 of 3)

Command	Description
SNMPConfFileGet hostname, username, password, directory path, filename	Update the SNMP configuration file on the ITG card with the SNMP configuration file on the indicated host, account and path. The SNMPConfFileGet task on the ITG 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 via FTP to the ITG 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 ITG host starts an FTP session with the given parameters and downloads the ITG 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 ITG host starts an FTP session with the given parameters and downloads the ITG card’s previous Operational Measurements file to the indicated location on the host.
Example:	ITG> prevOmFilePut “ngals042”, “anonymous”, “guest”, “/prevDir”, “omFile”
traceFilePut hostname, username, password, directory path, filename	The traceFilePut task on the ITG host starts an FTP session with the given parameters and downloads the ITG card’s call trace file to the indicated location on the host.
Example:	ITG> traceFilePut “ngals042”, “anonymous”, “guest”, “/trcDir”, “trcFile”

Table 51
File transfer commands (Part 3 of 3)

Command	Description
currLogFilePut hostname, username, password, directory path, filename	The logFilePut task on the ITG host starts an FTP session with the given parameters and downloads the ITG 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 ITG host starts an FTP session with the given parameters and downloads the ITG 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 ITG host starts an FTP session with the given parameters and downloads the ITG 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 ITG 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 ITG card).
Example:	ITG> hostFilePut "ngals042", "anonymous", "guest", "/hostDir", "hostFile", "/C:/CONFIG/CONFIG1.INI"

Table 52
NVRAM IP configuration commands (Part 1 of 2)

Command	Description
NVRIPSet IP address	Set the IP address in NVRAM.
Example:	ITG> NVRRIPSet "47.23.34.19"

Table 52
NVRAM IP configuration commands (Part 2 of 2)

Command	Description
NVRGWSet IP gateway	Set the default gateway address in NVRAM.
Example:	ITG> NVRRGWSet “47.0.0.1”
NVRSMSet subnet mask	Set the subnet mask in NVRAM.
Example:	ITG> NVRRSMSet “255.255.240.0”
NVRIPShow	Print the values of the IP parameters that exist in NVRAM.
Example:	ITG> NVRIPShow
nvramLeaderSet	Set the leader bit in NVRAM.
Example:	ITG> nvramLeaderSet
nvramLeaderClr	Clear the leader bit in NVRAM, but does not erase the IP parameters in NVRAM.
Example:	ITG> nvramLeaderClr
NVRClear	Clear IP parameters in NVRAM.
Example:	ITG> NVRClear
setLeader IP address, IP gateway, subnet mask	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.
Example:	ITG> setLeader “47.23.45.67”, “47.0.0.1”, “255.255.240.0”
clearLeader	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.
Example:	ITG> clearLeader

Table 53
DSP commands

Command	Description
DSPReset DSP Number	Reset the indicated DSP.
Example:	ITG>DSPReset 0
DSPSelfTest DSP Number	Run self-test on the DSP.
Example:	ITG>DSPSelfTest 0
DSPNumShow	Print number of DSPs on ITG card.
Example:	ITG>DSPNumShow
DSPPcmLpbkTestOn	Start PCM loopback test on the indicated DSP.
Example:	ITG>DSPPcmLpbkTestOn
DSPPcmLpbkTestOff	Stop PCM loopback test on the indicated DSP.
Example:	ITG> DSPPcmLpbkTestOff
DSPSndLpbkTestOn	Start Send loopback test on the indicated DSP.
Example:	ITG> DSPSndLpbkTestOn
DSPSndLpbkTestOff	Stop Send loopback test on the indicated DSP.
Example:	ITG> DSPSndLpbkTestOff
DSPRcvLpbkTestOn	Start Receive loopback test on the indicated DSP.
Example:	ITG> DSPRcvLpbkTestOn
DSPRcvLpbkTestOff	Stop Receive loopback test on the indicated DSP.
Example:	ITG> DSPRcvLpbkTestOff

Table 54
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 55
DCHIP-only commands

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.
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.

ITG card self-tests

During power-up, the ITG card performs diagnostic tests to check correct operation. You can use the faceplate RS-232 port on the ITG card to monitor these tests. ITG sends messages indicating the completion of each phase of testing and any detected faults, to this port.

Additionally, the ITG 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, see "ITG Trunk 2.0 faceplate maintenance display codes" on page 329.

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:

- 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 tries 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 will output an error to the RS-232 port. It will attempt 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 ITG card then enters the unrecoverable failure state. This makes sure 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 ITG card supports the backplane Card LAN interface for the purposes of communicating self-test errors and allowing maintenance access including resetting the card remotely.

BIOS self-test

The ITG 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 ITG card base code performs the following tests:

- flash integrity test
- PGA read/write test
- PCMCIA controller test (also tests the PCI bus)
- Timer and DMA tests
- DSP test

Field-Programmable Gate Array (FPGA) testing

Before communication with the Meridian 1, the 8051XA controller downloads FPGA data files and performs tests to check correct programming of the FPGA.

Upgrades

Several different types of upgrades are required for the Meridian 1 IP Gateway application. (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 MAT PC. It is recommended that you load the application from the network, rather than the faceplate PC card.

Application upgrade

In this instance, the customer is provided with a 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.

Capacity upgrades

MAT manages the channel capacity of an ITG node. Any restrictions on the maximum number of configurable channels are handled by MAT software. When the maximum number is reached, MAT prevents you from configuring more.

Flash storage upgrades

These are provided through standard 5 Volt ATA compatible PCMCIA Flash cards. When installed in an ITG card (“hot installation” allowed), the additional storage provided by the card is made available as a new DOS volume.

