Meridian 1

Meridian Internet Telephony Gateway (ITG) Trunk 1.0/Basic Per-Trunk Signaling

Description, Installation and Operation

Document Number: 553-3001-116
Document Release: Standard 2.00
Date: April 2000

Printed in Canada

Revision history

April 2000

Standard, release 2.00. This is a global document and is up-issued for X11 Release 25.0x.

January 1999

Standard, release 1.00.

Contents

About this document

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 document contains the following sections that provide information on the NTCW80 Meridian Internet Telephony Gateway (ITG) Trunk 1.0 card:

Description describes the ITG functional and physical characteristics.

Engineering Guidelines describes requirements for the successful integration of ITG with the customer's existing intranet.

Installation and configuration describes the steps involved in installing and configuring the ITG card.

Administration describes the ITG administration procedures and ITG parameter configuration.

Maintenance describes maintenance and report generating.

Appendix A describes ITG cabling.

Appendix B describes ITG card product integrity.

Appendix C describes how to convert subnet masks from Classless Inter Domain Routing (CIDR) to dotted-decimal format.

Description

The Meridian Internet Telephony Gateway (ITG) Trunk 1.0 application reduces customers' communication costs by routing voice traffic at low marginal cost over private IP network facilities. The private IP network facilities must have under-utilized bandwidth on the private Wide Area Network (WAN) backbone.

Organizations that send more traffic over IP networks can reduce costs through the reduction of required lines for voice and fax traffic.

The ITG Trunk 1.0 application compresses Pulse Code Modulation (PCM) voice, demodulates Group 3 fax, and routes the packetized data over a private internet, or intranet, to provide non-ISDN tie trunks between Meridian 1 Electronic Switched Network (ESN) nodes.

It is a requirement that the customer has already installed a corporate IP network, and that routers are available for WAN connectivity between networked Meridian 1 systems. ITG is offered for Intranet, rather than Internet use, since an Intranet is a more controlled and managed data network environment. 10BaseT Ethernet interfaces to the ITG card are required, as well as support of IP version 4 routing and addressing in the WAN. There is no restriction on the physical medium of the WAN.

The NTCW80 ITG card supports eight voice channels (trunk ports) per card and emulates an NT8D14 Universal Trunk (EXUT) card. The amount of ports supported on a card is controlled by a keycode.

The ITG supports standard H.323 call processing and ITU standard Digital Signal Processor (DSP) voice coding and compression algorithms (codecs), such as G.711, G.723, G.729A, and G.729. It supports real-time Group 3 fax support, Call Detail Recording (CDR), and Least Cost Routing. The design of the ITG card is flexible so that, in the future, emulation of other card types is possible.

A key feature of ITG is the ability to monitor the data network and automatically re-route calls to circuit-switched voice facilities if quality of service over the data network declines. This *Fallback to Conventional Circuit-Switched Voice Facilities* feature allows the system and craftsperson to determine what is the acceptable quality of service over the data network. The customer can configure quality of service parameters as required. If the quality falls below the expected level of quality of service, the regular circuit-switched route is selected until the quality of service is back to the acceptable level.

Software Licensing

ITG cards use a Security Device that is pre-installed on the motherboard. A keycode enables the card and provides for upgrades of port capacity or application software.

Applicable systems

The ITG system is available for Meridian 1 options 11C, 11E, 21E, 51, 51C, 61, 61C, 71, 81 and 81C systems running X11 release 21 or later software. It is also compatible with SL-1 systems NT, RT, and XT upgraded to support IPE cards.

System requirements

ITG requires X11 release 21 or later software.

ITG requires MAT 6.1 or later and the MAT Common Services, Alarm Notification, and Internet Telephony Gateway applications. Alarm Notification is part of the MAT Alarm Management package.

ITG requires either the Basic Alternate Route Selection (BARS, package 57), or Network Alternate Route Selection (NARS, package 58) packages.

The Coordinated Dialing Plan (CDP, package 59) and Flexible Numbering Plan (FNP, package 145) packages are optional if these dialing plans are used.

Table 1
Required and optional packages

Package	Required by ITG?
Basic Alternate Route Selection (BARS, package 57)	Required if package 58 is not equipped.
Network Alternate Route Selection (NARS, package 58)	Required if package 57 is not equipped.
Coordinated Dialing Plan (CDP, package 59)	Optional if this dialing plan is used
Flexible Numbering Plan (FNP, package 145)	Optional if this dialing plan is used
Fast TDS package (package 87)	Optional. Systems with older TDS cards (not systems with XCTs) will experience faster call setup times with this package equipped.

List of ITG components

Table 2 lists ITG components.

Note: MAT 6.1 or later, including the Common Services, Alarm Management, and Internet Telephony Gateway applications, is a pre-requisite and must be ordered separately.

Table 2
List of ITG components

Component	Code
ITG Large and Small System Package (8 port ITG card with pre-installed software, Keycode, required cables, NTP)	NTZC12CA A0796708
Meridian Internet Telephony Gateway ITG Platform (ITG card, Keycode, pre-installed software)	NTZC13BA A0796709
Spare Meridian Internet Telephony Gateway ITG card (no Security Device or Keycode included)	NTCW80CA A0787501
PC card (optional)	NTZC14AA A0745182
Meridian Internet Telephony Gateway (ITG) Trunk 1.0/Basic Per-Trunk Signaling NTP	P0905051
ITG Cables	
Shielded backplane to 2 x RJ45 and D-subminiature communications port cable	NTMF94DA A0782238
ITG Faceplate Maintenance Port cable	NTAG81CA A0655007

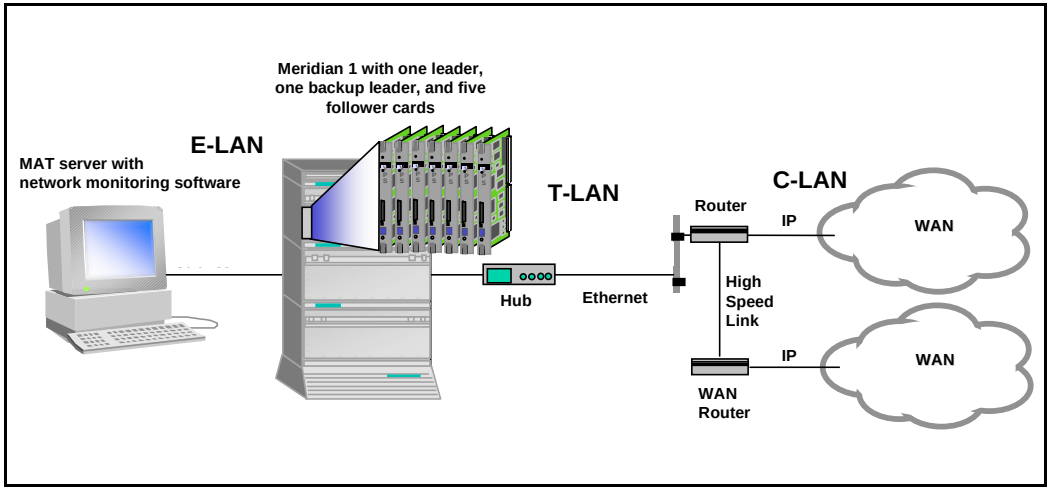
Basic ITG system setup

Figure 1 shows an example of a basic recommended ITG system setup, with separate voice and management networks. Throughout this document, the terms T-LAN, E-LAN, and C-LAN are used to distinguish between different parts of the network:

- *T-LAN* refers to the Telephony LAN and carries the ITG voice traffic.
- *E-LAN*, the embedded LAN, refers to the management LAN.
- *C-LAN* refers to the customer equipment beyond the router.

This is for illustrative purposes, and is not necessarily the setup you must use.

Figure 1
Basic setup of the ITG system



Dialing plan support

Dialing plan configuration allows the customer to set up the routing tables to route calls to appropriate destinations based on the dialed digits. The dialing plan is configured through the Electronic Switched Network (ESN) feature by using the overlays or MAT, as well as configuration of ITG card Address Translation through the MAT ITG application.

ESN configuration allows the Meridian 1 to route outgoing calls to the ITG card while Address Translation configuration allows ITG card call processing to translate the called party number to the IP address of the terminating node and to deliver calls to the destination via the IP network. Refer to the "Add ITG configuration data on a Meridian 1" on page 161 for details on ESN configuration and refer to "Create the ITG Dialing Plan on MAT" on page 133 for configuration of the Address Translation by the MAT ITG Dialing Plan.

ITG supports the following dialing plans:

- the ESN private network dialing plan with CDP (Coordinated Dialing Plan) and UDP (Uniform Dialing Plan),
- the North American dialing plan, and
- the Flexible Numbering Plan.

Customer-defined BARS and NARS access codes, such as AC1 and AC2 are used to access different dialing plans.

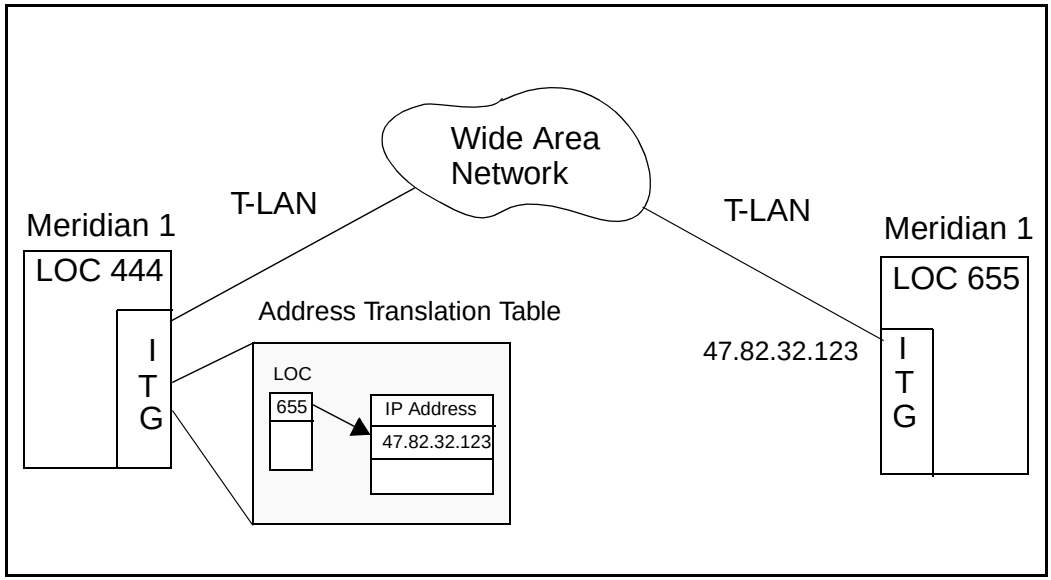
ESN private network dialing plan

The Meridian 1 Electronic Switched Network (ESN) feature provides two different dialing plans for private networks: the Uniform Dialing Plan (UDP) and the Coordinated Dialing Plan (CDP).

Uniform Dialing Plan (UDP)

The UDP format consists of a location code and a DN, such as 655-7486. The first three digits represent the location of the node, and the remaining digits represent the directory number of the set. Each node in the ESN private network will have a unique location code. UDP can be used to set up the a private network with nodes in different locations. Figure 2 shows a Uniform Dialing Plan ITG setup:

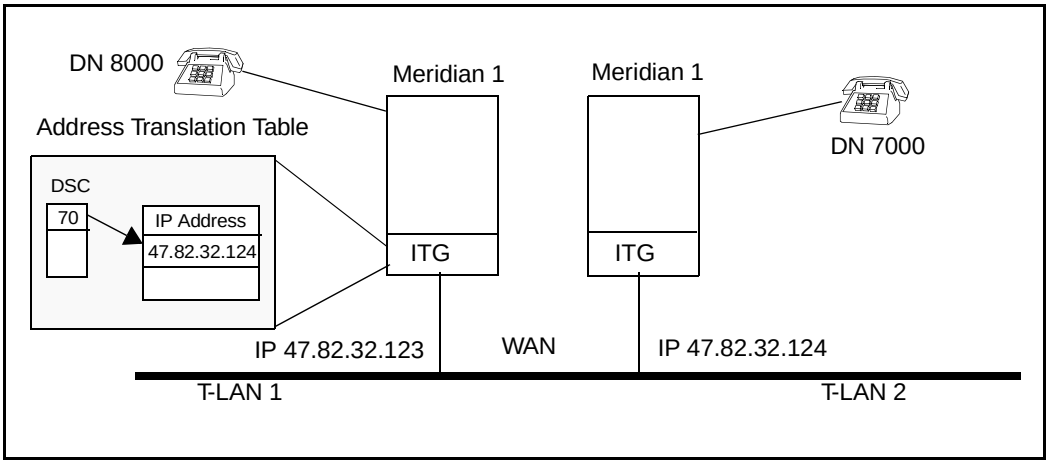
Figure 2
Uniform Dialing Plan ITG setup



Coordinated Dialing Plan (CDP)

The Coordinated Dialing Plan (CDP) can be configured to use a Trunk Steering Code (TSC) or Distance Steering Code (DSC). This dialing plan allows users to call any other telephone within a CDP group by dialing 3 to 7 digits. This plan is used to set up a private network within the same site with more than one ITG node. Figure 3 shows a Coordinated Dialing Plan setup:

Figure 3
Coordinated Dialing Plan ITG setup

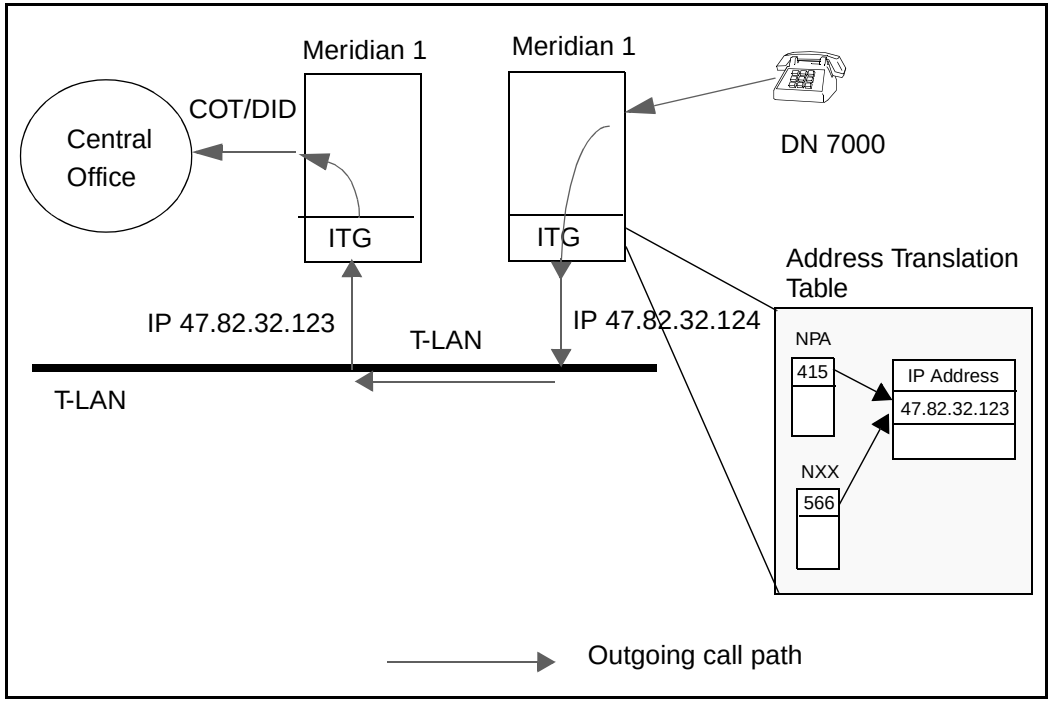


North American dialing plan

This dialing plan allows users to make public network calls via the private IP network. However, calls are not directly routed to the Central Office through the LAN connection. Instead, calls from the T-LAN are routed through a tandem switch that has regular trunk connections to the CO.

Figure 4 shows DN 7000 making a public call by dialing 1-415-456-1234 or 566-1234 via the T-LAN. The ITG card with IP address 47.82.32.124 searches for the NPA or NXX tables for the matched NPA or NXX entries. Once an entry is found, the corresponding IP address will be used to send H.323 call setup messages to the gateway (Meridian 1 with IP address 47.82.21.123) which will route the call to the PSTN through a regular CO or DID trunk.

Figure 4
North American dialing plan - call flow



Flexible Numbering Plan (FNP)

Flexible Numbering Plan (FNP) allows any station within the network to be represented by a flexible number of digits up to a maximum of 10 digits. It also allows flexibility for the length of the location codes from node to node. It can be used to support country-specific dialing plans, such as in Asia or Europe.

ITG card functional description

Leaders, Backup Leaders, and followers

Each Meridian 1 system can have one or more ITG cards. An ITG card may be either a Active leader, a backup leader, or a follower. Each customer in a Meridian 1 system has only one ITG card that is a Leader card, may have one card that is a Backup Leader card, and may have one or more ITG cards that are follower cards. There can be multiple ITG nodes per customer.

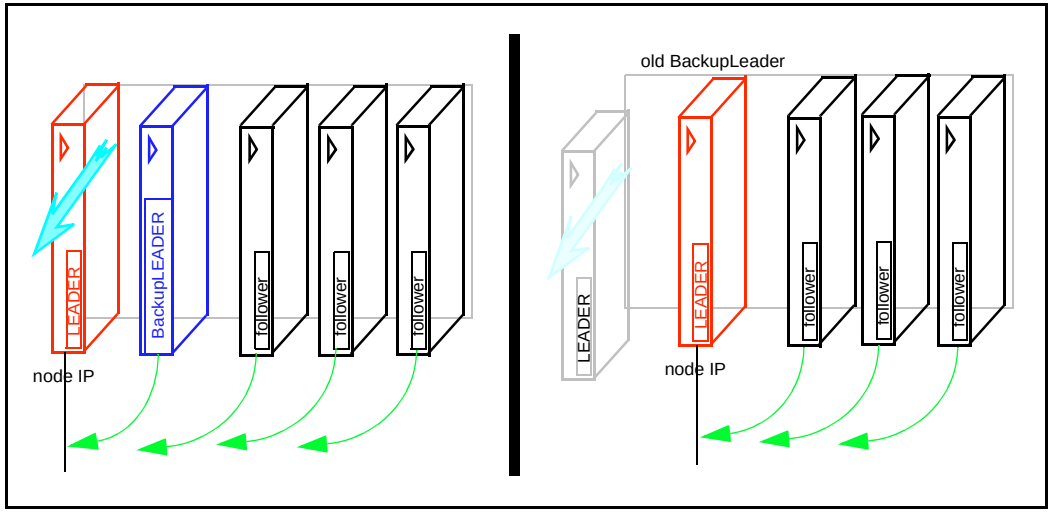
A active leader card is a designated ITG card that is a point of contact for all other Meridian 1 systems in the network. The backup leader card is a special case of a leader card that acts as a follower until the active leader goes out of service, then steps in to become the active leader.

The “Node IP” address is the address used by the ITG cards to communicate with the active Leader.

In order to support the hot standby/switch-over feature we designed the cards to have card roles (active leader, backup leader, or follower). These roles will be used to distinguish an active system/stand-by system and client system. The active leader will have a “Node IP” address on the voice interface. This “Node IP” is an aliased IP which is added to the original IP address on the voice interface. This “Node IP” will be used to keep track of the active leader by other machines on the network. The active leader and backup leader will exchange the “Node IP” when the active leader goes out of service, as shown in Figure 5.

The backup Leader sets up a heartbeat with the active Leader card’s Node IP address and if that IP address is not responding, the backup Leader becomes the active Leader by assigning the Node IP to its voice interface. The backup Leader has become the active Leader within 4-7 seconds.

Figure 5
Switch-over of "Node IP" address from active leader to backup leader



In the MAT ITG application, the term Leader 0 refers to the ITG card that is initially configured to perform the role of the active Leader. The term Leader 1 refers to the ITG card that is initially configured to perform the role of the backup Leader. Thereafter, the term active leader denotes the Leader 0 or the Leader 1 card that is performing the active leader role.

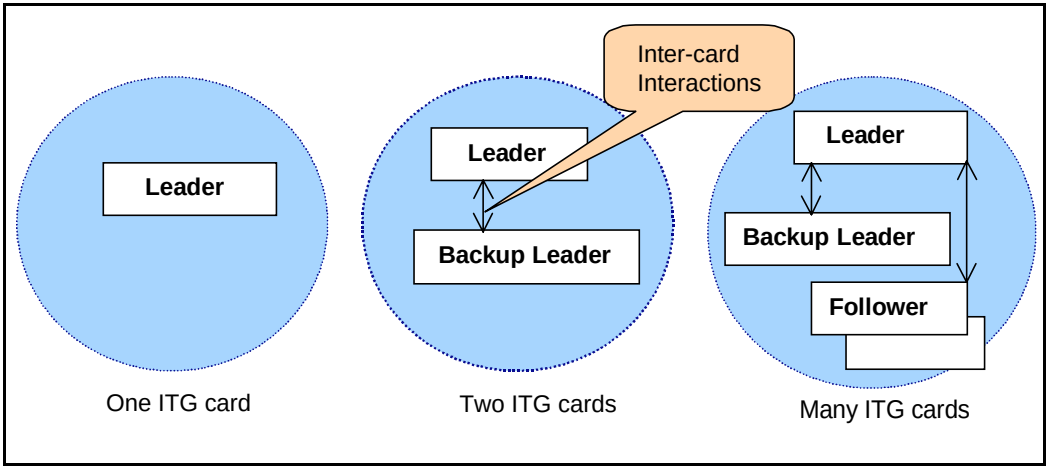
Figure 6 shows the interactions between Leader, Backup Leader, and follower cards.

Leader card functionality

The Leader card performs the following tasks:

- Distributing incoming IP calls to each registered card in its node, while load balancing amongst the registered cards.
- Network performance monitoring for outgoing calls in its node, and
- Assignment of IP addresses for other cards in its node,
- Time server for all other ITG cards in its node,

Figure 6
Leader, Backup Leader, and follower interactions



The backup leader also runs these tasks but they are not used by the followers unless the Leader's heartbeat is lost and the backup Leader becomes the active Leader.

All calls from a remote Meridian 1 ITG node are presented to the active leader card. The active leader card consults its internal follower card resource table and selects the follower card that has the smallest number of calls to receive the new call. It sends a message to that follower card to reserve a channel for the call, and redirects the call to the follower.

Leader and follower card interaction

The active leader card controls the assignment of IP addresses for all the ITG cards in the ITG node. In the event a new ITG card is added, the new card's MAC and IP address configuration data, as programmed in MAT, will only need to be transmitted with the Node Properties to the active leader card. When it boots up, the new follower card will send a bootp request containing its MAC address and will receive its IP addresses and card index from the active leader card via bootp protocol.

When follower cards boot up, they get their IP addresses for the voice and management interfaces, and the Node IP address that they use to communicate with the active leader card (Leader 0 or Leader 1).

The active leader card continually sends messages to its follower cards about changes in the network performance for each destination node in the dialing plan.

All the follower cards continually send Update messages to the active leader card that inform the active leader card of their most recent status and resources.

If a follower card fails (e.g., a DSP failure) it will report the unavailability of the failed resources to the active leader, and the particular trunk ports involved will be considered to be faulty and will appear busy to the Meridian 1. Meridian 1 call processing is maintained on the remaining ITG trunks.

If a follower card loses communication with the active leader, it will make all its ports appear busy to the Meridian 1. Alarms will be raised by sending an SNMP trap to the IP addresses in the SNMP manager list.

Leader 0 and leader 1 redundancy interactions

Whenever a leader card reboots, it sends bootp requests to determine whether an active leader card is present. If it receives a bootp response, the rebooting leader card becomes the backup leader. If it does not receive a response, the rebooting leader becomes the active leader. Leader 0 sends bootp requests for a shorter time than leader 1, therefore leader 0 will normally become the active leader.

Leader 1 normally boots as a follower card when it is first installed in a node. Upon receiving a bootp response from the initial active leader (Leader 0), the Leader 1 card discovers its identity (card role and card index), sets itself as a leader, and automatically reboots itself. Similarly, if Leader 0 card fails and is replaced, the replacement card normally boots as a follower card when it is first installed in the node. Upon receiving a bootp response from the active leader (Leader 1), the Leader 0 card discovers its identity, sets itself as a leader, and automatically reboots itself.

The Leader 0 and Leader 1 cards keep their node properties synchronized. The backup leader obtains a copy of the “bootp.1” file, containing the bootp table from the active leader upon bootup and whenever node properties are downloaded to the active leader. Critical synchronized data includes the card role and card index, management interface MAC address, the node IP address, the E-LAN and T-LAN gateway IP addresses, the individual card IP address, and TN for all ITG cards in the ITG node.

The backup leader card monitors the active leader card’s sanity by pinging the active leader card’s “Node IP.” The active leader’s heartbeat is the ping response.

In the event of an active leader card’s failure (the active leader is not responding to the pinging of the Node IP address by the backup leader), the backup leader card takes over as the active leader card by assigning the “Node IP” to its voice interface, and announces its leadership to all the follower cards. The followers will then re-register with the new active leader card and, as a result, a new Resource Table is built almost instantaneously on the new active leader.

In the event of backup leader failure, the active leader card will generate an SNMP trap to the management station, MAT, indicating this failure.

Leader card maintenance

If maintenance is being performed on both the active leader and the backup leader, the entire ITG node will be unable to route IP traffic over the IP network.

ITG card physical description

The ITG card plugs into the Meridian 1 IPE shelf. A maximum of eight cards can fit on one IPE shelf or five card per shelf for Meridian 1 option 11C, and 11E systems; each ITG card takes up two slots on the IPE shelf. The ITG cards have an ethernet voice port on the faceplate, and management ethernet on the backside of the shelf. Ethernet is the only supported interface at this time. The ITG card has a serial port connection on the faceplate as well as on the I/O backplane (although only one of these connections can be made at a time), so that a TTY can be connected via an NTAG81CA cable and the ITG shell command line interface can be accessed.

The ITG card consists of a motherboard with the addition of a DSP daughterboard connected via a PCI interconnect board that connects to PCI connectors on the two boards. The DSP daughterboard consists of DSP sections, each connected to 128 Kwords of high speed SRAM.

The core ITG processor is an Intel x86 processor, interfaced to the rest of the system via an Intel 82420 PCI chipset. The ITG card has 16MB of DRAM memory, as well as 4MB of file storage flash memory, 4MB of application flash memory, and 512 Kbytes of BIOS flash memory that loads the application memory.

The are no switches or jumpers to be configured on the ITG card.

Figure 7 shows the how the ITG card is assembled, with a PCI interconnect board connecting the ITG motherboard and DSP daughterboard.

CAUTION

The PCI Interconnect Board is polarity sensitive, and is not physically keyed. There is an “M/B” marking on the PCI Interconnect Board and an arrow that should point toward the motherboard. Inserting the PCI Interconnect Board in the wrong way may cause damage.

Figure 7
ITG card assembly

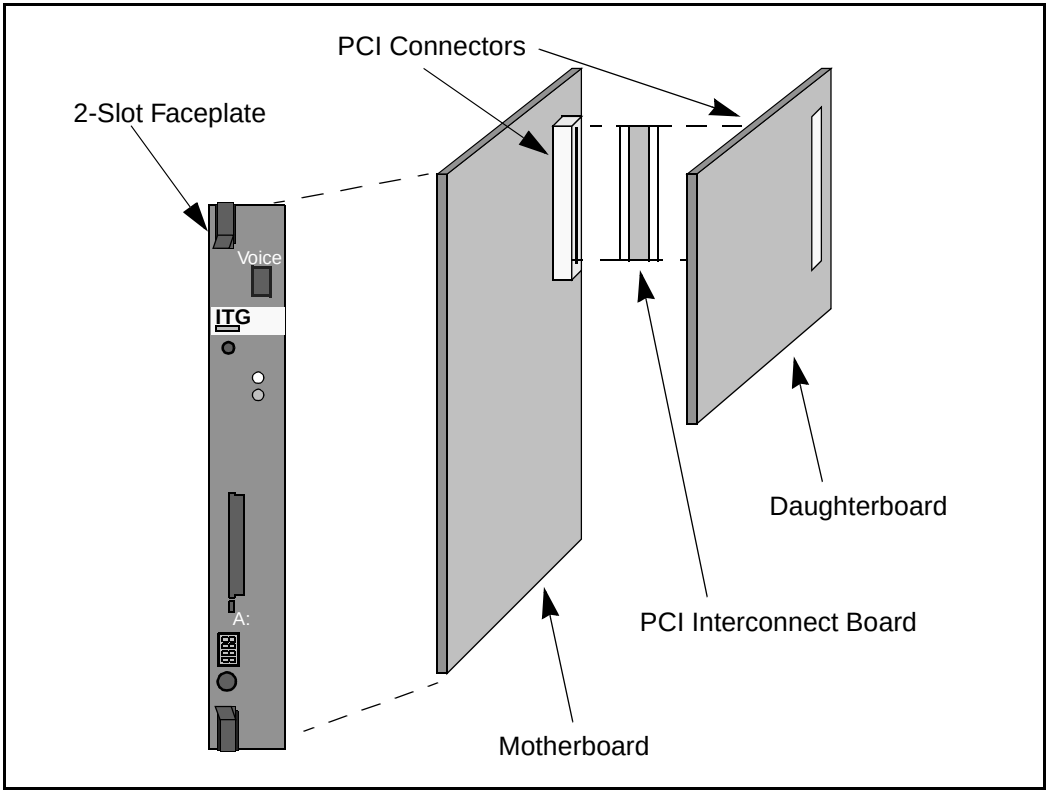
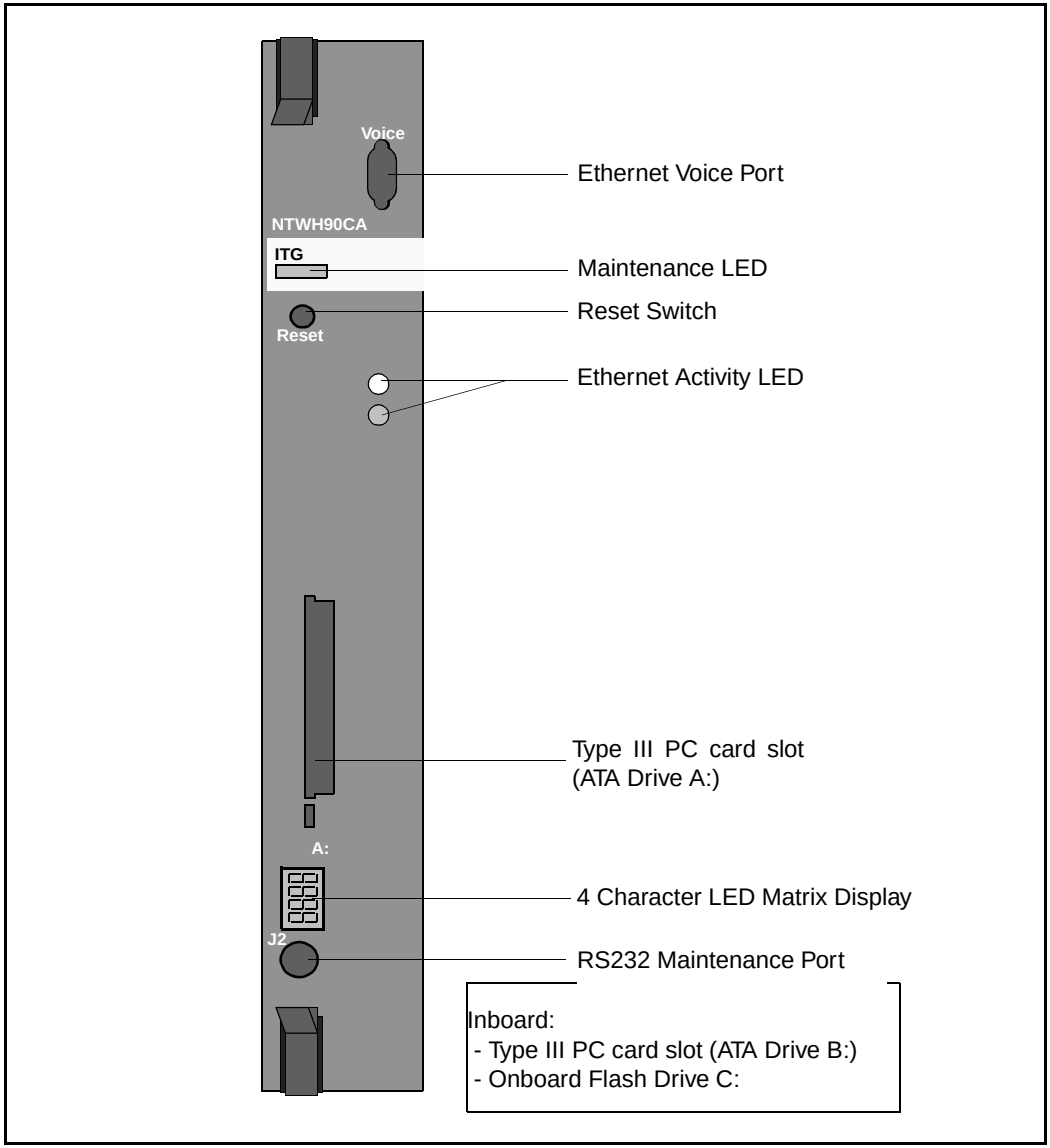


Figure 8 shows a faceplate view of the ITG card:

Figure 8
ITG card faceplate



PC cards

The ITG card has two PC card slots. It has one PC card slot on the faceplate (designated drive A:) and one inboard slot (designated drive B:). It supports PC based hard disks (ATA interface) or high-capacity PC flash memory cards for mass storage.

Supported interfaces

Table 3 is a summary of the interface types supported on an ITG card:

Table 3
Interface summary

Interface	Number of connections
DS-30X	1
Card LAN	1
Enhanced IDE	1 (see Note)
PC card (Standard)	2 Type III
Ethernet	2
Maintenance RS-232	2

Note: This interface is part of the ITG card architecture, but is not yet supported.

ITG card Security Device

The ITG card requires a Security Device before it will allow the entry of keycodes to enable the features available on the card. The Security Device will come pre-installed on the ITG card motherboard for new system orders (refer to “List of ITG components” on page 18). The spare part ITG card (NTCW80CA) does not include a Security Device or a Keycode. Attached to the Security Device is a tab that will facilitate removal of the Security Device in order to transfer it to a spare card when replacing a failed card.

Figure 9 shows the ITG Security Device. Figure 10 shows the location of the Security Device on the ITG card motherboard:

Figure 9
ITG card Security Device

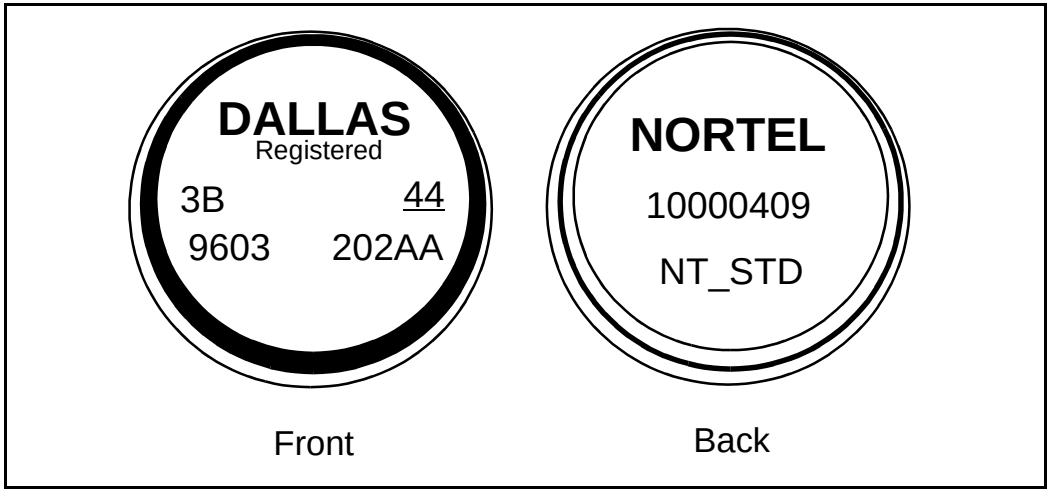
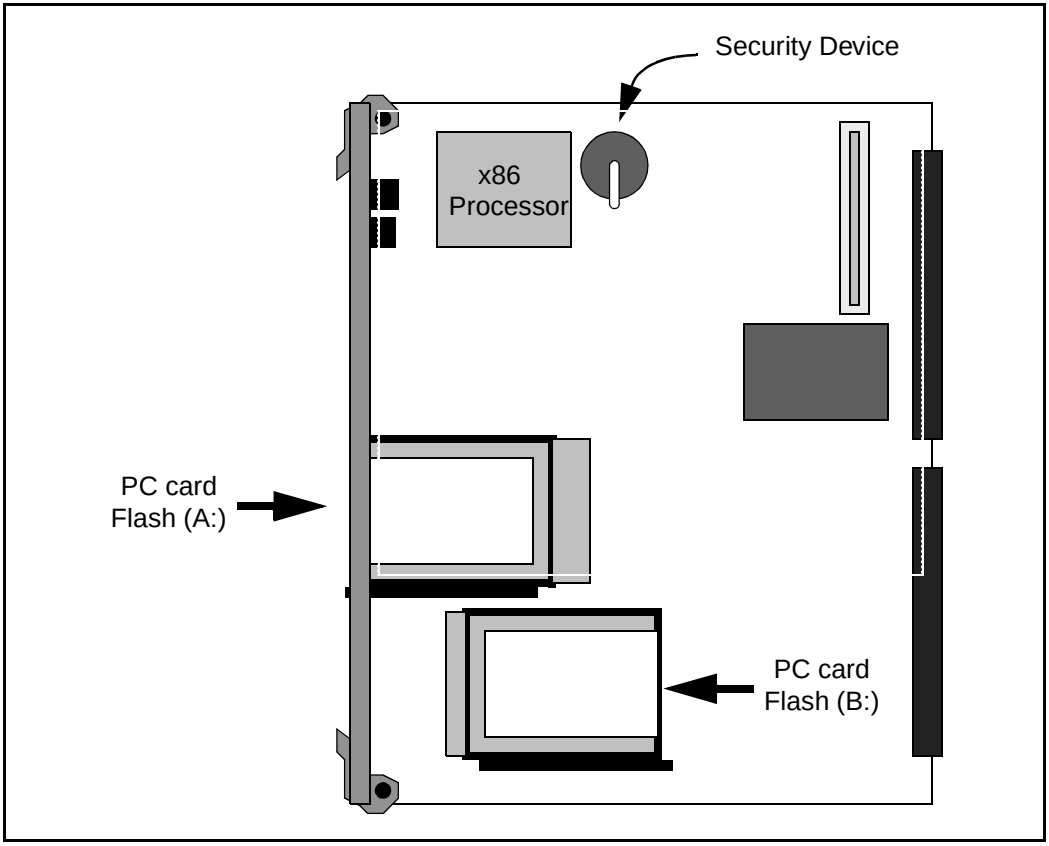


Figure 10
ITG card Security Device location - beneath the daughterboard



ITG card software upgrades

Two types of upgrade are possible for the ITG card, those requiring keycodes and those not requiring keycodes. All upgrades are performed by updating the on-board flash memory. The new card software is normally downloaded from the MAT ITG application. If MAT is temporarily unavailable, then the ITG shell command-line interface can be used. The specific types of ITG card software upgrades available are described below:

Upgrades requiring keycodes

Upgrades for new optional features that are purchased by the customer require new keycodes. The customer obtains the new software from the ITG software website, and installs it on the ITG card. However, the newly purchased features cannot be used until a new keycode is installed.