Protocol table upgrade

The UIPE’s protocol tables are included in the application binary; a protocol table upgrade is an application upgrade. If changes are made to the protocol tables, the host application must be relinked to pick up the new tables and a new load created and distributed.

Software upgrade mechanisms

Use MAT to upgrade software. You must reboot the ITG card to run the new software.

Upgrade software using MAT

The new ITG software application can be downloaded from the MAT PC to the ITG card. Use the following procedure to upgrade software:

1 Get the latest Meridian 1 recommended ITG 2.0 software version from Nortel Networks. Select the location on the MAT PC hard drive where it is to be loaded. Record the MAT 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 card software” on page 225.

2 Open MAT and launch the ITG ISDN IP Trunks application.

3 Check the current software version of the ITG cards to be upgraded. To check the software version, double - click on a card and click the “Configuration” tab where “S/W version” displays the current software version as read from the ITG card.

4 Select the cards from the main card list view that are to be upgraded. Upgrade all the cards in the node together, unless installing a spare card that has older software.

5 Disable all ITG cards to be upgraded. Use:

- the Meridian 1 LD 32 DISI command from the MAT Maintenance Windows,
- the MAT System Passthru terminal,
- or from a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1.

6 In the MAT IP Telephony Gateway Main window, select “View / Refresh” and check that the card status is showing “Disabled.”

7 Select menu **Configuration | Synchronize | Transmit**.

8 An ITG – Transmit Options dialog box is displayed.

9 In the Transmit Options group box, select the radio button “Transmit to selected cards.”

10 In the Software Download group box, check “Card software.”

11 Click on the “Browse” button to locate the ITG card software downloaded earlier to the MAT hard drive. Select the software file and click “Open” to save the selection. The path and file name of the ITG card software appear in the edit box next to the “Browse” button.

12 Click on the “Start Transmit” button to begin the ITG card software upgrade process.

The software is transmitted to each card in turn and burned into the flash ROM on the ITG card.

Monitor the status in the Transmit Control window. Confirm that the card software is transmitted correctly to all cards. Note any error messages, examine, and correct any problems. Repeat card software transmission until it is completed correctly on each ITG card. The cards continue to run the old software until they are rebooted.

13 Reboot each ITG 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 ITG cards have been reset and have correctly rebooted, they respond to the MAT ITG status refresh (that is, disabled: active; disabled: backup: disabled).

14 These cards should remain in the disabled state after the upgrade, so that 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. Or you can reset the cards by pressing the “reset” button on the card faceplate using a pointed object.

15 Double click each upgraded card and check the software version on the “Configuration” tab of the Card Properties.

16 Use the LD 32 ENLC command to re-enable the ITG cards.

The software upgrade procedure is complete.

Replace an ITG card

If, following a reboot, the ITG card displays an “F:xx” on the LED Maintenance Display, this indicates an unrecoverable hardware failure. The card will not register with the Meridian 1. For a complete listing of faceplate Maintenance Display codes, see “ITG Trunk 2.0 faceplate maintenance display codes” on page 329.

Remove the card for two to three seconds and then reinstall it. If the failure continues, you must replace the card. Use the following procedure to replace the card:

1 Locate the node of the bad card:

- **a** Open the **ITG ISDN IP Trunks** application in MAT.
- **b** In the upper part of the **IP Telephony Gateway - ISDN IP Trunk** window, click on the site name. All the cards in the node are listed in the lower part of the window.
- **c** Locate the card to be replaced in the lower window by card TN.

2 Disable the bad ITG card in LD 32 by using the DISI command.

3 If the card that is to be replaced is an 8-port NTCW80AA card, disconnect the T-LAN Ethernet cable from the faceplate of the bad card. Label the cable to identify that it is the T-LAN Ethernet connection so that you can later reattach it to the replacement card.

If the card that is to be replaced is an 8-port NTCW80CA or a 24-port NT9061AA card, disconnect the T-LAN Ethernet cable from the I/O cable. Label the cable to identify that it is the T-LAN Ethernet connection so that you can reinstall the cable on the replacement card. Remove the bad ITG card from the Meridian 1.

4 Select Leader 0 or any ITG card in the node, from the lower window.

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 bad ITG card from the list of cards in the node.

8 Change the MAC address to the MAC address of the replacement ITG card. The MAC address is the “Motherboard Ethernet” address on the faceplate label of the replacement ITG card.

9 Click “OK”.

10 Select Leader 0 or any ITG card in the node.

11 Select menu **Configuration | Synchronize | Transmit** to transmit the Node Properties from MAT to the Active Leader card of the ITG node. Click the “Node Properties” box, and then click “Start Transmit.” This will update the node properties of the Active Leader card with the MAC address of the replacement ITG card.

12 Install the replacement ITG card into the Meridian 1:

a Pull the top and bottom locking devices away from the ITG faceplate.

b Insert the ITG card into the card guides and carefully push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When you install ITG cards, 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 ITG Faceplate Maintenance display to see start-up 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 “ITG Trunk 2.0 faceplate maintenance display codes” on page 329 for a complete listing of the codes.

13 Attach the T - LAN Ethernet cable to the faceplate of the replacement ITG card.

Note: When connecting the ITG card to the T - LAN, the link status LED on the ITG 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 ITG card. This indicates that the corresponding port is set to operate at 100 Mbit/s and is the link is good.