Upgrades not requiring keycodes

For a maintenance or bug fix upgrade, no keycode is required. The user installs the new software from the network or the PC card. The existing keycode is reused.

Downloading the ITG software from the ITG web site

The Internet World Wide Web address, or URL, where ITG software can be downloaded is *https://www.nortel.com/secure/cgi-bin/itg/enter.cgi*

Upon accessing this site, enter the username and password.

Select the download option, select which software load to download, and select the location on your PC where the file is to be saved. Normally the software would be downloaded to the MAT PC. However, it can be downloaded to any PC, and made available on an FTP server, or copied to a PC card.

MAT

The new card software is normally downloaded from the MAT ITG application. The MAT ITG application allows you to automatically download ITG software to all cards in a node, or to selected cards.

ITG shell command-line interface

If MAT is temporarily unavailable, the following ITG shell command-line interface can be used to upgrade the ITG card software.

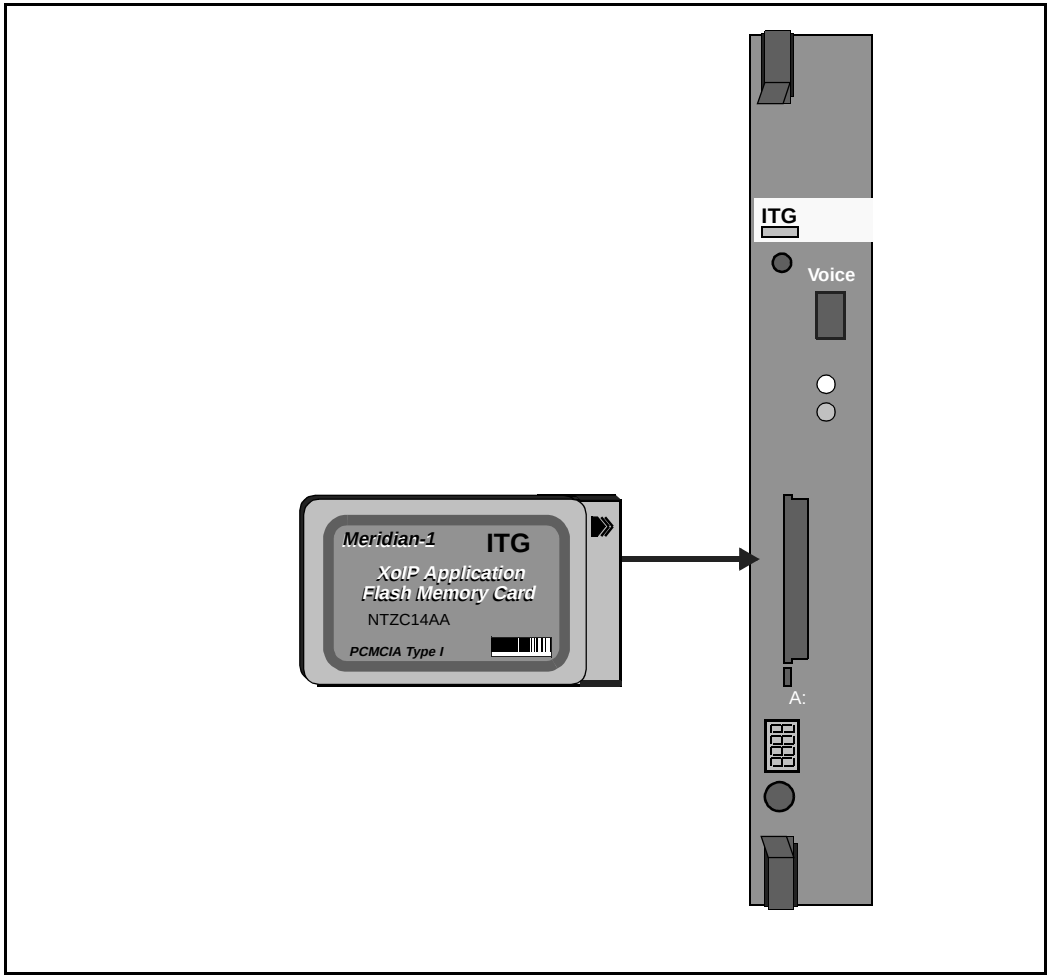
Network installation of ITG card software

The ITG card software can be downloaded from an FTP server over the IP network to the ITG card flash memory by invoking the **swDownload** command from the ITG shell. The ITG card will need to be rebooted in order to run the new software.

Software upgrade from PC card

An upgrade may be performed by inserting a PC card into the drive A: PC card slot on the ITG card faceplate, as shown in Figure 11. The PC card must have the binary application file on a DOS file system. The upgrade is invoked from the ITG shell. The ITG card will need to be rebooted in order to run the new software.

Figure 11
PC card installation



ITG card backup and restore procedures

The ITG card supports backup and restore procedures for critical configuration data. In the event that a failed ITG card is replaced by a spare, the dialing plan tables, DSP configuration, passwords, keycode, and other configuration data will normally be restored from the MAT ITG network management application.

The Meridian Administration Tools (MAT) application has its own backup and restore procedure for all data that is downloaded from/to the ITG card. If MAT is temporarily unavailable, then the ITG shell command-line interface can be used to retrieve the configuration files from an FTP server or from a PC card.

All of the 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 the user selects the Disaster recovery option in the "MAT Backup Wizard." This option backs up all MAT data and can only be used to restore all data, including the ITG configuration data.

[The user has the option of copying the MAT ITG database file manually. This file can then be restored to any MAT PC thereby providing both a backup and data transfer mechanism. The file is located in the MAT directory at \Nortel\Common Data\Mix\MIX.mdb. The OM reports are also stored there.

> ***Note:*** This procedure is not practical unless we can also manually copy the MAT site and system database.]

Log files, such as Alarms and Trace files, are written to flash memory on the card, but they are not automatically uploaded to the MAT ITG application. They can be manually uploaded, displayed, and saved, but they cannot be restored to the replacement ITG card. Operational measurement (OM) files are written hourly to the flash memory on the ITG card. The MAT ITG application can be scheduled to retrieve the OM files automatically in order to generate reports. OM files are normally not restored to a replacement card.

Maintenance

Fault clearance procedures are described below for the DSPs on the ITG card, and for the ITG cards themselves:

DSP failure

If one of the DSPs on the ITG card fails to respond to the main CPU, a DSP reset will be automatically initiated and a “dspResetAttempted” alarm will be raised. If the DSP fails to recover after the reset, a “dspResetFailed” alarm will be raised and that DSP will be marked as unusable. Call processing will be maintained on the remaining ITG card ports.

ITG card failure

Following a reboot, if an ITG card displays a code of the form F:xx on the faceplate hex display this indicates an unrecoverable hardware failure and the card will not register with the Meridian 1.

The card should first be removed for 2-3 seconds and then re-seated in the IPE shelf. If the failure persists, the card must be replaced.

Power loss

Since the ITG card is based on Flash EPROM technology, all configuration data is preserved for 10 years, so there is no requirement for battery backup. The ITG card may even be removed from the IPE shelf indefinitely and still retain all configuration.

Network Quality of Service (Qos)

ITG uses a method similar to ITU-T Recommendation G.107, the E-Model, to determine the voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating “R” for the network transmission quality. The model further correlates the network objective measure, “R”, with the subjective QoS metric for voice quality, MOS or the Mean Opinion Score. This model serves as an effective traffic shaping mechanism by invoking the *Fallback to Circuit-Switched Voice Facilities* feature to avoid quality of service degradation.

Network monitoring

The ITG network monitoring function exchanges UDP probe packets between active leader cards at all configured nodes to collect the network statistics for each remote location. All the packets make a roundtrip from the Sender to the Receiver and back to Sender. From these three pieces of information the latency and loss in the network for a particular location are calculated.

It may take about 3 minutes before the ITG network monitoring function reacts to marginal changes in the network condition. Fallback can be due to any of the following reasons:

- Bad network conditions.
- The remote node is dead.
- An ethernet cable is unplugged.
- The far end does not have the near end IP entry in its dialing plan table.

Note 1: Quality of Service is not supported for non-M1 remote locations and must be disabled.

Note 2: A single Quality of Service threshold is configurable per destination node. If there are multiple dialed digit translations per destination node the Quality of Service configuration for the last digit translation entered will apply.

Note 3: Fallback is per codec type per remote destination.

Note 4: The Fallback decision is made only at the originating node using the QoS thresholds configured at the originating node for the remote node.

Note 5: The dialing plan database must contain the IP addresses correlated to a set of dialed digits, or else the node will be in fallback.

For good voice quality, the ITG cards will reassemble the voice packets in an ordered continuous speech stream and play it out at regular intervals despite varying packets arrival times.

ITG allows for manual configuration of QoS thresholds depending on the customer trade-off between cost and voice quality. The *ITG Engineering Guidelines* provide the necessary guidelines to effectively weigh the trade-off and determine the quality of service that can be supported for any given network.

Quality of service parameters

Quality of Service for both voice and fax is largely dependent on end-to-end network performance and available bandwidth. A number of parameters determine the ITG voice Quality of Service (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 high delay and congestion. In a voice conversation, packet loss is heard as gaps in the conversation. Some packet loss, less than 5%, may be acceptable without too much degradation in voice quality. Sporadic loss of small packets may 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 the more manageable delay, since fixed delay is dependent on the network technology itself. Variable delay is caused by the particular network routing of packets. The ITG node should be as close as possible to the network backbone (WAN) with a minimum number of hops, to minimize packet delay and maximize voice quality. ITG provides echo cancellation so that delay up to 200 ms may be acceptable.

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 to assemble voice packets received at irregular intervals into a continuous voice stream.

Fallback to circuit-switched voice facilities

Fallback due to network monitoring

As discussed under "Network Quality of Service," *Fallback to circuit-switched voice facilities* is invoked when Network Quality of Service falls below the configured threshold for about 3 minutes, as determined by the ITG network monitoring function. This will occur even when there is no call traffic through the ITG node.

Fallback due to call setup failure

Fallback to circuit-switched voice facilities is also invoked during call processing when any of the following conditions block call setup:

- A call setup message is rejected by the destination ITG node,
- There is no response to a call setup message

Note: There is no fallback in case of failing the digit translation in the ITG dialing plan table.

Network performance utilities

Two common network performance utilities, Ping and Traceroute are described below. Other utilities can be used to find more information about the ITG network performance.

Note 1: Since network conditions can vary at different times, collect performance data over at least a 24 hour time period.

Note 2: Performance utilities should be used to measure network performance from each ITG node to every other ITG node.

Ping

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

Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine 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 throw away the packet *and* return to the originating IP address an ICMP “time exceeded” message. 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 will send back a “time exceeded” message. This identifies the first router on the route. Then trace route sends out a datagram with a TTL of 2. This will cause the second router on the route to return a “time exceeded” message and so on until all hops have been identified. The trace route IP datagram will have an UDF Port number unlikely to be in use at the destination (usually > 30,000). This will cause the destination to return a “port unreachable” ICMP packet. This identifies the destination host. Traceroute can be used to measure roundtrip times to all hops along a route, thereby identifying bottlenecks in the network.

Codecs

The term codec refers to the voice coding and compression algorithm used by the Digital Signal Processors (DSPs) on the ITG 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 craftsperson can configure a preferred codec, via the MAT ITG application, for making outgoing IP calls for each ITG card.

ITG supports the following codecs:

G.711

This codec delivers “toll quality” audio at 64 kpbs. This codec is optimal for speech since it the smallest delay, and is very resilient to channel errors. However, it consumes the largest bandwidth.

G.729

The G.729 codec allows the ITG card to support only 4 ports. When using G.729 and using NT8D14 Universal Trunk (EXUT) card emulation, only trunk units 0, 1, 4, and 5 are configured.

G.729A

This is the default and preferred codec for ITG. Provide near toll quality at a low delay. Uses compression to 8 kbps (8:1 compression rate).

G.723.1

Provides the greatest compression, 5.3 kbps or 6.3 kbps.

An ITG card will have one of three downloadable DSP images that support the codecs described in Table 4.

Table 4
Codecs supported by ITG Release 1.0

Image 1	Image 2	Image 3
PCM A-law (G.711)	PCM A-law (G.711)	PCM A-law (G.711)
PCM Mu-law (G.711)	PCM Mu-law (G.711)	PCM Mu-law (G.711)
G.729A	G.723 5.3 kbps	G.729
Clear Channel	G.723 6.3 kbps	Clear Channel
FAX	Clear Channel	FAX
	FAX	

ITG card OA&M

The ITG OA&M access is provided through three different means: the MAT Internet Telephony Gateway application, the ITG shell command-line interface, and existing Meridian 1 system management interfaces (MAT GUI, especially the Maintenance Windows, or the Service Change and Maintenance Overlays the MAT system terminal passthru or direct TTY connection.

MAT ITG application

The majority of ITG system management procedures are performed through a MAT PC running the ITG application. The MAT ITG application is accessed by clicking the “Internet Telephony Gateway” icon in the “MAT Navigator” window in the “Services” folder.

ITG shell command-line interface

The ITG shell command line is normally accessed from the MAT ITG application by invoking the “Telnet to the card” from the **Maintenance|Card** menu.

The ITG shell command-line interface can also be accessed by connecting the COM port of a PC running a TTY or VT-100 terminal emulation program to the maintenance port on an ITG card via an NTAG81CA Faceplate Maintenance cable. Alternatively, you can connect to the maintenance port via the female DB9 connector on the NTMF94DA I/O Panel Ethernet and Serial Adaptor cable assembly, using the NTAG81BA Maintenance Extender cable.

Once connected via Telnet or RS-232 cable, the ITG shell command-line interface is available. The ITG shell is used initially to program the IP address of the Leader 0 ITG card during ITG node installation. Also, certain ITG administration, maintenance, and file transfer commands are available.

Meridian 1 system management commands.

The ITG card uses a subset of the existing Meridian 1 system management commands and diagnostic messages used for the NT8D14 Universal Trunk (EXUT) card. Route Data Block (RDB), ESN data blocks, and CPND data blocks must also be configured for ITG using the appropriate Meridian 1 service change overlays, as described in the *Installation and configuration* section

The Meridian 1 ITG OA&M tasks are described in the *Installation and configuration*, *Administration*, and *Maintenance* sections.

A list of ITG shell commands and Meridian 1 system commands is described in the *Installation and configuration* and *Maintenance* sections.

Alarm Notification

ITG uses the MAT Alarm Notification application which can receive SNMP traps from any recognized network-connected device. Received traps are displayed in an event browser. The user can write scripts to generate notification messages to pagers, e-mail, and SNMP network management systems. Figure 12 shows the Event List which shows alarms with severity ratings and Figure 13 shows the Event Properties window which gives details on a particular alarm. Each ITG card must be configured to send SNMP traps to the MAT PC and the local modem router on the E-LAN.

The Meridian 1 can be configured to send SNMP traps to the MAT Alarm Notification application so that ITG alarms can be viewed in the context of Meridian 1 alarms. MAT Alarm Notification can be scripted to write all alarms to a text file on the MAT PC. The text file can be viewed with any text file browser or editor. The text file can provide a non-volatile log of alarms for all ITG cards and Meridian 1 PBXs in the same context.

For more details, refer to the *MAT Alarm Notification User Guide.*

We have third party solutions for Remote Access to Alarm Notification. The reader is requested to consult product bulletins for more information.

Figure 12
MAT Alarm Notification Event List

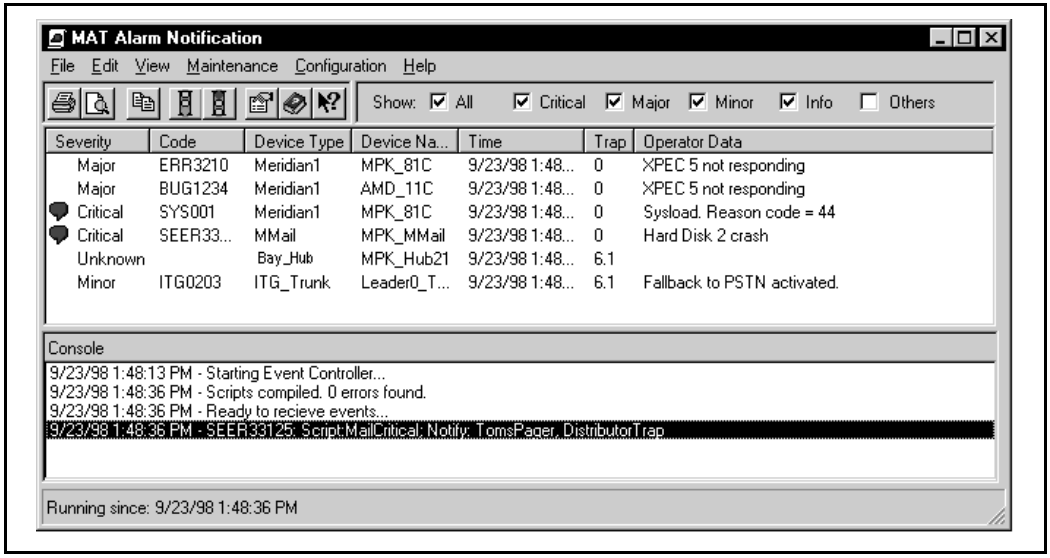
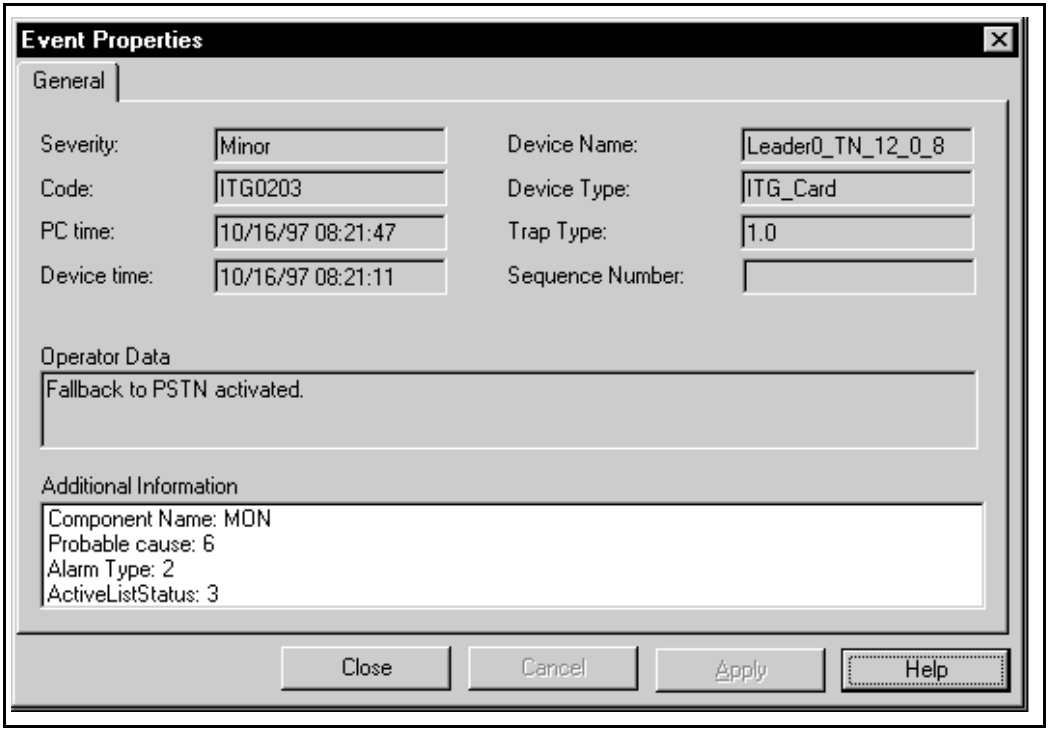


Figure 13
Event Properties window



ITG Trunk 1.0 engineering guidelines

The Meridian Internet Telephony Gateway (ITG) Trunk 1.0 application compresses PCM voice, demodulates Group 3 fax, and routes the packetized data over a private internet, or intranet, to provide virtual analog non-ISDN TIE trunks between Meridian 1 ESN nodes. Communications costs may be reduced as voice traffic is routed at low marginal cost over existing private IP network facilities with available under-utilized bandwidth on the private Wide Area Network (WAN) backbone.