14 If the card that is being replaced is an 8-port NTCW80AA and the replacement card is an 8-port NTCW80CA, the I/O cable must be replaced:

a Locate the NTCW84LA cable that was included in the 1.0 to 2.0 upgrade kit.

b Remove the NTCW84MA cable from the I/O panel.

c Disconnect the E-LAN Ethernet cable and label it as the E-LAN connection.

d If connected, disconnect the DCH and maintenance cable from the NTCW84MA.

e Connect the new NTCW84LA to the I/O panel.

f Connect the E-LAN, T-LAN, DCH and Maintenance cables (if previously connected) to the I/O cable. If the card being replaced is an 8-port NTCW80AA, connect the T-LAN to the card faceplate.

15 In the MAT **IP Telephony Gateway - ISDN IP Trunk** Main window, select menu **View | Refresh** and check that the replacement ITG card status is showing “Unequipped”.

Check card software

1 In the IP Telephony Gateway window, double - click the replacement ITG card to open the Card properties window. Leave the default selection of the ITG card in the Card Properties window and click the “Configuration” tab.

2 Check that the “S/W release” shows the latest recommended software version.

If the replacement card requires a software upgrade, refer to “Software upgrade mechanisms” on page 319.

Transmit card properties and dialing plan

It is not necessary to disable ITG cards when transmitting a dialing plan alone.

1. In the IP Telephony Gateway window, select the replacement ITG 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 ITG card.
6. In the “IP Telephony Gateway” main window, select menu **View | Refresh**. The card status displays “Enabled.”
7. Check the TN, management interface MAC address, and IP addresses for each ITG card. Compare the displayed values with those on the ITG Installation Summary Sheet.
8. Update the ITG Installation Summary Sheet with the new MAC address of the replacement ITG card.

Backup and restore procedures

ITG card

Data configured on the MAT PC (for example, address translation tables and DSP configuration) are locally saved on the MAT PC and also downloaded to the ITG cards. The ITG card stores this data in its internal Flash File volume (Flash EPROM which acts as a disk drive). The MAT PC can query the card and retrieve data from it. If the ITG card is replaced, you can use the version of data stored on the MAT PC to configure the new card with the same data as the replaced 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 MAT PC or other external device for generating weekly or monthly traffic reports.

MAT

MAT 6.6 has backup and restore procedures for all data downloaded from, or to, the card. When a MAT terminal is connected to the card, user intervention is necessary to transmit all lost data from the MAT terminal to the ITG card.

Command line interface

If MAT is temporarily unavailable, the ITG shell command line interface can be used to retrieve configuration files from an FTP server or from a PC card.

Fault clearance procedures

DSP failure

In the case where 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 will cease to respond to the Meridian 1 and are ultimately taken out of service by the Meridian 1 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 Meridian 1 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 Meridian 1 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 Meridian 1 to reset the trunks to the “IDLE” state. The leader card is informed and incoming calls can be assigned to those channels.

Card failure

If following a reboot, the ITG card displays a code in the form of F:xx on the faceplate Maintenance display, this indicates an unrecoverable hardware failure. The card will not register with the Meridian 1.

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

This section covers the following three types of DCH failure which can affect the ITG card:

- DCH link failure (DCH releases)
- PC card failure
- DCH card failure

When the DCH fails (with no backup DCH):

- 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 Meridian 1 to inform the core the call is released.
- When the near end user releases an established call, the Meridian 1 informs the Follower through SSD messages.
- ISDN features across the IP will 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, through

- 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 for making sure of 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 ITG card is plugged in.

DCHIP card failure

This occurs when the DCHIP ITG card goes out of service. The DCHIP ITG 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 cancelled.

Power loss

Since the ITG 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 ITG card can be removed from the IPE shelf indefinitely and still retain all configuration data.

ITG Trunk 2.0 faceplate maintenance display codes

The ITG maintenance display provides startup codes, operating mode and error information on the functional card state. Table 56 lists the startup codes and operating mode codes.

When the ITG 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 card goes on to the next test. If more than one test fails, the message displayed indicates the last failure.

Table 56
Faceplate maintenance display message summary (Part 1 of 4)

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

Table 56
Faceplate maintenance display message summary (Part 2 of 4)

Normal Code	Fault Code	Description
T:10	F:10	Testing for presence of security device. The NT0961 has no security device. ***Note:*** For ITG Trunk 2.0, 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
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 O.K.
PT:1	PF:1	Pentium module powered OK. ***Note:*** If the ITG card displays this message, check that the Pentium module is fully seated in the motherboard socket.
T:19		Waiting for application start-up message from host

Table 56
Faceplate maintenance display message summary (Part 3 of 4)

Normal Code	Fault Code	Description
T:20		CardLAN enabled, waiting for Request Config. Message. Card is looking for an active leader by sending bootp requests on the management LAN. If no bootp response is received on the management LAN, 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 management LAN 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.
BIOS		Card is running the ROM BIOS. The card detected no valid ITG Trunk software image or the JKL escape sequence was entered during startup from the keyboard of a terminal connected to the local maintenance port. If faceplate displays BIOS, it is not functioning as an ITG trunk card.
T:21		CardLAN operational, A07 interface to Meridian 1 enabled, display now under ITG Trunk software control. ITG > shell is available for manual card configuration.
T:22		ITG card is starting up the ITG ISL Trunk application.
LDR		Card is running active leader tasks.

Table 56
Faceplate maintenance display message summary (Part 4 of 4)

Normal Code	Fault Code	Description
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 MAT.
FLR		Card has detected the active leader, and is running Follower tasks.

Appendix A: Cable description and NT8D81BA cable replacement

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. If you have a network that uses 100-Base-T and you have an NT8D81BA ribbon cable, you must install an NT8D81AA cable.

NTMF94EA E - LAN, T - LAN and Serial Port cable

The NTMF94EA cable connects the I/O connector on Option 11 or large systems to the E-LAN, T-LAN and one RS232 port. (See Figure 58 and Table 57.)

Figure 58
NTMF94EA E-LAN, T-LAN and serial port cable

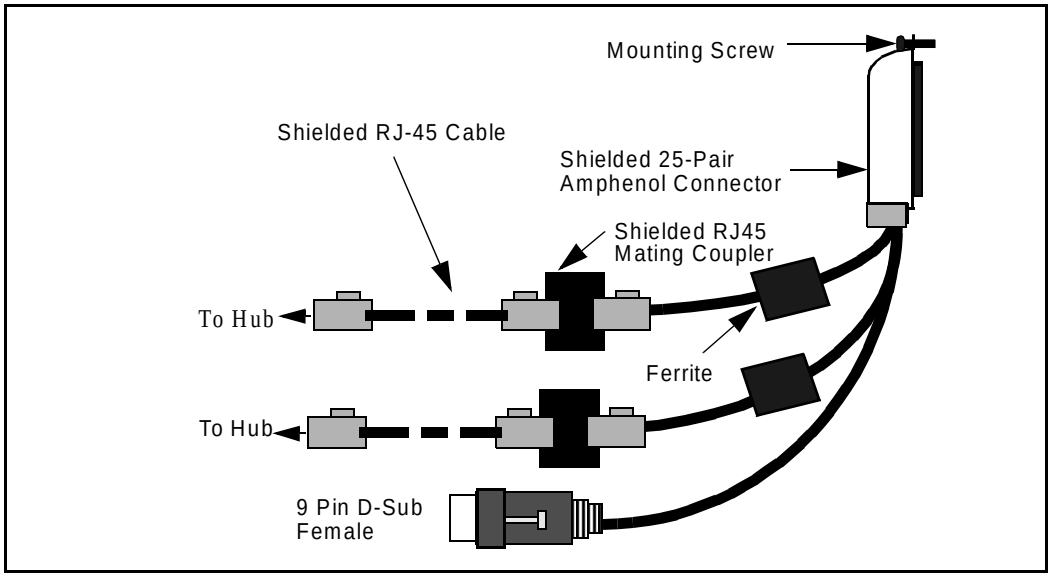


Table 57
NTMF94EA E - LAN, T - LAN and Serial Port cable connections

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 E-LAN, T-LAN, DCH & Serial cable

The NTCW84KA cable connects the I/O connector on Option 11 or Large System to the ethernet management and telephony voice ports with one RS232 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 59 and Table 58.)

Figure 59
NTCW84KA E-LAN, T-LAN, DCH and serial cable

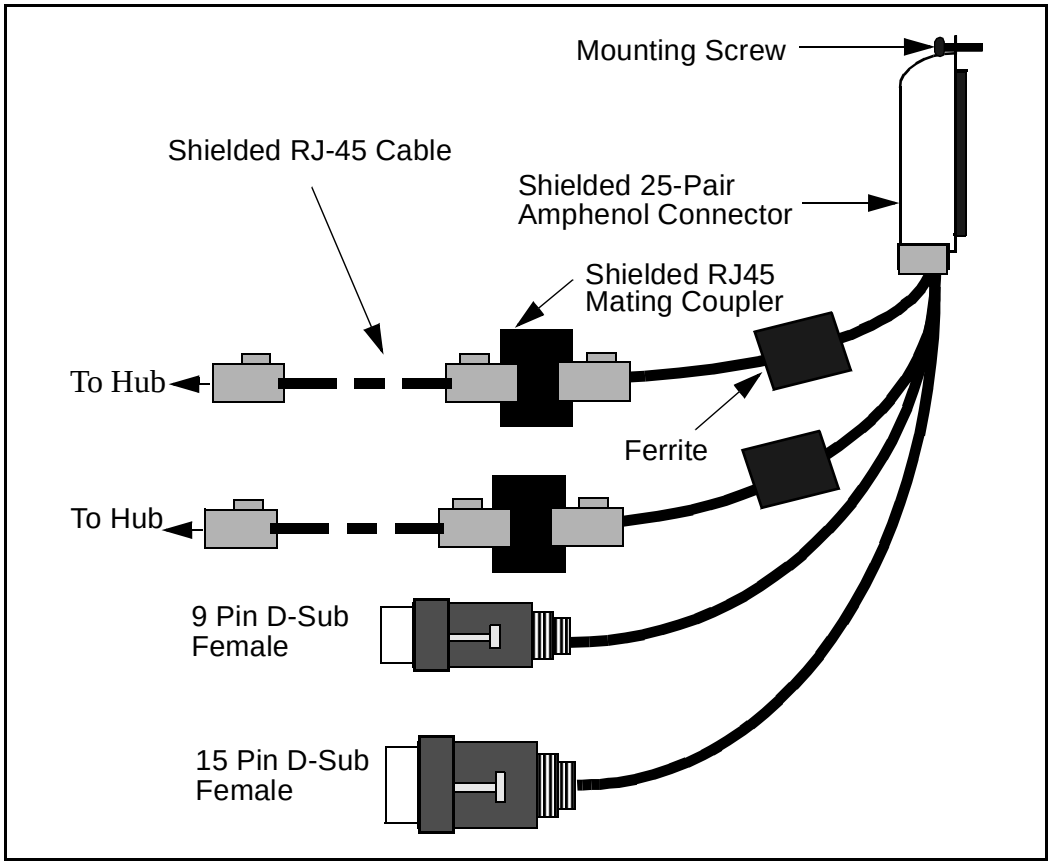


Table 58
NTCW84KA E - LAN, T - LAN, DCH & Serial I/O cable connections (Part 1 of 2)

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

Table 58
NTCW84KA E - LAN, T - LAN, DCH & Serial I/O cable connections (Part 2 of 2)

I/O Panel: P1	Signal Name	P2, P3, P4, P5	Color
P1-44	TX-	P4-2	White / Orange
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 a MAT PC or terminal to the ITG card through the maintenance port connector on the faceplate. You can connect this cable directly to the 9-pin D-type RS232 input (COM port) on a standard PC. (See Figure 60 and Table 59.)