The ITG is targeted at the enterprise customer who already has both a Meridian 1 system in place for providing corporate voice services, as well as an intranet for corporate data services. Such a customer is expected to use the ITG system to migrate traffic from a PSTN-based network to the intranet. In doing so, voice and fax services which traditionally relied on circuit-switched and Time Division Multiplexing technology will now be transported using packet-switched and statistical multiplexing technology.

This document provides guiding principles for properly designing a network of ITG nodes over the corporate intranet, describe how to qualify the corporate intranet to support an ITG network, and decide what required changes are needed in order to preserve the quality of voice services as much as possible when migrating those services from the PSTN. It addresses requirements for the successful integration with the customer's existing local area network (LAN). By adhering to these guidelines the designer should be able to engineer the ITG network so that the cost and quality tradeoff is at best imperceptible, and at worst within a calculated tolerance.

Audience

This document is addressed to both telecommunications and datacom engineers who are going to design and implement the ITG network. It is assumed that the telecommunications engineer is familiar with engineering

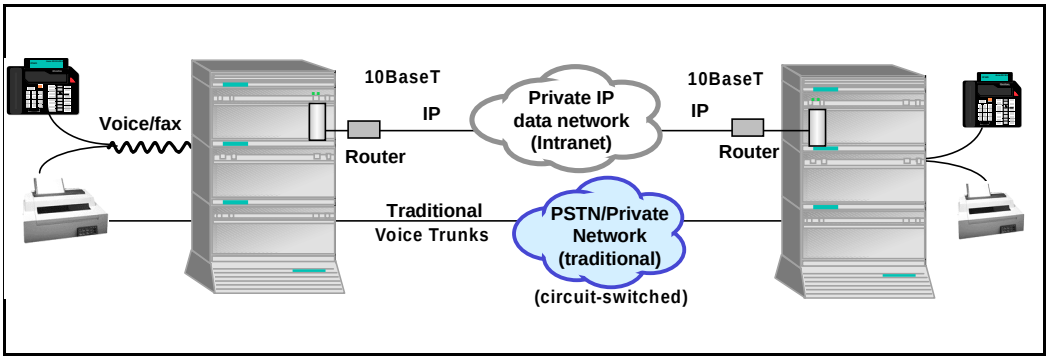
the Meridian 1, and obtaining system voice and fax traffic statistics. It is assumed that the data communications engineer is familiar with the intranet architecture, LAN implementations, tools for collecting and analyzing data network statistics, and data network management systems. The term "technician" used in this document refer to the person in either the telecommunications or data communications engineering role.

ITG system

The ITG system is designed to work on an adequately provisioned, stable LAN. Delay, delay variation or jitter, and packet loss must be minimized end-to-end across the LAN and WAN. The technician must carefully determine the design and configuration of the LAN and WAN that link the ITG system. If the intranet becomes congested, new calls to the ITG system will fall back to traditional circuit-switched voice facilities so that the quality of service is not degraded for new calls.

The ITG product is for intranet use only, providing virtual analog TIE trunks between two Meridian 1 systems in an ESN network, as shown in Figure 14.

Figure 14
The Meridian Internet Telephony Gateway intranet



The ITG system is available for options 11E, 11C, 21E, 51, 51C, 61, 61C, 71, 81 and 81C systems running X11 release 21 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 11E and 11C systems can hold five cards in the main cabinet, and an additional five cards in an expansion cabinet. An option 11C or 11E system can have up to two expansion cabinets.

The ITG card has two 10BaseT Ethernet ports; one that is located on the faceplate carries Voice over IP (VoIP) traffic and connects to the Telephony LAN (T-LAN); another that is located on the card backplane I/O connector carries ITG system management traffic and connects to the Embedded LAN (E-LAN).

Electromagnetic Compatibility (EMC)

The ITG Trunk 1.0 card is approved for CISPR 22 Class A (and FCC Part 15 Class A) limits and approved to CISPR 22 Class B limits, resulting in compliance to CISPR 22 Class A by default.

For specific information on card placement, turn to See “Physical placement of the cards” on page 139..

Scope

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

- ITG nodes
- Telephony LANs (T-LANs) on which the ITG nodes are attached to
- A corporate intranet which connects the various T-LANs together

The guidelines assume that the Enterprise customer already 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 rely on voice services such as Local Exchange Carrier (LEC, including FAX) and Inter-Exchange Carrier (IXC) private lines. With ITG technology, the Meridian 1 can now choose a new kind of delivery mechanism, one that uses packet-switching over a data network, specifically a corporate intranet. The role of the ITG node in this regard is essentially to convert steady-stream digital voice into fixed-length IP packets.

In the data world in the late 1960s, IP evolved from a protocol that allowed multi-vendor hosts to communicate with each other. The protocol adopted packet switching technology, thereby providing bandwidth efficiency. 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, primarily delay, delay variation, and error, 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, whereas delay variation and packet errors causes introduces glitches in conversation. Simply connecting the ITG nodes to the corporate intranet without preliminary assessments may result in unacceptable degradation in the voice service; instead proper design procedures and principles must be considered.

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

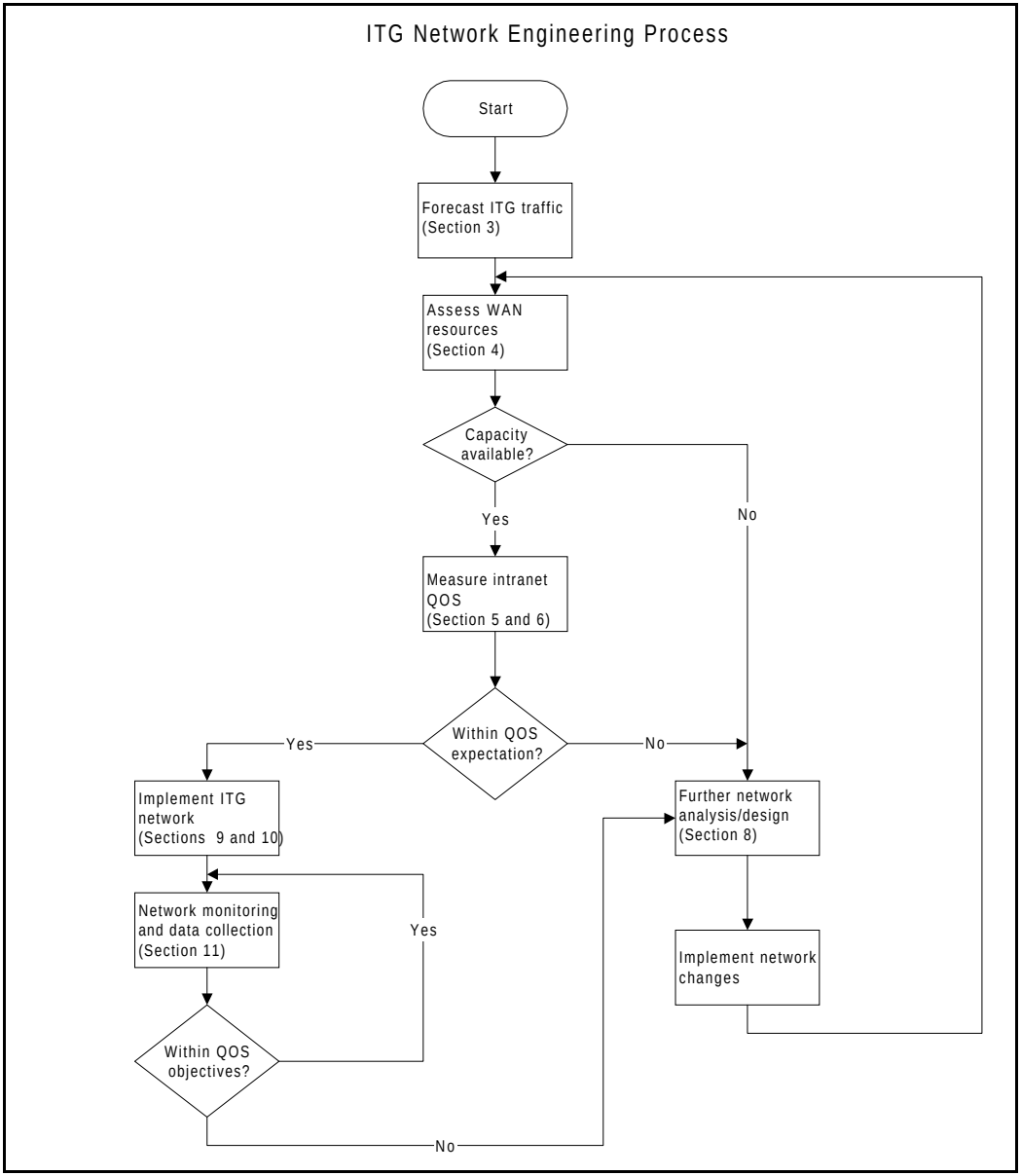
- Forecast ITG traffic. The technician must estimate the amount of traffic that the Meridian 1 system will route via the ITG network. This in turn will place a traffic load on the corporate intranet. This is described in See “ITG traffic engineering” on page 55.
- Assess WAN link resources. If resources in the corporate intranet are insufficient to adequately support voice services, it is usually due to insufficient WAN resources. “Assess WAN link resources” on page 74 outlines how this check can be made.
- Measuring existing intranet's QoS. The technician must estimate the quality of voice service the corporate intranet can deliver. “Measure intranet QoS” on page 84 describes how to measure prevailing delay and error characteristics of an intranet.

After the assessment phase, the technician can design and implement the ITG network. This design not only involves the ITG elements, but may also involve making design changes to the intranet.

- "Further network analysis" on page 91 and "Implement QoS in IP networks" on page 99 provides guidelines for making modifications to the intranet
- "Implement the ITG network" on page 102 provides guidelines for integrating the ITG node into the corporate LAN

The following flowchart shows the design and planning decisions that should take place. Each action and decision point is addressed in this document.

Figure 15
ITG network engineering process



ITG traffic engineering

To design a network is essentially to size the network such that it can accommodate some forecasted amount of traffic. The purpose of the ITG network is to deliver voice traffic in such a way that QoS objectives are met. Since traffic dictates 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

Ethernet and WAN bandwidth use

Table 5 on page 56 lists the Ethernet and WAN bandwidth usage of ITG ports with various codecs. One port is a channel fully loaded to 36 CCS, where CCS (Centi-Call-Second) is a channel/circuit being occupied 100 seconds, a 100% utilization in an hour is 36 CCS. To calculate the bandwidth requirement of a route, the total route traffic should be divided by 36 CCS and multiplied by the bandwidth usage to obtain data rate requirement of that route. All traffic data should be based on busy hour.

Note that to calculate resource requirements (ITG ports and T-LAN/WAN bandwidth), traffic parcels are summarized in different ways: (1) All sources of traffic destined for the ITG network, e.g., voice, fax sent, fax received should be added together to calculate ITG port and T-LAN requirements. (2) For data rate requirement at each route, 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. Therefore, the engineering procedures for T-LAN and WAN are slightly different. The following calculation procedure is for T-LAN (the modification required for WAN engineering is included in these procedures).

Table 5
T-LAN Ethernet and WAN IP bandwidth use per ITG port (36 CCS per port per hour)

Codec type	Frame duration in ms (payload)	Voice/fax payload in bytes	IP packet in bytes	Ethernet frame bytes	Bandwidth usage on T-LAN: kbps	Bandwidth usage on WAN: kbps
G.711 (64 kbps)	**10**	**80**	**120**	**146**	**116.8**	**48.0**
	20	160	200	226	90.4	40.0
	30	240	280	306	81.6	37.3
G.729A/ G.729 (8kbps)	10	10	50	76	60.8	20.0
	20	20	60	86	34.4	12.0
	30	**30**	**70**	**96**	**25.6**	**9.3**
G.723.1 (5.3 kbps)	**30**	**20**	**60**	**86**	**22.9**	**8.0**
G723.1 (6.3 kbps)	**30**	**24**	**64**	**90**	**24.0**	**8.5**
Modem 14400bps 9600 bps	**16.6**	**30**	**70**	**96**	**46.3**	**33.7**
	25	30	70	96	30.7	22.4

Note 1: The shaded row contains the default payload/packet size for each codec in the MAT.

Note 2: T-LAN data rate is the effective Ethernet bandwidth consumption.

Note 3: T-LAN kbps = Ethernet frame bytes*8*1000/Frame duration in ms

Note 4: 50% voice traffic reduction due to silence suppression; no suppression for fax.

Note 5: 8 ports/conversations per card, except for G.729 codec - which has 4 ports per card.

Note 6: Overhead of IP packet over voice packet is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.

Note 7: Ethernet bandwidth must be set aside to support an Interframe gap of at least 12 bytes per frame. This gap is not included in the above bandwidth calculation.

Silence suppression or Voice Activity Detection

When a 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 excessively low audio level, silence suppression should be disabled using the ITG shell command 'itgSetVAD 0'.

Disabling silence suppression *approximately doubles* LAN/WAN bandwidth usage. Disabling silence suppression consumes more real-time on the ITG card. To avoid real-time capacity problems on the ITG card when silence suppression has been disabled, you should set the voice payload to 20 ms or 30 ms for the G.711 and G.729A codec types. This restriction is not required for other codecs types.

> ***Note:*** When silence suppression is disabled, if the technician happens to set a payload size of 10 ms for the G.711 or G.729A codec types, the ITG card software will automatically reject the settings and use a 20 ms payload size instead.

Table 6 shows the full-duplex 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.

Table 6
T-LAN Ethernet and WAN IP bandwidth usage per ITG port without silence suppression (VAD = OFF) (loaded to 36 CCS per port per hour)

Codec type	Frame duration in ms (payload)	Voice/fax payload in bytes	IP packet in bytes	Ethernet frame bytes	Bandwidth usage on T-LAN: kbps	Bandwidth usage on WAN: kbps
G.711 (64 kbps)	**10**	**80**	**240**	**292**	**233.6**	**96.0**
	20	160	400	452	180.8	80.0
	30	240	560	612	163.2	74.6
G.729A/ G.729 (8kbps)	10	10	100	152	121.6	40.0
	20	20	120	172	68.8	24.0
	30	**30**	**140**	**192**	**51.2**	**18.6**
G.723.1 (5.3 kbps)	**30**	**20**	**120**	**172**	**45.8**	**16.0**
G723.1 (6.3 kbps)	**30**	**24**	**128**	**180**	**48.0**	**17.0**
Modem 14400bps 9600 bps	**16.6**	**30**	**70**	**96**	**46.3**	**33.7**
	25	30	70	96	30.7	22.4

Note 1: The shaded row contains the default payload/packet size for each codec in the MAT.

Note 2: T-LAN data rate is the effective Ethernet bandwidth consumption.

Note 3: T-LAN kbps = Ethernet frame bytes*8*1000/Frame duration in ms*2 (for duplex)

Note 4: No silence suppression for voice; no suppression for fax.

Note 5: 8 ports/conversations per card, except for G.729 codec - which has 4 ports per card.

Note 6: Overhead of IP packet over voice packet is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.

Note 7: Ethernet bandwidth must be set aside to support an Interframe gap of at least 12 bytes per frame. This gap is not included in the above bandwidth calculation.

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 might 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 should 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 chosen should 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%

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

The number of trunks (ITG ports) in Table 2 which provides a CCS higher than T is the solution.

5 Calculate bandwidth output (refer to Table 1) (Tv/36 and Tx/36 denote the average number of simultaneous callers)

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.

The procedure presented 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

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

The codec of choice is G.729A, voice packet payload is 30 ms. For fax, the modem speed is 14.4 kbps, 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 kbps 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) = 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 Poisson P.01 Table to find # of ITG ports required for 1% blocking Grade of Service.

804 CCS can be served by 35 ITG ports with P.01 blocking Grade of Service. In other words, 5 ITG cards are needed to serve this customer.

5 Calculate average bandwidth usage on T-LAN

For voice:

720/36*25.6 =512 kbps

Refer to Table 5, data output for G.729A and 30 ms payload is 25.6 kbps.

For fax:

84/36*46.3 =108 kbps

Total bandwidth = 512 + 108 = 620 kbps

6 Adjust requirement for traffic peaking

Peak hour bandwidth requirement = 620*1.3 = 806 kbps

This is the spare bandwidth a T-LAN should have in order to handle the VoIP and fax traffic.

Note that this example is based on the G.729A codec with 30 ms payload size. For relations of user selectable parameters (e.g., payload size, codec type, packet size and QoS), refer to “Set QoS” on page 79.

The relationship between bandwidth requirement and the number of calls/fax to IP network is based on a linear model here. When the IP network is large and traffic from many routes aggregated to the same backbone network, the efficiency of traffic handling at the backbone could be increased and the adjustment for peakedness could be decreased. The bandwidth requirement calculation based on the linear model is a conservative approach.

It is a crucial requirement that the customer's T-LAN be engineered to handle the VoIP traffic generated by the ITG node using the specified codec, without Ethernet delay or packet loss. The customer must pick one configuration and then set up the T-LAN so that there is more bandwidth on the T-LAN than the VoIP traffic output from the ITG cards. Refer to "Configuring the ITG Telephony LAN or T-LAN" on page 64. Refer to standard Ethernet engineering tables for passive 10BaseT repeater hubs. Refer to manufacturer's specifications for intelligent 10BaseT layer switches.

Traffic to Wide Area Network (WAN) is obtained by using the formula: 0.5*IP packet in bytes*8*1000/payload in ms. The reason the data rate being halved is due to the nature of a duplex channel on a WAN. For example, with G.711 codec, a two-way conversation channel has a rate of 128 kbps. However, the same conversation on WAN (e.g, a T1) will require a 64 kbps channel only, since a WAN channel is a full duplex channel.

In other words, both "talk" and "listen" traffic will use a part of the 10 Mbps Ethernet channel while a conversation will occupy a 64 kbps (DS0) duplex channel in a T1 or other WAN media.

Fax calculation is based on 30 bytes packet size and data rate of 64 kbps (no compression). The frame duration (payload) is calculated by using the equation: 30*8/14400=16.6 ms, where 14,400 bps is the modem data rate. Bandwidth output is calculated by the equation: 108*8*1000/16.6=52.0 kbps. Bandwidth output to WAN is: 70*8*1000/16.6=33.7 kbps.

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 will both 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.

If traffic to all nodes is equal, then the ITG TIE trunks can be grouped into one route. If there is a deviation from the average probable rate of fallback calls, ITG TIE trunks to a particular destination that have a higher probability of fallback should be grouped into a separate route to prevent loss of all trunks due to fallback routing to the high traffic destination.

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) avoid offering 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. Therefore, 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 set Time of Day Schedule (TODS).

b) Go to LD 86 RLB and apply the on/off toggle for that route list entry associated with an ITG trunk route.