Figure 60
NTAG81CA PC maintenance cable

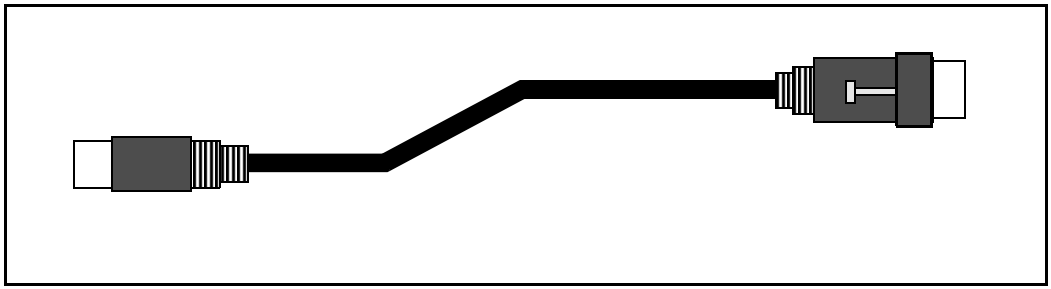


Table 59
NTAG81CA Faceplate Maintenance cable connections

Signals (ITG 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 61 and Table 60.)

Figure 61
NTAG81CA Maintenance Extender cable

Table 60
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 62 and Table 61.)

Figure 62
NTCW84EA pigtail cable

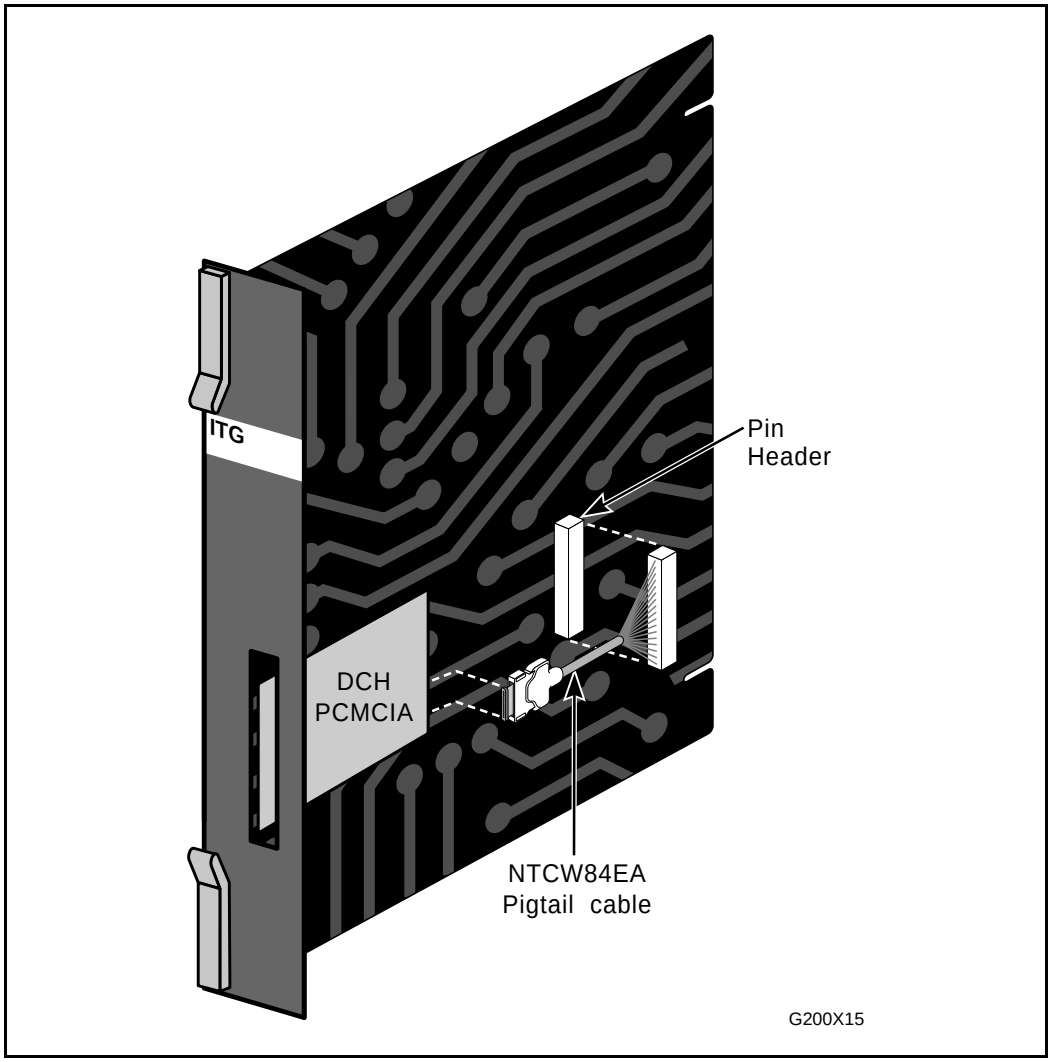


Table 61
NTCW84EA pigtail cable connections

PCMCIA 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 (DChannel) 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 female15 way D-sub port of the NTCW84KA. (See Figure 63 and Table 62.)

Figure 63
NTMF04BA MSDL extension cable

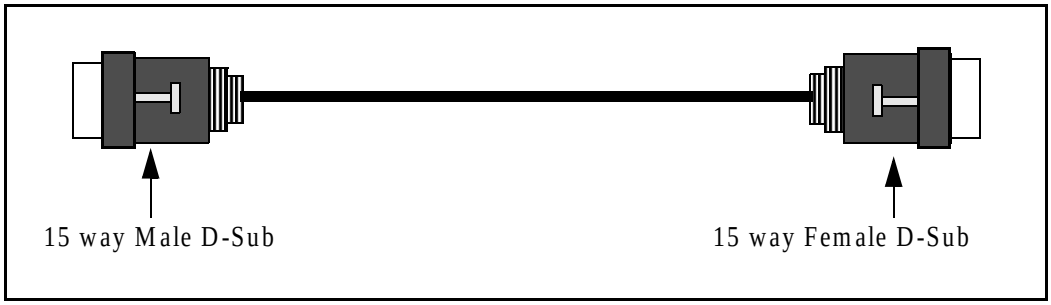


Table 62
NTMF04BA MSDL extension cable connections

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 1.0 to 2.0 in field upgrades. It breaks out the signals from the I/O connector on large systems and Option 11 to the ethernet management port (E-Lan connection) , ethernet voice port (T-Lan connection), one maintenance RS232 port brought out on a 9-way D-type connection plus the Dchannel 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 System) 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 Meridian 1/ Option 11 systems via the mounting screw provided on the top of the 25 pair Amphenol connector.

The NTCW84LA/MA cable provides a shielded RJ45 to RJ45 coupler at the end of its E-LAN and T-Lan interfaces. This provides the connection point to the customers E-LAN equipment. Shielded Cat. 5 cable must be used for connection from this point to the customers Hub or Router. See Figure 64 and Table 63.

Note: For all LAN cables originating from the ITG card, standard cable ties should be adopted to bundle these cables together as they route out of the system.

Figure 64
NTMF94LA upgrade cable

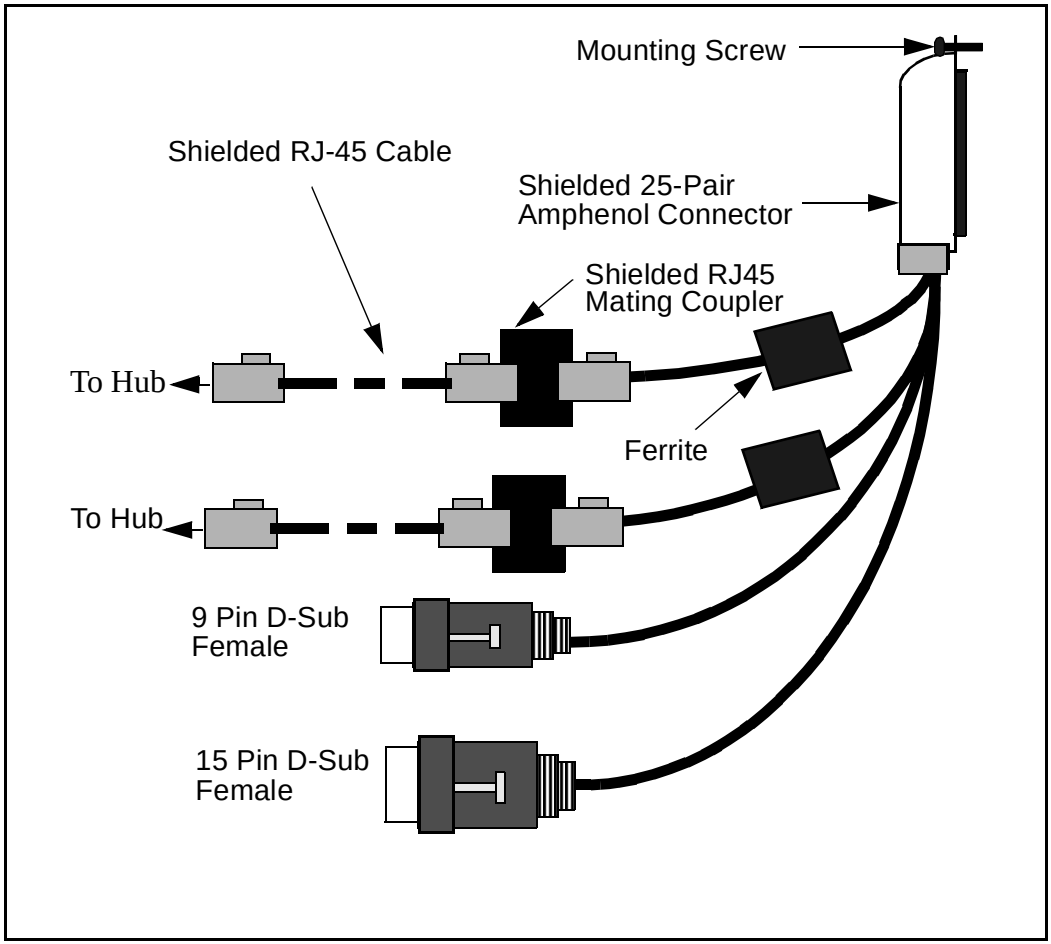


Table 63
NTMF94LA cable connections (Part 1 of 2)

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 63
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 RJ45 coupler is the connection point for the customer's shielded Category 5 LAN cable to the hub, switch, or router supporting the T-LAN and E-LAN. You must use shielded Category 5 RJ45 cable to connect to the customer's T-LAN/E-LAN equipment.

1 Connect the customer-provided shielded Category 5 LAN 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 RJ45 cable and building ground.