Configuring the ITG Telephony LAN or T-LAN

A Meridian 1 system can have multiple ITG nodes composed of multiple ITG cards. An ITG node may consist of (1) a leader card only, (2) a leader card and a backup leader card, (3) a leader card, a back up leader card, and one or more follower cards that belong to a customer. The ITG node IP address is administered and stored on the leaders, and the followers are automatically configured via the boot up protocol when follower cards are added or replaced.

The leader cards and followers must not be split by a router for the voice or management network.

Every customer in the Meridian 1 system must only have one ITG node per T-LAN subnet.

Configure the IP router on the T-LAN

As previously mentioned, the ITG system telephony network, or T-LAN should be placed on its own subnet. The router should have a separate 10BaseT 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 packets should have this feature enabled in order to improve Quality of Service performance. For example, if the Type of Service (TOS) field or other differentiated services is supported on the router, it should be utilized.

Leader Card Real Time Engineering

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 far-end Follower Card as well as provide network performance statistics in order for the Follower Card to set up the call successfully. Therefore, the Leader Card CPU real time needs to be engineered in order to reserve enough capacity to provide this call processing assistance functionality.

The real time capacity of the Leader Card depends on various factors: (1) the number of ports on the Leader Card that are configured to carry voice or fax traffic (and which codec and voice sample size are selected), (2) the size of the ITG network (number of Leader Cards in the network), (3) number of probe packets sent to every Leader Card at remote node, etc. Factors (2) and (3) 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.

Table 7 shows the projection for the number of calls per hour that can be supported by the Leader Card CPU for call processing assistance for the case that the Leader Card is not configured to carry voice/fax traffic. 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 (as well as 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 projection 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 projection for the case with G.729A codec and 30 ms voice sample size. For both tables, 40% voice activity is assumed.

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

Network Size (#nodes)	**Case I** 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
	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
Leader Card RT Capacity - G.711, 10ms voice sample, 4 or 8 ports configured (Part 1 of 2)

Network Size (#nodes)	**Case I** 50% Call Origination, 50% Call Termination				**Case II** 100% Call Termination			
	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

Table 8
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
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
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
Leader Card RT Capacity - G.729A, 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.729A 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.729A 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

Provision TIE trunks and routes

TIE trunks are provisioned based on average busy hour traffic tables, using the calculated amount of traffic between ESN/ITG nodes. Table 10 shows the number of trunks required based on average busy hour CCS for a 1% blocking Grade of Service.

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

Table 10
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	31	703	61	1595	91	2530	121	3488
2	5.4	32	732	62	1626	92	2563	122	3520
3	15.7	33	760	63	1657	93	2594	123	3552
4	29.6	34	789	64	1687	94	2625	124	3594
5	46.1	35	818	65	1718	95	2657	125	3616
6	64	36	847	66	1749	96	2689	126	3648
7	84	37	876	67	1780	97	2721	127	3681
8	105	38	905	68	1811	98	2752	128	3713
9	126	39	935	69	1842	99	2784	129	3746
10	149	40	964	70	1873	100	2816	130	3778
11	172	41	993	71	1904	101	2847	131	3810
12	195	42	1023	72	1935	102	2879	132	3843
13	220	43	1052	73	1966	103	2910	133	3875
14	244	44	1082	74	1997	104	2942	134	3907
15	269	45	1112	75	2028	105	2974	135	3939
16	294	46	1142	76	2059	106	3006	136	3972
17	320	47	1171	77	2091	107	3038	137	4004
18	346	48	1201	78	2122	108	3070	138	4037
19	373	49	1231	79	2153	109	3102	139	4070
20	399	50	1261	80	2184	110	3135	140	4102

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

Table 10
Trunk traffic—Poisson 1 percent blocking Grade of Service (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
21	426	51	1291	81	2215	111	3166	141	4134
22	453	52	1322	82	2247	112	3198	142	4167
23	480	53	1352	83	2278	113	3230	143	4199
24	507	54	1382	84	2310	114	3262	144	4231
25	535	55	1412	85	2341	115	3294	145	4264
26	562	56	1443	86	2373	116	3326	146	4297
27	590	57	1473	87	2404	117	3359	147	4329
28	618	58	1504	88	2436	118	3391	148	4362
29	647	59	1534	89	2467	119	3424	149	4395
30	675	60	1565	90	2499	120	3456	150	4427

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

WAN route engineering

Once 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 node is 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 11 summarizes traffic flow of a 4-node ITG network.

Table 11
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 totaling the traffic on a per node basis (based on Table 10 on page 70).

Table 12
Example: Determining ITG card requirements

ITG Site	Traffic in CCS	ITG Ports	ITG Cards
Santa Clara	120	9	2
Richardson	115	9	2
Ottawa	98	8	1
Tokyo	53	6	1

Assuming that the preferred codec to handle VoIP calls in this network is G729A.

The WAN traffic in kbps for each route is summarized in Table 13. Note that the recommended incremental bandwidth requirement is included in the column adjusted for 30% traffic peaking in busy hour

Table 13
Example: Incremental WAN bandwidth requirement

Destination Pair	CCS on WAN	WAN traffic in kbps	Peaked WAN traffic (x1.3) in kbps
Santa Clara/Richardson	60	15.5	20.2
Santa Clara/Ottawa	45	11.6	15.1
Santa Clara/Tokyo	15	3.9	5.1
Richardson/Ottawa	35	9.0	11.7
Richardson/Tokyo	20	5.2	6.8
Ottawa/Tokyo	18	4.7	6.1

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.729A with 30 ms payload, the bandwidth usage on the WAN is 9.3 kbps. WAN traffic is calculated using the following formula: (60/36)*9.3=15.5 kbps. Augmenting this number by 30% would give us the peak traffic rate of 20.2 kbps. 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)*9.3 + (14/36)*33.7 = 23.4 kbps, where 14 CCS is the larger of two fax traffic parcels (14 CCS vs. 6 CCS). After adjusting for peaking, the incremental data rate on WAN for this route is 30.4 kbps. Compare this number with 20.2 kbps when all 60 CCS is voice traffic, it appears that the reduction in CCS due to one-way fax traffic (20 CCS vs. 14 CCS) will not compensate for higher bandwidth requirement of a fax vs. voice call (33.7 kbps vs. 9.3 kbps) 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. For a detailed discussion of routing strategy and WAN design, refer to See “Assess WAN link resources” on page 74.

Assess WAN link resources

For most installations, ITG traffic will be routed over WAN links within the intranet. WAN links are the most expensive recurring expenses in the network and they frequently 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 assess the state of WAN links in the intranet prior to implementing the ITG network.

Each voice conversation, (G.729A codec, 30 ms payload) consumes 9.3 kbps of bandwidth for *each* link that it traverses in the intranet; a DS0 would support just below 7 simultaneous phone conversations.

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 84).

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 may be averaged over a week, a day, or one hour. In order to be consistent with the dimensioning considerations, 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 usage remains below some determined utilization level. For example a planning policy might state that the utilization of a 56 kbps link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, say at 85%. The carrying capacity of the 56 kbps link would be 28 kbps, and for the T1 1.3056 Mbps. In some organizations the thresholds may 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 85% would have an available capacity of about 568 kbps.

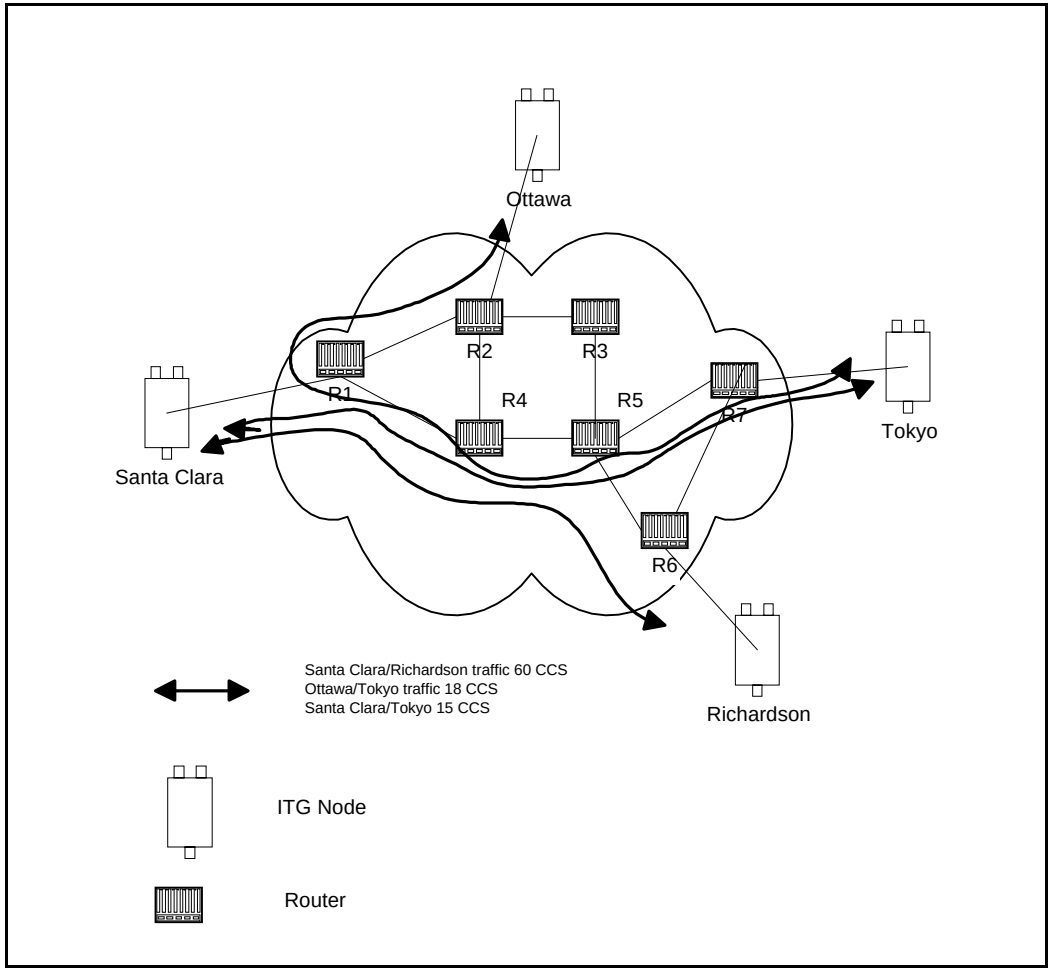
Estimate network loading due to ITG traffic

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

Suppose the intranet has a topology as shown in Figure 16, and the technician wants 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 kbps as the incremental traffic that R4-R5 will need to support.

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

Figure 16
Calculating network load with ITG traffic



Decision: Sufficient capacity?

Table 14 organizes 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 (568 kbps) to accommodate the additional 24 kbps of ITG traffic.

Table 14
Computation of link capacity versus ITG load

Link		Utilization (%)		Available capacity (kbps)	Incremental ITG load		Sufficient capacity?
End-points	Capacity (kbps)	Threshold	Used		Site pair	Traffic (kbps)	
R1-R2	1536	85	75	154	Santa Clara/ Ottawa Santa Clara/ Tokyo	15.5	Yes
R1-R3	1536						
R2-R3	1536						
R2-R4	1536						
R4-R5	1536	85	48	568	Santa Clara/ Richardson Ottawa/ Tokyo Santa Clara/ Tokyo	24	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 the technician 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 insufficient link capacity, one or more of the following options can be decided:

- Use the G.723 codec family. Compared to the default G.729A 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 thorough assessment the technician should also 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.

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' expectations. QoS metrics or parameters are what quantifies those expectations demanded by the "user" on the "service".

In the context of a Meridian 1 and ITG system, Figure 17 illustrates the relationship between users and services:

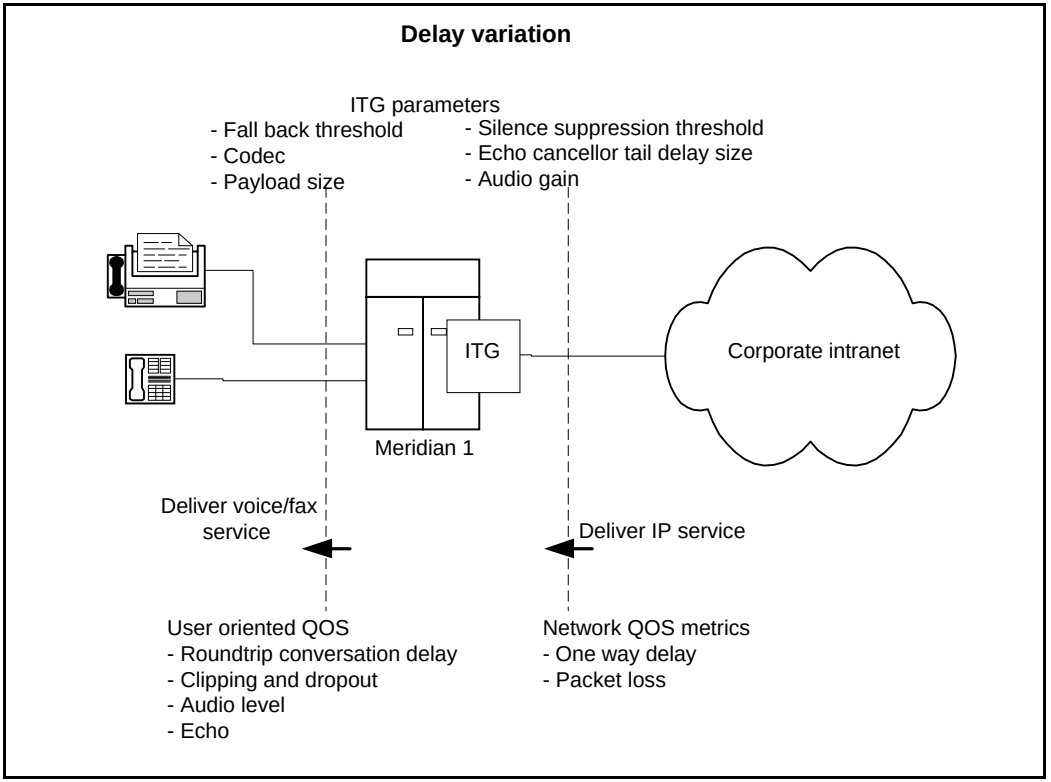
From the diagram it can be seen that there are two interfaces that the technician needs to consider.

- 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 computes the prevailing QoS level per site pair based on its measurement of

Figure 17
Relationship between users and services



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

and when the QoS level falls below the fall back threshold, any new calls to that destination is routed over the PSTN.

The computation is derived from ITU-T G.107 Transmission Rating Model; see Appendix D: “Estimate QoS Level” on page 271 for a table that maps from intranet QoS to the ITG's QoS level. 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 over the traditional PSTN network.

The following graphs show the operating regions in terms of *one-way delay* and *packet loss* for each codec and desired QoS level as computed by the ITG. Note that among the codecs G.711A/G.711U delivers the best quality for a given intranet QoS, followed by G.729A and then G.723. These graphs in effect stipulate the delay and error budget for the underlying intranet in order for it to deliver a desired 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 18
QoS levels with G.729A codec

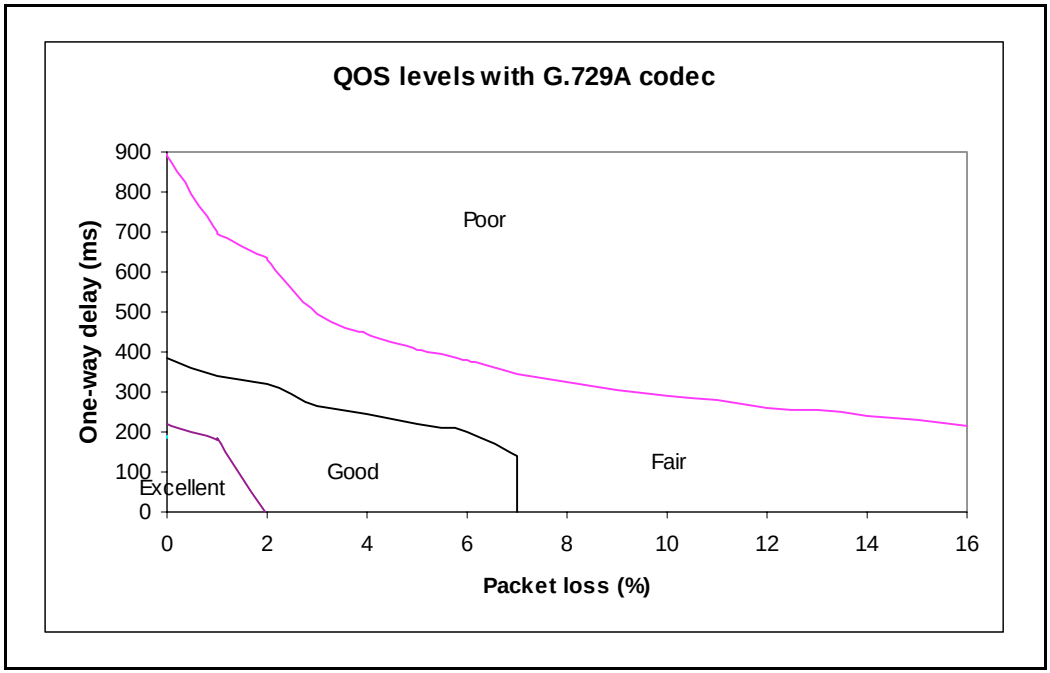


Figure 19
QoS level with G.711A/G.711U codec

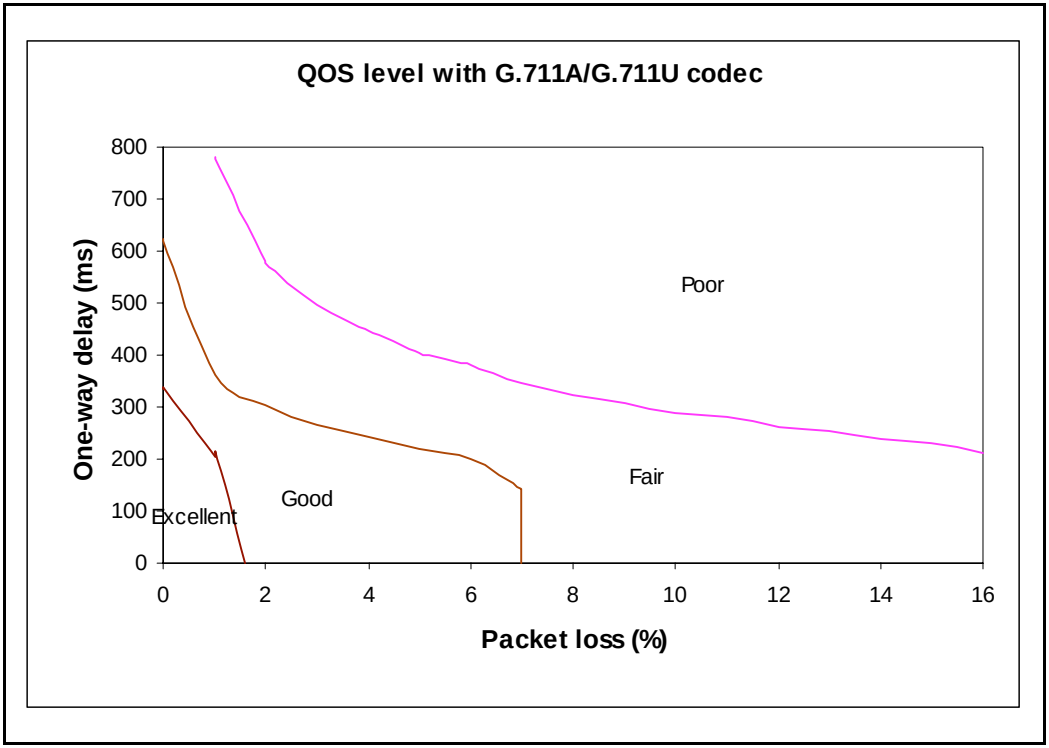
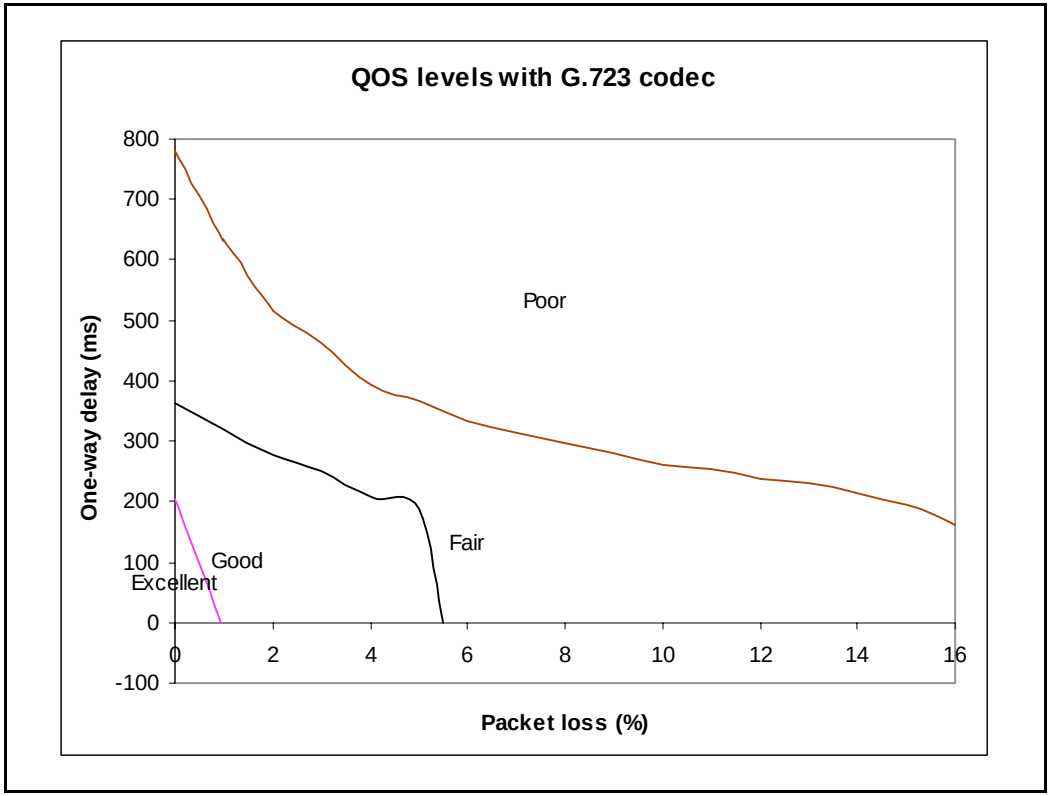