The ohmmeter *must* measure Open to ground before plugging it into the shielded RJ45 coupler on the end of the NTMF94DA.

If it does *not* measure Open, you must install the unshielded RJ45 coupler (provided) on the end of the NTMF94DA to prevent ground loops to external LAN equipment.

Replace cable NT8D81BA with NT8D81AA

This procedure explains how to replace the NT8D81BA cable with the NT8D81AA cable and how to install the NTCW84JA special IPE filter.

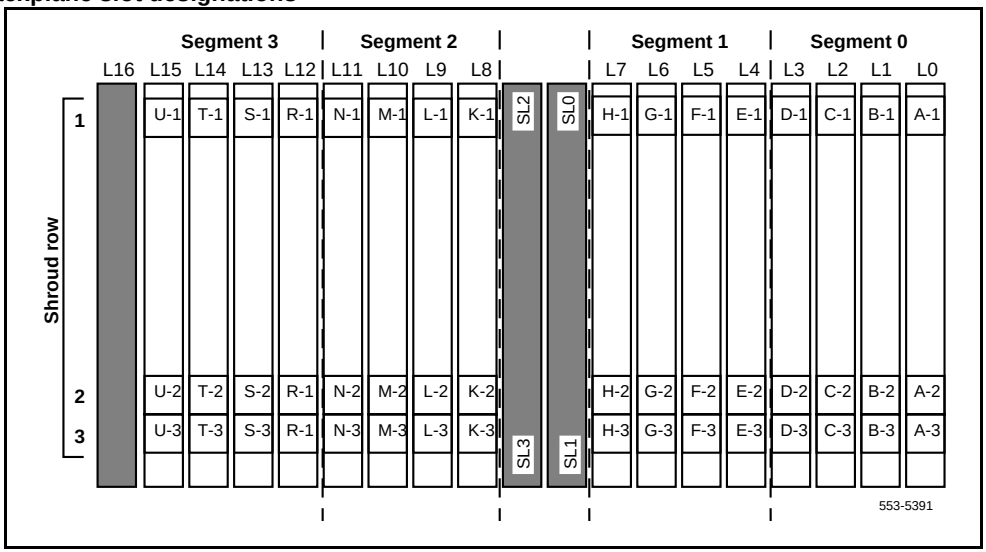
Cables are designated by the letter of the I/O panel cutout (A, B, C, and so on) where the 50-pin cable connector is attached. Each cable has three 20-pin connectors (16 positions are used), designated 1, 2, and 3, that attach to the backplane. Using the designations described, the backplane ends of 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 64 shows the cable connections from the backplane to the inside of the I/O panel. Figure 65 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 64
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 65
Backplane slot designations



Tools list

- Ty-wrap cutter
- Ty-wraps
- Needle nose pliers
- Slotted screwdriver

NT8D81BA cable removal procedures

1 Identify the I/O panel and backplane designation that corresponds to the LEFT slot of the pair of card slots, viewed front the front, in which you installed the ITG ISL Trunk card.

2 Disconnect filter from I/O panel using screwdriver and needle nose pliers. Retain fasteners.

3 Power down IPE shelf.

4 Remove IPE module I/O safety panel.

5 To remove the ribbon cables from IPE backplane:

Apply gentle pressure on the tab on the right side of the shroud while pulling on the connector until it pulls free from shroud.

Remove connector 1 first, then remove connectors 2 and 3.

6 Discard NT8D81BA cable.

Install NTCW84JA filter and NT8D81AA cable

1 Install NTCW84JA special IPE filter connector in the vacant I/O panel slot using retained hardware.

2 Install NT8D81AA ribbon cable connectors in 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 IPE module and restore original arrangement. Start with the cables that are going to be underneath.

4 Attach NTCW84JA special IPE filter to NT8D81AA 50-pin connector using bail clips.

5 Restore power to IPE module.

6 Replace I/O safety panel.

Appendix B: Environmental and electrical regulatory data

Environmental specifications

Table 65 lists measurements of performance under test conditions of temperature and shock.

Table 65
ITG temperature and humidity specifications

Specification	Minimum	Maximum
	Normal operation	
Recommended	15° C	30° C
Relative humidity	10%	55% (non-condensing)
Absolute (less than 72 hours)	0° C	45° C
Relative humidity	5%	95% (non-condensing)
Rate of change	Less than 1° C per three minutes	
Temperature cycling	0° C to 65° C, 1° C/min., three cycles	

Table 65
ITG temperature and humidity specifications (Continued)

Specification	Minimum	Maximum
	Storage	
Recommended	-50° C	+70° C
Relative humidity	0%	95% (non-condensing)
	Temperature shock	
In three minutes	-50° C	25° C
In three minutes	70° C	25° C

Mechanical conditions

Refer to Table 66 for ITG mechanical tolerance ranges.

Table 66
ITG 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	

Electrical regulatory standards

The following three tables list the safety and electromagnetic compatibility regulatory standards for the ITG card, listed by geographic area. Specifications for the ITG card meet or exceed the standards listed in these regulations.

Safety

Table 67 provides a list of safety regulations met by the ITG card, with the type of regulation and the country or area covered by each regulation.

Table 67
Safety regulations

Regulation identifier	Regulatory agency
UL 1459	Safety, United States, CALA
CSA 22.2 225	Safety, Canada
EN 41003	Safety, International Telecom
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
AS3260, TS001 - TS004, TS006	Safety/Network (Australia)
JATE	Safety/Network (Japan)

Electromagnetic Compatibility (EMC)

Table 68 lists the electromagnetic emissions regulations met by the ITG card, with the country's standard that lists each regulation.