Figure 20
QoS levels with G.723



Measure intranet QoS

End-to-end delay and error characteristics of the current state of the intranet should be measured in order help the technician set realistic QoS expectations when using the corporate intranet to carry 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, and waits for the packet to make a round trip. The output of `ping` looks 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 round trip time (*rtt*) is indicated by the time field.

In order that the delay sample results match what the ITG node would experience, the `ping` host should be on a healthy LAN segment attached to the router intended to support the ITG node. The choice of destination host is just as crucial, following these same guidelines for the source host.

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

Some implementations of `ping` support the `-v` option[1] for setting the TOS. The ITG sets the 8-bit TOS field to IP Precedence = Priority and Reliability = High. Note that if the technician made `ping` measurements on an intranet that does prioritization (see "Queue management" on page 101) 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. The technician can also check whether 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.

Measuring end-to-end packet loss

The `ping` program also reports whether the ICMP packet made its round trip successfully 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

Record routes

Routing information for all source-destination pairs needs to be recorded down 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 also be used to verify whether routing in the intranet is symmetric or not for each of the source-destination pairs. This can be done using the `-g` loose source routing option[1], as illustrated in the following command syntax:

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

The `traceroute` program is used to identify the intranet links that are used to carry ITG traffic. For example, if traceroute of four site pairs yield the results shown in Table 15, then the load of ITG traffic per link can be computed as shown in Table 16:

Table 15
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 may be different depending on vendor implementation

Table 16
Intranet links loaded by ITG traffic

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

Adjust ping measurements

One-way vs. 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 due to 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 thus 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 technician 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. Compute the percentage of late packets, and add that to the *packet loss* statistic.

Measurement procedure

The following procedure is an example of obtaining delay and error statistics for a specific site pair during the peak hour.

- Program a script to run the `ping` program during the peak hour of the intranet, repeatedly sending a series of 50 `ping` requests. Each `ping` request generates a summary of packet loss (with a granularity of 2%), and for each successful probe that made its roundtrip, that many *rtt* samples. For a healthy network there should be at least 3000 delay samples and 60 packet loss samples. Have the raw output of the `ping` results stored in a file. The following is a Perl script that implements this task.

```
#!/usr/bin/perl
$\="\n";
for ($i=0; $i<100; $i++) {
print `date`;
print `ping -s santa_clara_itg4 60 50`;}
```

Program another script to parse the raw output to extract sample *rtt* and PLR statistics.

```
#!/usr/bin/perl
$\="\n";
while (<>) {
    if (/(\d+)%/) {
```

```
print PLR $1;
    }
    if (/time=(\d+)/) {
print RTT $1;
    }
}
```

- Import the *rtt* and PLR statistics into a spreadsheet. On the spreadsheet, halve each *rtt* and PLR statistic, then add to that the quantities indicated in “Adjust ping measurements” on page 87. Discard samples from late packets.
- Compute the average and standard deviation of *one-way delay* and *packet loss*.
- Refer to Appendix D: “Estimate QoS Level” on page 271 to derive the expected QoS level.

Repeat this for each site pair. At the end of the measurements, the following results can be tabulated as shown below:

Table 17
QoS measurements

Destination Pair	Measured one-way delay (ms)		Measured packet loss (%)		Expected QoS Level (see Appendix D: "Estimate QoS Level" on page 271)	
	Mean	Mean+σ	Mean	Mean+σ	Mean	Mean+σ
Santa Clara/ Richardson	171	179	2	2.3	Good	Good
Santa Clara/Ottawa						
Santa Clara/Tokyo						
Richard-son/Ottawa						
Richard-son/Tokyo						
Ottawa/Tokyo						

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, the technician 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 55.

Obtaining 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 ITG QoS expectations?

At the end of this measurement and analysis, the technician 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 Table 17, the technician 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 D: “Estimate QoS Level” on page 271, the technician can estimate the amount of *one-way delay* that needs to be reduced to raise the QoS level. “Further network analysis” on page 91 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 also decide on the side of keeping costs down, and accept say a "Fair" QoS level for the moment for a particular route. In that case, having made a calculated trade-off in quality, the technician will need to closely monitor the QoS level, reset expectations with the end users, and be receptive to user feedback.

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:

- Reducing link delay

- Reducing hop count
- Adjusting jitter buffer size
- Implementing 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 kbps)

Table 18 shows what the serialization delay for voice packets on a 64kbps and 128kbps link. The serialization delay on higher speed links are considered negligible.

Table 18
Serialization delay

Codec	Frame duration	Serialization delay over 64kbps link (ms)	Serialization delay over 128kbps 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.729 G.729A	10 ms	5.25	0.33
	20 ms	6.50	0.41
	30 ms	7.75	0.48
G.723.1 5.3 kbps	30 ms	6.50	0.41
G.723.1 6.3 kbps	30 ms	7.00	0.44

Queuing delay

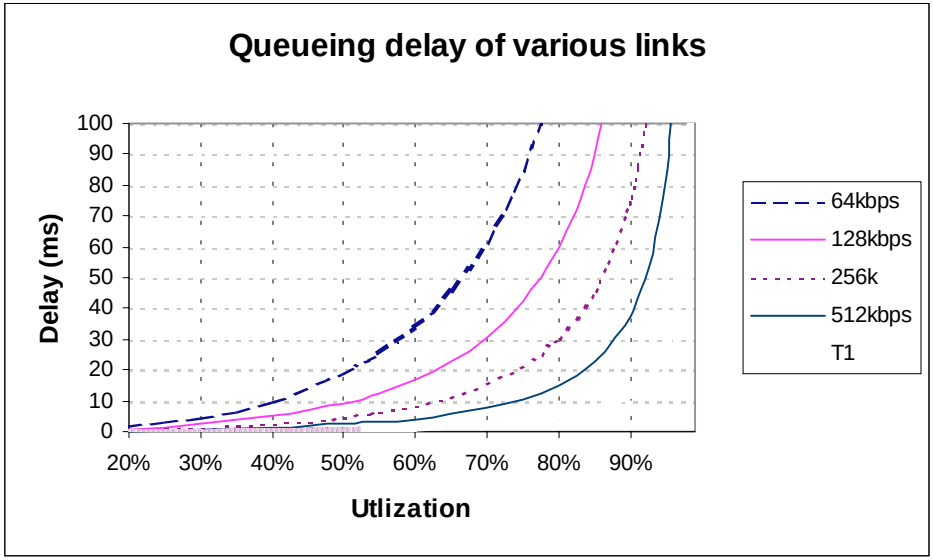
Queueing delay is the time it takes for a packet to wait in transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queueing time in ms is estimated by the formula:

p*p*(average intranet packet in bytes)/(1-p)/(link speed in kbps),

where p is the link utilization level

The average size of intranet packets carried over WAN links generally lies between 250 and 500 bytes. The following chart plots the average queueing delay of the network based on a 300-byte average packet size.

Figure 21
Queuing delay of various links



As can be seen, queueing delays can be significant for links with bandwidth under 512 kbps, 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 contribute to end-to-end delay. Sound routing in the network depends on proper network design at many levels, such as the architecture, topology, routing configuration, link speed, etc.

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 packetized speech, and by the decoder to reconstruct and depacketize the voice packets.

There is a second component of delay which takes place 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 explore 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, thereby reducing the queueing delay as well. To estimate how much delay can be reduced, refer to the tables and formulas given in "Serialization delay" on page 92 and "Queuing delay" on page 93. Before upgrading a link the technician should 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 101.

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 256kbps 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 due to queueing. Looking at the chart in "Queuing delay" on page 93, if the technician upgrades this link to T1, he will 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. Combine co-located nodes onto one larger and more powerful router.

Essentially these suggestions affect the whole intranet, as they temper 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 this comes at the expense of giving less waiting time for voice packets that arrive late. Refer to "ITG parameter settings" on page 109 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 tend to be 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 should also 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 resolution.

- 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 also 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 97.

Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation may overlook a substantially better route. A high delay variation could be due to 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 quite difficult or laborious 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 evolved primarily because of the need to support data services, services which for the most part a "best effort" IP delivery mechanism suffices. Thus it is not surprising that traditionally intranets are designed to support a set of 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 might do well. On the other hand 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, thereby 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 moment, 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 IP QoS

When the ITG node packetizes voice and fax traffic, it sets the 8-bit Type of Service (TOS) field in the IP header to `00100100`, which in effect is tagging the IP packet. The first three bits known also as the IP precedence denote that the packet is tagged a priority of `001.` The next four bits `0010`, referred to as TOS bits also, signify that the packet should be treated to maximize the reliability of packet delivery.

In contrast, most IP packets in the intranet do not have the TOS field set at all. If the intranet provides differentiated services based on the TOS field, then the ITG and other traffic marked with this TOS value could be delivered with the goal of meeting this class of traffic's QoS objectives.

Queue management

From “Queuing delay” on page 93, 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 100 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 applied to favor dropping packets from long-lived TCP sessions, while disfavoring dropping 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.

Implement the ITG network

ITG card connections

10BaseT Ethernet ports

The ITG card has two 10BaseT Ethernet ports: one that is located on the faceplate carries Voice over IP (VoIP) traffic and connects to the Telephony LAN, or T-LAN; another that is located on the card backplane I/O connector carries ITG system management traffic and connects to the Embedded LAN, or E-LAN.

RS-232 serial ports

The ITG card has two RS-232 serial ports: one that is located on the faceplate, is a TTY interface providing raw ASCII access to the CLI for system management; another that is located on the card backplane I/O connector is reserved for future development.

ITG cabling

The NTMF94DA cable breaks out the signals from the I/O connector on both large systems and Option 11 to the Ethernet management port (E-Lan connection), Ethernet voice port (T-Lan connection) and one maintenance RS232 port through a 9-way D-type connection.

Figures 22 and 23 show the cabling required for an ITG card in an option 11C and an IPE module. The required cables are:

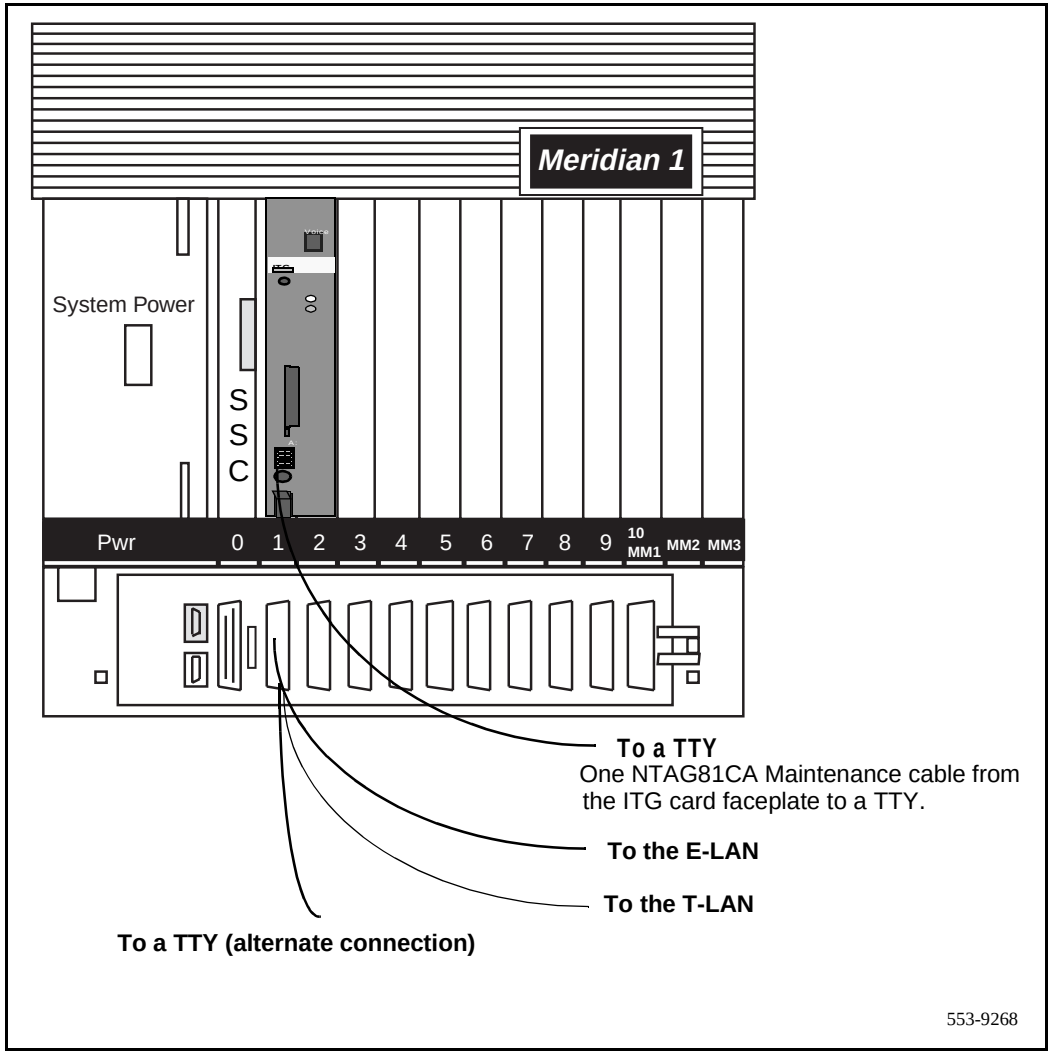
- one NTMF94DA cable
- one NTAG81CA Maintenance cable from the RS-232 port on the ITG card faceplate to a TTY.

Note: Please refer to “Cabling” on page 255 for more details.

Set up separate subnets for voice and management

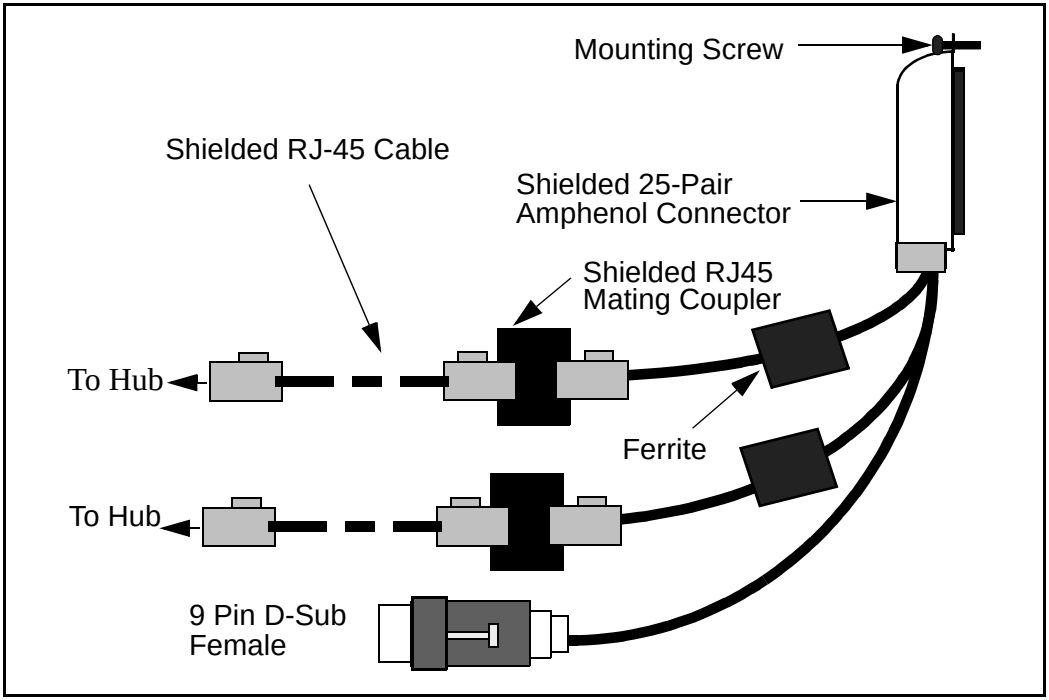
The ITG cards have two Ethernet ports per card, so the ITG system can support two different networks for the voice interface (Telephony LAN or T-LAN) and management interface (Embedded LAN, or E-LAN) connections. The advantages of this setup are:

Figure 22
NTMF94DA cable installed in an option 11C



- 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.

Figure 23
NTMF94DA card installed in an IPE module



- to optimize E-LAN performance, e.g., for Symposium Call Center Server (SCCS) and MCE functional signaling, by segregating the E-LAN from ITG T-LAN VoIP traffic.
- to facilitate security of the E-LAN and Customer Enterprise Network (C-LAN) by connecting the E-LAN to a firewall router on the C-LAN.

It is highly recommended that the customer place the voice and management LANs on separate subnets, separated by a router. No other IP devices, whether Nortel or other vendor's products, should be placed on the same T-LAN subnet with the ITG cards belonging to a single ITG node.

Each ITG node, corresponding to a separate customer in the Meridian 1, must have its own separate T-LAN for each customer that has its own separate WAN.

Set up the management subnet

The management LAN, or E-LAN, is 10BaseT Ethernet. Very little traffic is generated by the ITG node on this network. A standard configuration is an 8-port passive hub connecting the ITG system management Ethernet to the MAT PC via 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 may be configured on a switching hub to maximize data throughput.

Select public or private IP addresses

The customer must consider a number of factors to determine whether 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 may 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 onto 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 scarce 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.

Note: It is not a requirement to have a router which has priority packet routing capability. The ITG can function without any priority routing mechanisms if the intranet is designed to minimize traffic congestion through the WAN backbone links and routers. Refer to "Implement QoS in IP networks" on page 99.

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 systems, assuming adequate bandwidth on the WAN links for the shorter route. This will reduce the fixed and variable IP packet delay, and improve the Voice over IP Quality of Service. It is recommended that up to 8 cards share the same 10BaseT LAN collision domain, provided that the preferred codec throughout the ITG network is set to G.729A, G.729, 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 10Mbps collision domain; in a switched Ethernet hub, each port has its own collision domain.) Due to the much higher bandwidth consumption of the G.711 codec family, it is recommended that no more than 2 ITG cards share the same LAN collision domain in a G.711-only ITG network.

If the technician wishes to deploy a mixed codec ITG network or uses a non-default payload size or fax settings, then he should use the LAN bandwidth consumption in Table 5 to estimate the amount of LAN bandwidth consumed by each card. It is recommended that the 10Mbps collision domain not be utilized beyond 25-30% at the peak.

If the uplink from the T-LAN hub (whether passive or switched) to the router is 10Mbps, then the maximum number of ITG cards allowed per hub is the same as the limit described in the previous paragraph. If the uplink is 100Mbps, 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.

The technician 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 still provide voice services even if 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 burst 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.

Set 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 24 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 24
Basic setup of the ITG system

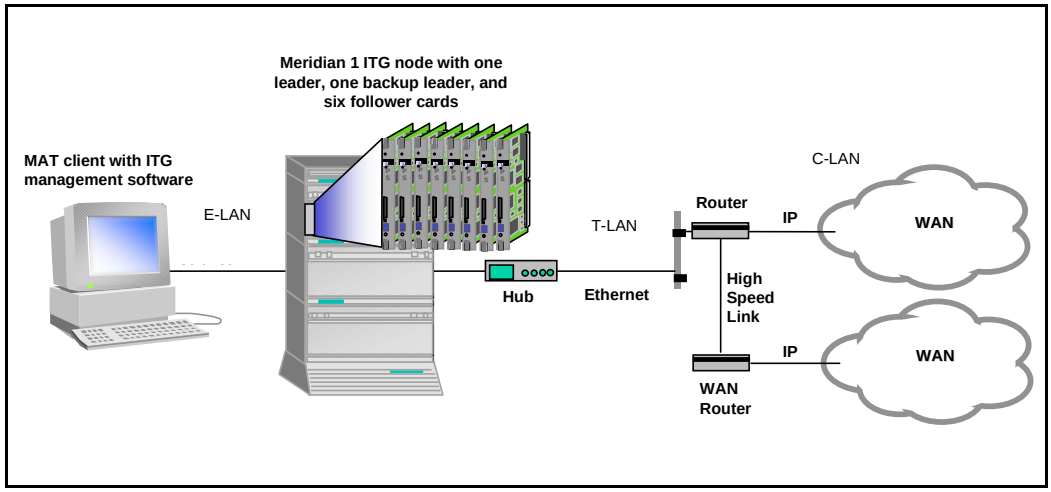
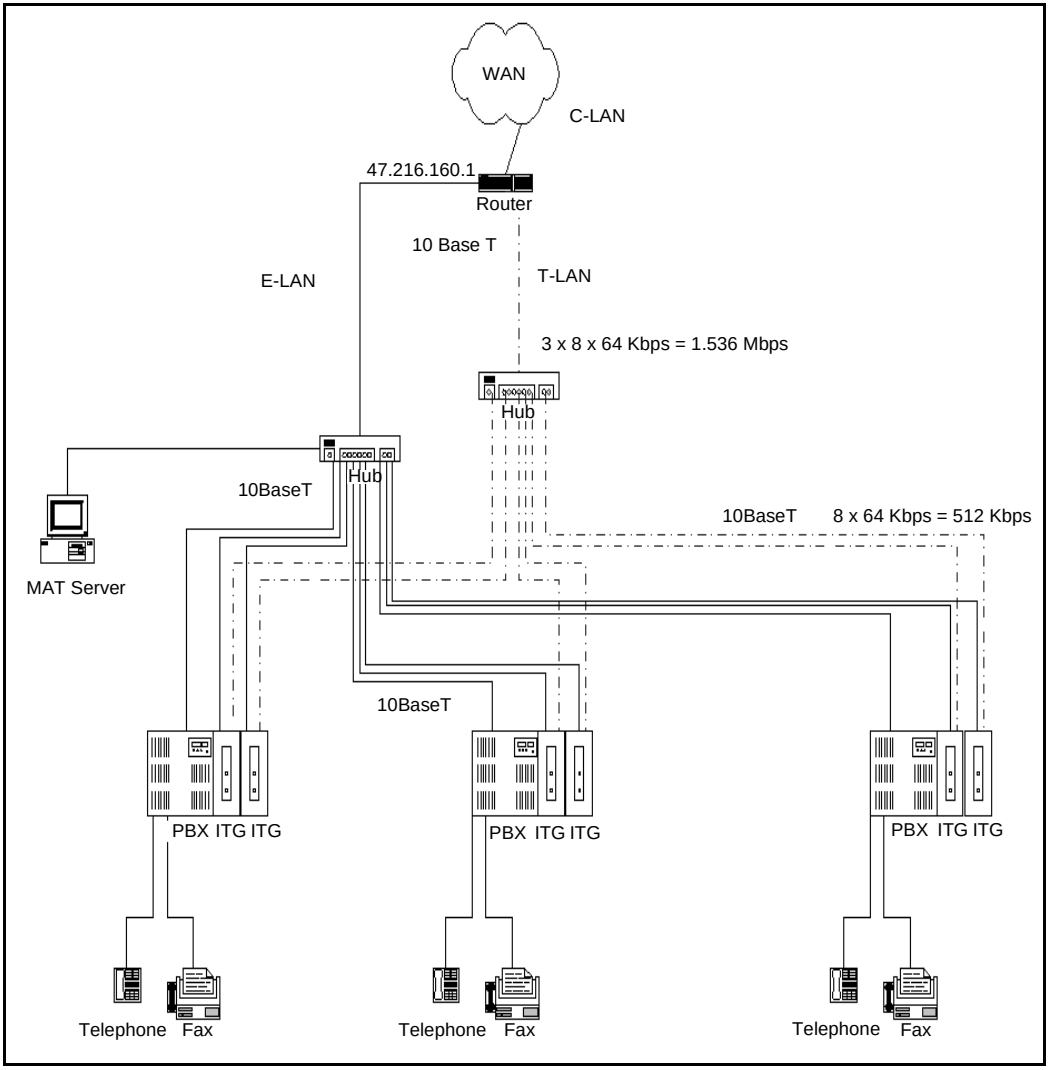


Figure 25 is an another example of an ITG system:

Figure 25
Example of an ITG system



ITG parameter settings

Codec types

There are three codec images that the technician can set an ITG card to:

- Image 1: G.711A, G.711U G.729A
- Image 2: G.711A, G.711U, G.723 5.3K, G.723 6.3 K
- Image 3: G.711A, G.711U G.729

The DSP coding algorithm parameter sets the preferred codec of each ITG card. The recommendation is to use Image 1, and to set the preferred codec to G.729A with a payload setting of 30 ms. At this codec-payload combination the ITG can deliver a fairly good QoS and yet loads less than 10 kbps per port on the intranet.

It is recommended that all the cards in the ITG system 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. As indicated in Table 5, among the three codec families, the default codec consumes the most bandwidth.

Consider whether the ITG network results in tandem encoding for some of the users. Too much consecutive coding and encoding by G.729A, G.723 6.3K, G.723 5.3K, or G.729 codecs can lower the end-to-end quality of service.

Unlike the G.729A codec and other codecs, using the G.729 codec reduces the number of usable ports per card from eight to four.

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

To avoid real-time capacity problems on the ITG card when silence suppression has been disabled, you should set the voice payload to 20 ms or 30 ms for the G.711 and G.729A codec types. This restriction is not required for other codecs types.

Note: When silence suppression is disabled, if the technician happens to set a payload size of 10 ms for the G.711 or G.729A codec types, the ITG card software will automatically reject the settings and use a 20 ms payload size instead.

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.

The Set QoS and Measure intranet QoS sections describe the process of determining the appropriate QoS level for operating the ITG network. Site pairs can have very different QoS measurements, perhaps because some traffic flows are local, while other traffic flows are inter-continental. The technician can consider setting a higher QoS level for the local sites compared to the international ones, thereby keeping costs of international WAN links down.

Normally the fall back threshold in both directions should be set to the same QoS level. In site pairs where the applications are primarily such that one direction of flow is more important, the technician can set up asymmetric QoS levels.

Payload size

The ITG default payload sizes are as follows:

- 30 ms for G.729A, G.729, 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.729A codec families. In a site pair that experience packet losses, choosing a smaller payload size improves voice and fax quality, but at the expense of a higher bandwidth consumption (see Table 5).

Silence suppression parameters

When silence is detected, the ITG node sends a flag to the destination ITG node that denotes start of silence. Thereafter, 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

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 97, 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 the technician wishes to discard to downsize the jitter buffer, he 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 84 or “Post-installation network measurements” on page 111. 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 whether 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
- Implement 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

The technician needs to state the design objective of the ITG network, the purpose of which is to set the standard for assessing 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 84. Initially the QoS objective is to be set such 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 desired QoS

level. The graphs of Figures 18 to 20, together with the QoS measurements, should help the technician determine what threshold levels are appropriate.Table 19 describes examples of ITG QoS objectives::

Table 19
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.

Analyze ITG traffic

Hourly ITG traffic needs to be gathered and archived. The traffic data comes from two sources: the Meridian 1 TFC001 and TFC002 reports, and from ITG Operational Measurement reports. Together, these sources provide offered, carried, and fall back traffic statistics. At the end of the month, the hours with the highest CCS and fall backs can be tabulated as shown in Table 20:

Table 20
Comparison of beginning ITG traffic to ending ITG traffic

Site	Busy hour offered traffic (CCS)		ITG ports installed	
	Start	End	Installed	Required
Santa Clara Richardson				

Compare the statistics with that of the previous period. Note in particular:

- Increases in offered traffic during the busy hour, since that may mean that additional ITG cards need to be added to the network, and
- Increases in fall back traffic: a sign that the intranet QoS may be degraded.

This table will determine whether additional ITG ports need to be installed in order to provision a P.01 grade of service.

Intranet QoS monitoring

In order to monitor the *one-way delay* and *packet loss* statistics, a delay and route monitoring tool such `ping` and `traceroute` need to be installed on the T-LAN of each ITG site. See “Measure intranet QoS” on page 84 for guidelines concerning the implementation of the `ping` hosts, the use of scripting, and information concerning other delay monitoring tools. 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 significant. At the end of the month, the hours with the highest *one-way delay* are noted; within those hours, the *packet loss* and standard deviation statistics can be computed.

At the end of the month, the technician can analyze each site's QoS based of information summarized in Table 21:

Table 21
QoS monitoring

Site pair	One-way delay Mean+σ (ms)		Packet loss Mean+σ (%)		Busy hour offered traffic (CCS)		Carried traffic (CCS)		QoS objective
	Last period	Current period	Last period	Current period	Start	End	End	Start	
Santa Clara/ Richardson									
Santa Clara/ Ottawa									
Etc.									

Declines in QoS can then be correlated with increasing ITG traffic, as well as intranet health reports to locate the sources of delay and error in the network, and proactive steps can be taken to strengthen the intranet.

QoS Levels

Turn to Appendix D: "Estimate QoS Level" on page 271 for a table that shows codec QoS levels based on packet loss percentage and one-way delay statistics.

ITG network inventory and configuration

The technician should record the current ITG design as well as log all adds, moves and changes to the ITG network that occur. Keep the following data:

- 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 whether the theoretical QoS settings match what end users perceive. The feedback may come from a Helpdesk facility, and should include information such as time of day, origination and destination points, and a description of service degradation.

The fall back threshold algorithm assumes 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. In particular, users may 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.

Install and configure the ITG node

This chapter describes the installation and configuration of a Meridian Internet Telephony Gateway (ITG) Trunk 1.0 node on MAT and the Meridian 1. This installation assumes that MAT, including Alarm Management and the MAT ITG application has already been installed, that no ITG cards have been installed so far in the new ITG node, and that the *Engineering Guidelines* section has been read and applied for the new ITG node or network.

The ITG node configuration must be coordinated with the IP data network and the Meridian 1 ESN (Electronic Switched Network).

Installation summary

This section describes the following sequential steps to perform ITG installation and configuration:

Create the ITG Installation Summary Sheet

It is recommended that an ITG Installation Summary Sheet (Table 22) be filled in as the cards are unpacked, inventoried, and provisioned in the Meridian 1 system. IP information will normally be supplied by the customer's IS department. Use of the Installation Summary Sheet will greatly facilitate entry of configuration data on MAT and Meridian 1.

Table 22
ITG Installation Summary Sheet

Site_____**M1 system**_____**M1 customer**_____
T-LAN Node IP address_____**SNMP Management addresses**_____
T-LAN subnet mask_____**T-LAN gateway**_____
E-LAN subnet mask_____**E-LAN gateway**_____

TN	MAC address	E-LAN Management IP address	T-LAN Voice IP address	Card role	Card index	NT_SDID	Keycode
				leader	0		
				leader	1		
				follower	2		
				follower	3		
				follower	4		
				follower	5		
				follower	6		
				follower	7		
				follower	8		
				follower	9		
				follower	10		
				follower	11		
				follower	12		
				follower	13		

Table 22
ITG Installation Summary Sheet

Site_____**M1 system**_____**M1 customer**_____
T-LAN Node IP address_____**SNMP Management addresses**_____
T-LAN subnet mask_____**T-LAN gateway**_____
E-LAN subnet mask_____**E-LAN gateway**_____

TN	MAC address	E-LAN Management IP address	T-LAN Voice IP address	Card role	Card index	NT_SDID	Keycode

Add an ITG node on MAT manually

This section uses the MAT ITG application to manually add and configure an ITG node, and add ITG cards to the node. Every ITG node must be first be added manually on the first MAT ITG PC, and the MAT ITG configuration data must be transmitted to the ITG node during installation. Thereafter, an existing ITG node can optionally be added on another MAT ITG PC by retrieving the configuration data from the existing ITG node.

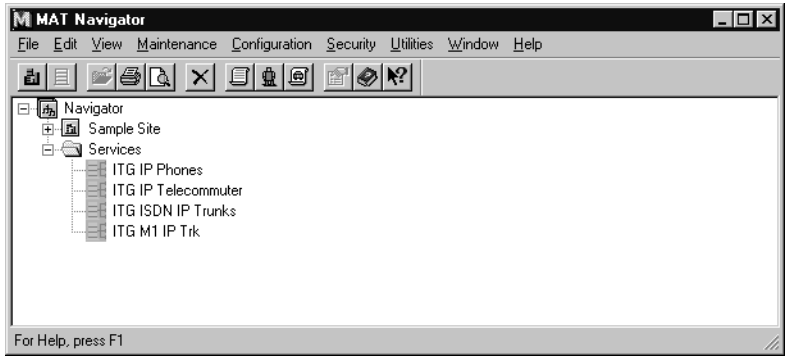
The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the MAT Navigator before you can add a new ITG node. Only one ITG node can be added in the MAT ITG application per Meridian 1 customer on a MAT Meridian 1 system.

If multiple ITG nodes are required per Meridian 1 customer, then additional “dummy” customer numbers must be created in MAT Navigator under the MAT Meridian 1 system.

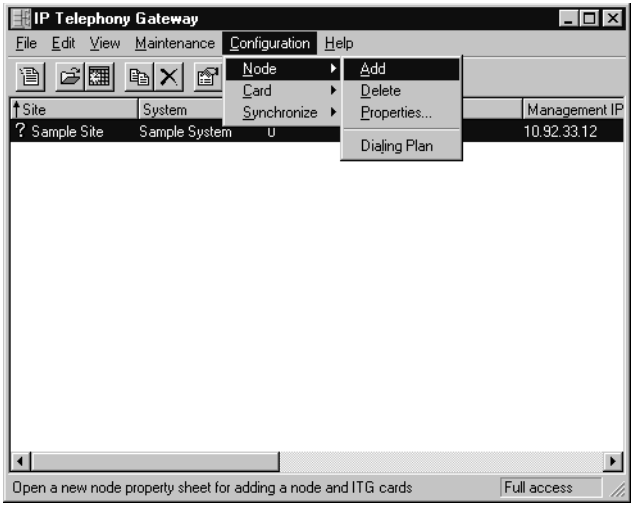
If ITG trunks must be segregated by Codec type, destination nodes, or caller groups, then multiple ITG nodes must be implemented to control incoming traffic on the different ITG routes.

Note: Each ITG node must have a separate LAN segment (LAN broadcast collision domain) and IP subnet address.

1 Launch the Meridian Administration Tools application on the MAT PC.

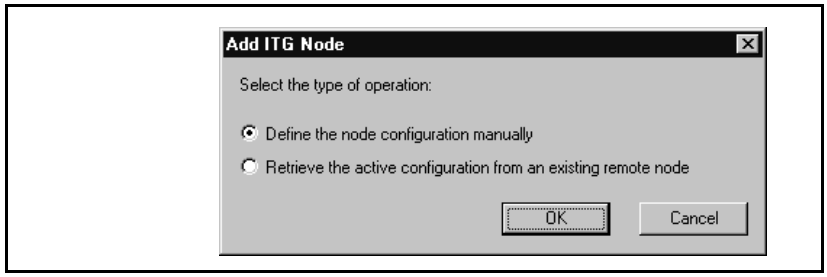


2 From the “MAT Navigator” window, double-click the **ITG M1 IP Trk** icon from the “Services” folder. The “IP Telephony Gateway” window opens.



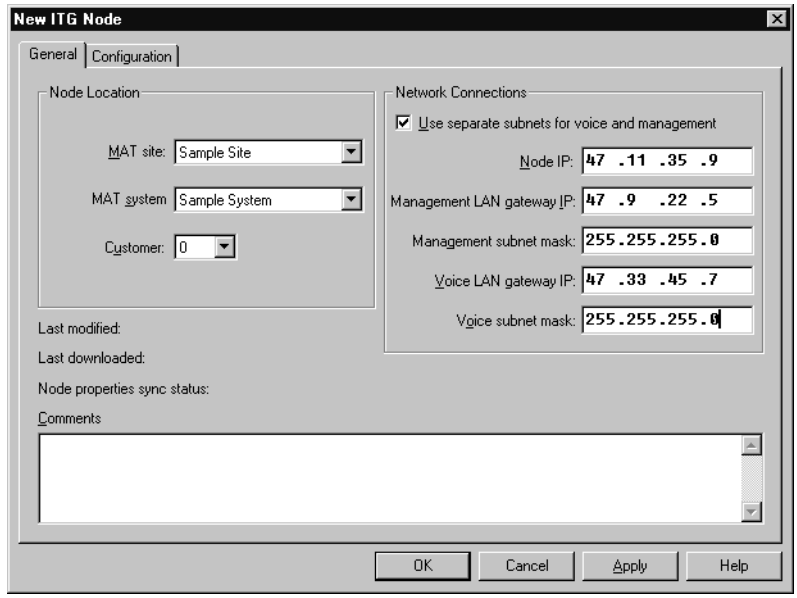
3 In the “IP Telephony Gateway” window, click the **Configuration** menu and select **Node**, then **Add**.