Table 68
Electromagnetic Emissions

Regulation identifier	Regulatory agency
FCC part 15 Class A	United States Radiated Emissions
CSA C108.8	Canada Radiated Emissions
EN50081-1	European Community Generic Emission Standard

Table 68
Electromagnetic Emissions

Regulation identifier	Regulatory agency
EN55022/CISPR 22 CLASS A	Radiated Emissions (Basic Std.)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard
AS/NZS 3548	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Table 69 lists the electro-magnetic immunity regulations met by the ITG card, with the country's standard that lists each regulation.

Table 69
Electro-magnetic immunity

Regulation identifier	Regulatory agency
CISPR 22 Sec. 20 Class A	I/O conducted noise
IEC 801-2 (level 4)	ESD (Basic Standard)
IEC 801-3 (level 2)	Radiated Immunity (Basic Standard)
IEC 801-4 (level 3)	Fast transient/Burst Immunity (Basic standard)
IEC 801-5 (level 4, preliminary)	Surge Immunity (Basic Standard)
IEC 801-6 (preliminary)	Conducted Disturbances (Basic Standard)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard
AS/NZS 3528	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Appendix C: 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.

To convert 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 70, “CIDR format remainders,” on page 358 to get the dotted decimal value for the field following the last field containing “255”.

In the example of /20 above, the remainder is 4. In Table 70, “CIDR format remainders,” on page 358, 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 70
CIDR format remainders

Remainder of CIDR format value divided by eight	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 D: Configure a Netgear RM356 modem router for remote access

Management and support of the ITG network depend on IP networking protocols including SNMP, FTP, and Telnet. A modem router should be installed on the Meridian 1 site management and signalling LAN (called the embedded LAN or E-LAN as opposed to the customer's enterprise network or C-LAN) in order to provide remote support access for ITG and other IP-enabled Nortel Networks products. The Nortel Networks 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 E-LAN 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

- Password Authentication Protocol (PAP) for dial-in PPP connection.
- RM356 manager password.
- CLID for dial-in user authentication (requires C.O. 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

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 Cat5 10BaseT Ethernet cables to connect the modem router to the Management interface of up to four ITG cards. Other IP-enabled Nortel Networks products on the E-LAN may be connected to the RM356 modem router, including the Meridian 1 PBX, a local MAT PC, Symposium Call Center Server, and Call Pilot.

Note: The up-link connection to an additional E-LAN hub or optional C-LAN 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 received on the LAN.

3 Connect the RJ45 plug end of the local manager cable to the RS232 Manager port RJ45 jack on the rear of the modem router. Connect the other end of the cable to an RS232 terminal or PC COM port configured for the following communication parameters: 9600 bps, 8, none, and 1. The local maintenance cable connects directly to data terminal equipment (DTE).

4 The analog telephone line should be a C.O. line or a PBX extension with a Direct Inward Dialing(DID) number if that is in compliance with the customer's network security policy.

Configure the MAT ITG PC to communicate with a remote Meridian 1 site via modem router

If your version of MAT does not support the modem router communication profile for Meridian 1 system types, you may work around the limitation by configuring a Dial-up Networking (DUN) session under MS Windows to connect to the modem router at a particular Meridian 1 site.

In the MAT Navigator, you must configure the Meridian 1 system communication profile as "Ethernet." You must establish the Dial-up Networking session from MS Windows before attempting to connect to the Meridian 1 system from the MAT Navigator. ITG nodes on the same E-LAN will also be accessible over the same Dial-up Networking connection to the modem router.

Configure the RM356 modem router by the manager menu

Configuring the RM356 modem router by the manager menu can be completed from a terminal or PC connected to the local RS232 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 menu selection number when prompted to display a sub-menu, configuration form, or command prompts.

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" is displayed.

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 Meridian 1 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 "Active=Yes". 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 Ethernet interface on the E-LAN.

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 GW router, and if the modem router is permitted access over the C-LAN to other ITG nodes on remote E-LANs, define a default network route pointing to the Management GW IP address on the local E-LAN. 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 C-LAN.

Note 2: To prevent access from the modem router to the C-LAN via the Management GW router on the E-LAN, 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 e.g. "DefaultGW" (no spaces). Toggle "Active=Yes/No" for security purposes. 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 GW IP address on the E-LAN 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 Setup " is displayed.

16 Under "Telco Options" toggle "CLIDAuthen=None/Preferred/Required".

CLID requires a C.O. line subscribed for CLID service where available. "Preferred" means some dial-in user profiles may 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 router: 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 E-LAN IP address that will be assigned to the Dialup Networking (DUN) PPP client on the remote MAT PC.

Note: The remote MAT PC will receive this E-LAN 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 MAT PC function as if the PC were located on the customer's E-LAN.

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 timeout 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 may 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 "Active=Yes/No" for security purposes. Type in a password for PAP. The DUN client on the remote MAT PC must provide the user name and password defined here when dialing up the modem router.

Set "Callback=Yes/No" according to the customer's network security policy and practices. Nortel Networks 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 MAT PC dials up the modem router, if CLID authentication is required for the user profile. CLID depends on providing a C.O. 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 Networks 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 E-LAN. The modem router's security features are worthless if the manager password is not changed regularly according to good network security practices.

RM356 modem router manager menu (application notes on Meridian 1 E-LAN installation)

This section displays the various menus of the RM356 modem router:

```
                        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
```

Index

T

V

Meridian 1

Meridian Internet Telephony Gateway (ITG) Trunk 2.0/ ISDN Signaling Link (ISL)

Description, Installation and Operation

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.
SL-1 and Meridian 1 are trademarks of Nortel Networks.
Publication number: 553-3001-202
Document release: Standard 1.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.