4 When the Add Node dialog box appears, click **OK** to accept the default choice of manually defining an ITG node.



Configure the node

1 In the “General” tab of the “New Node Properties” dialog box, do the following:.



2 Select the “Site name”, “System name” and “Customer” from the pull-down menus.

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.

3 Enter the IP addresses as follows:

NOTICE

It is *strongly recommended* that separate LANs (i.e, separate Ethernet broadcast domains) for the voice and management networks are used.

If the same LAN is used for the voice and management networks, then all voice and management data goes through the management Ethernet interface.

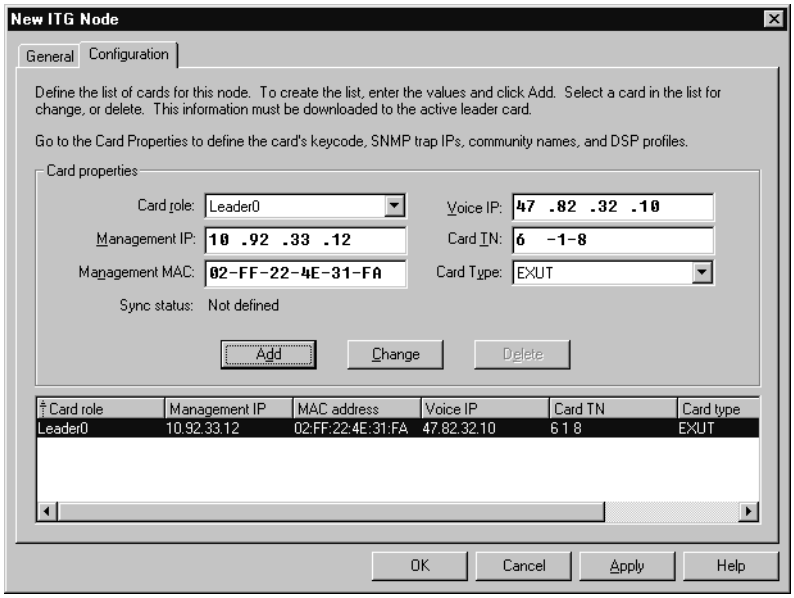
- If you will be using the same subnet for the voice and management networks, enter the “Node IP,” “Management gateway IP,” and “Management subnet mask” fields.
- If you will be using a separate subnet for the voice and management networks, check the “Use separate subnet for voice and management” check box, and enter the “Node IP,” “Voice gateway IP,” “Management gateway IP,” “Voice subnet mask,” and “Management subnet mask” fields. IP addresses and subnet masks must be entered in dotted decimal format.

Subnet masks may be expressed in Classless Inter-Domain Routing (CIDR) format, appended to the IP address. For example 10.1.1.1/20. To convert subnet mask from CIDR format to dotted decimal format refer to *Appendix C*.

Note: See your network administrator for information on IP addresses. The network administrator should refer to the Engineering Guidelines in assigning IP addresses. Refer also to the ITG Installation Summary Sheet.

Add ITG cards to the node

1 Click the **Configuration** tab in the upper left corner of the dialog box.



The “Configuration” tab is used to add ITG cards within the node.

“When adding the first card, select the Card role “Leader 0.” If adding a second card, select “Leader 1.” If adding the third and additional cards, select “Follower.”

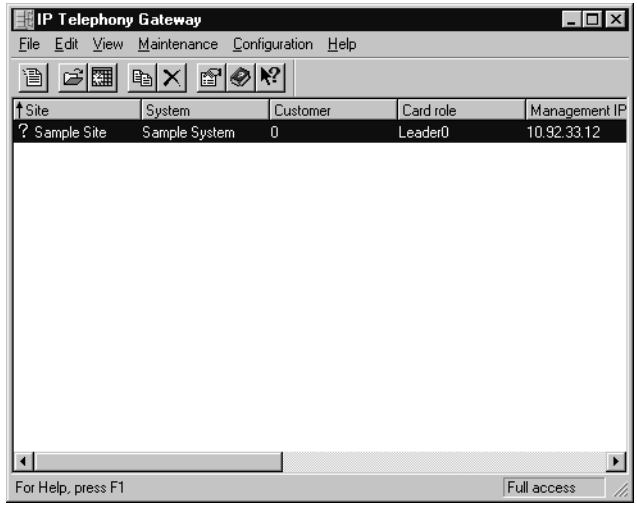
Note: Leader 0 or Leader 1 may have the card state of “active leader.” The other leader card will then have the card state of “backup leader.” Upon system power-up, Leader 0 will normally function as the active leader and Leader 1 as the backup leader. At other times, the leader card states may be reversed so that Leader 1 functions as the active leader and Leader 0 as the backup leader.

2 To add a card:

- Enter the “Management IP”, “Management MAC”, “Voice IP”, and “Card TN” fields. These fields are mandatory. The “Management MAC” address is labeled on the faceplate on the ITG card.
- Select “Leader 0”, “Leader 1”, or “Follower” from the “Card role” pull-down menu.
- Click **Apply** then **OK**.

3 Repeat the previous steps for each card to be added within that ITG Node.When all ITG cards have been configured, click **OK**.

The “IP Telephony Gateway” window displays all configured ITG cards.



4 Repeat this section for each ITG node to be added manually. Use the next section, “Retrieving and viewing ITG node configuration” to copy the data of one node to another.

Add an ITG node on MAT by retrieving an existing node

This is an optional procedure that may be used in the following cases:

- You may choose to add existing nodes to a particular MAT ITG PC in order to manage the ITG network from a single point of view.
- This procedure may also be used to restore the ITG configuration database to a MAT ITG PC whose hard drive had crashed, as an alternative to restoring the MAT ITG nodes from the MAT Disaster Recovery Backup.

Once the ITG node has been installed and configured manually, that node may be added to another MAT ITG PC by retrieving the configuration data from the existing ITG 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. Only one ITG node can be added in the MAT ITG application per Meridian 1 customer.

Note: If multiple MAT ITG PCs are used to manage the same ITG network, care must be taken to synchronize the different copies of the ITG database. The MAT ITG **Configuration|Synchronize|Retrieve** function can be used to synchronize the MAT ITG database with the database on the ITG node.

Configure the node and Leader 0

1 Launch the Meridian Administration Tools application on the MAT PC.From the “MAT Navigator” window, double-click the **ITG M1 IP Trk** icon from the “Services” folder. The “IP Telephony Gateway” window opens.

2 In the “IP Telephony Gateway” window, click the **Configuration** menu and select **Node**, then **Add**.

3 When the Add Node dialog box appears, click the second option “Retrieve the active configuration from an existing node” and click **OK**.

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. Only one ITG node can be added in the MAT ITG application per Meridian 1 customer.

5 Enter the management IP address field for the active leader on the existing node.

6 Enter the SNMP read/write community name. The default is “private”.

7 Click the **Start Retrieve** button.

The results of the retrieval are shown in the “Retrieve control” dialog box. The node properties are retrieved from the active leader. The card properties and the node dialing plan are retrieved from Leader 0.

8 Click **Close** when the download is complete.

9 Refresh the card status from the View menu, and verify that the cards in the newly added node are responding.

Add the remaining ITG cards to the node

1 In the main window, select Leader 0 of the newly added node.

2 Use the **Configuration|Synchronize|Retrieve** command to retrieve the card properties for all ITG cards in the selected node.

Note: If the Leader 0 ITG card was not responding in step 9, then the dialing plan can be retrieved from Leader 1 or any follower card. You need only retrieve the dialing plan from a single card in the node. If you retrieve the dialing plan from multiple cards, the last retrieved dialing plan table will apply.

This completes the procedure of adding a new node by retrieving.

Add a “dummy” node for retrieving and viewing ITG node configuration

This procedure should be used to create a “dummy” ITG node for retrieving and viewing the actual ITG node configuration, without over-writing the existing ITG configuration data for an existing node in the MAT ITG database. Retrieving the actual 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, in order to determine the desired direction of database synchronization:

- transmit MAT ITG to ITG node, or
- retrieve ITG node to MAT ITG node.

The dummy node can be added 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 the need arises to view the actual data of an existing ITG node, the craftsperson will select the “dummy” node and change the management IP address in the node properties to access the desired node. Then the data is retrieved from that node using the **Configuration|Synchronize|Retrieve** function and confirming to over-write the MAT ITG data for the “dummy” node.

Retrieve ITG configuration information from the ITG node

This is an Optional procedure that may be used in the following cases:

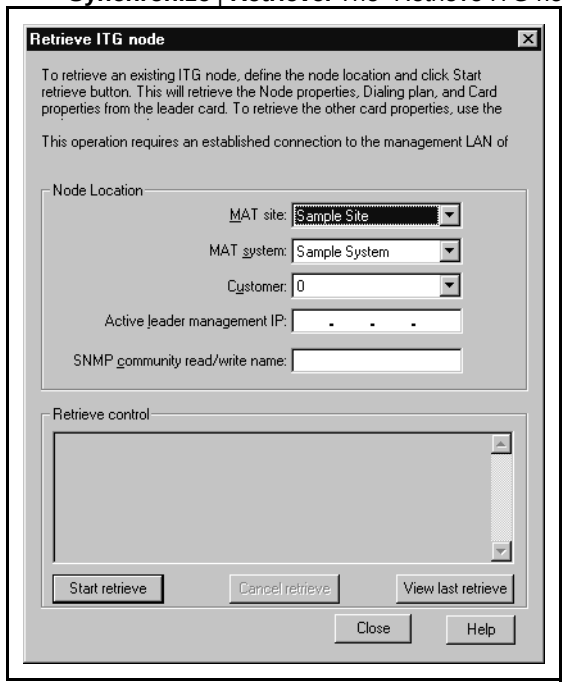
- When adding an ITG node on MAT by retrieving an existing node
- When you suspect that the ITG node configuration on the ITG card differs from the MAT ITG database (e.g., during maintenance and fault isolation procedures).
- When you have multiple MAT ITG PCs with multiple instances of the database (administration).

Use the MAT ITG **Configuration|Synchronize|Retrieve** command to retrieve the ITG configuration information from the ITG node.

1 Launch the Meridian Administration Tools application on the MAT PC.From the “MAT Navigator” window, double-click the **ITG M1 IP Trk** icon from the “Services” folder. The “IP Telephony Gateway” window opens.

2 In the “IP Telephony Gateway” window, select Leader 0 or any card from the node.

3 In the “IP Telephony Gateway” window, click the **Configuration** | **Synchronize** | **Retrieve.** The “Retrieve ITG node” window appears.



4 Leave the defaulted “Retrieve to selected nodes” Option selected, or click the “Retrieve from selected cards,” depending upon the situation:

- Leave the defaulted “Retrieve to selected nodes” when 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, or if you are adding a node on MAT by retrieving from an existing node that consists of more than one card.
- Select “Retrieve from selected card” when you are attempting to isolate a problem with ITG configuration on a particular card.

5 Check the boxes for the ITG configuration data that you wish to retrieve, depending upon the situation:

- 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.
- Select “Card Properties” if you are adding a node on MAT by retrieving from an existing node that consists of more than one card.
- 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.

6 Click the **Start retrieve** button.

Monitor the progress 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.

Whenever a dialing plan table is retrieved, it is compared with the existing node dialing plan on MAT ITG and discarded if it is identical. If it is different, you will be 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.

Create the ITG Dialing Plan on MAT

The ITG dialing plan must be configured both on MAT and on the Meridian 1 system and transmitted from MAT ITG to the ITG node during installation, card replacement, or whenever the dialing plan is changed on MAT ITG. The procedure "Configure the Meridian 1 ESN dialing plan for the ITG network" on page 165 must be used to coordinate the dialing plan entries between Meridian 1 and the ITG node.

Each ITG node requires a single dialing plan shared by all the cards to translate the dialed digits outpulsed by the Meridian 1 into the Node IP address of the active leader on the destination ITG node. A dialing plan is composed of one or more dialing plan entries for each destination node in the ITG network. A dialing plan entry consists of a translation type, ESN Access Code if applicable, dialed digits, number of digits, digit manipulation to be applied to the "Dialed Number" in the outgoing setup message, destination ITG node IP address, and Quality of Service settings.

Configure Dialing Plan Access Codes

1 In the "IP Telephony Gateway" window, select the **Configuration** | **Node** | **Dialing Plan**. The "ITG Dialing Plan" window appears.

2 Select **Dialing Plan Properties** from the **Configuration** menu. The "ITG Dialing Plan Properties" window appears.

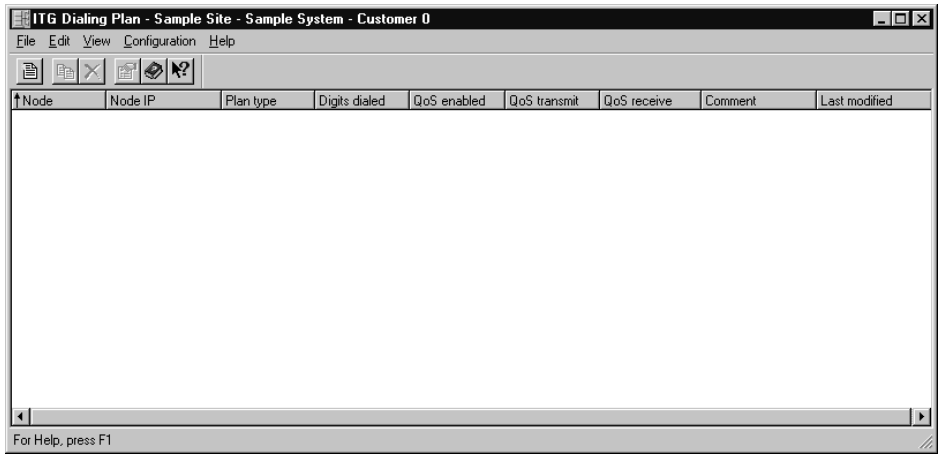
3 In the "AC1" box, enter the access code and check the boxes for the ESN translation types to which the access code applies.

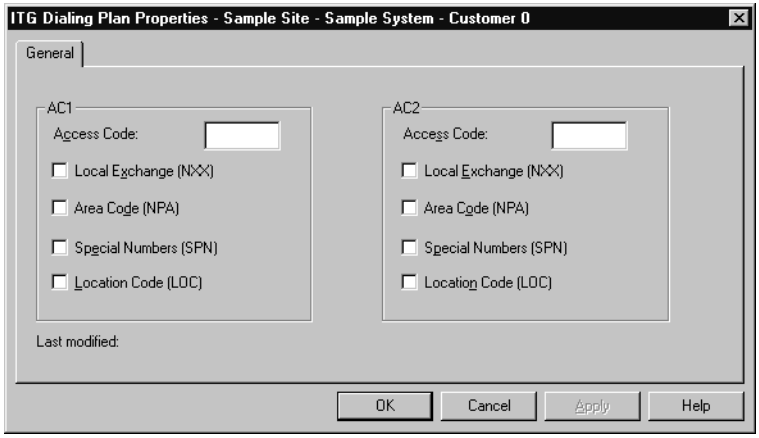
4 In the "AC2" box, enter the access code and check the boxes for the ESN translation types to which the access code applies.

Note: The checkboxes should match settings in the ESN overlays.

Note: Typically, the checkbox settings should be different between AC1 and AC2. For example, if LOC is checked for AC1, then it should not be checked for AC2.

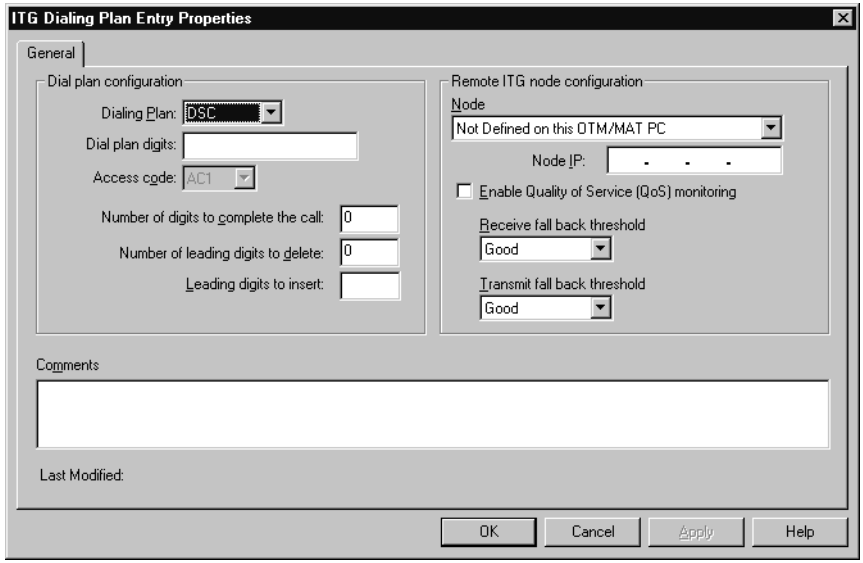
5 Click **OK**.


ITG Dialing Plan - Sample Site - Sample System - Customer 0
File Edit View Configuration Help
Node
Node IP
Plan type
Digits dialed
QoS enabled
QoS transmit
QoS receive
Comment
Last modified
For Help, press F1


ITG Dialing Plan Properties - Sample Site - Sample System - Customer 0
General
AC1
Access Code:
Local Exchange (NXX)
Area Code (NPA)
Special Numbers (SPN)
Location Code (LOC)
AC2
Access Code:
Local Exchange (NXX)
Area Code (NPA)
Special Numbers (SPN)
Location Code (LOC)
Last modified:
OK
Cancel
Apply
Help

Add dialing plan entries

1 In the “ITG Dialing Plan” window, select **Add** from the Configuration menu. The “Dialing Plan Entry Properties” window appears:



In the “Dialing Plan Entry Properties” window, configure the following:

2 From the Dialing plan pull-down menu, select the dialing plan translation type of LOC (Location Code), NPA (Area Code), NXX (Local Exchange), SPN (Special Number), DSC (Distant Steering Code), or TSC (Trunk Steering Code).

3 Select “AC1” or “AC2” from the “Access Code” pull-down menu, unless Distant Steeting Code (DSC) or Trunk Steering Code (TSC) has been selected. CDP steering codes (DSC and TSC) do not require AC1 or AC2.

4 In the “Dial plan digits” field, enter the dialed digits outpulsed by the Meridian 1 that will be translated into the Node IP address of the destination ITG node.

5 In the “Number of digits to complete the call” field, enter the total number of digits translated by ITG, including the number of digits in AC1 or AC2. This is used to determine when to stop waiting for digits dialed by the user and send the call setup message to the remote ITG node.

6 Two fields are provided in the ITG “Dialing Plan Entry” window to perform digit manipulation on the dialed digits that are contained in the outgoing setup message. If the ESN dialing plan is not uniform across the ITG network, the necessary digit manipulation for the different destination ITG nodes should be performed in each ITG dialing plan entry, not in the Meridian 1 Route List Block (RLB) containing the ITG tie trunk route.

Note: The digit manipulation in the ITG dialing plan entry does not apply when the ITG *Fallback to circuit-switched voice facilities* occurs.

7 In the “Number of leading digits to delete” field, enter the number of leading digits that are to be replaced.

8 In the “Leading digits to insert” field, enter the specific leading digits that are required by the destination ITG node for incoming calls on the ITG tie trunks into the remote Meridian 1 ESN node.

9 If the destination ITG node exists in the local MAT ITG database, it will appear in the “Node” pull-down list. Select the destination node that is associated with the “Dial plan” outpulsed dialed digits field. The Node IP address is inserted automatically.

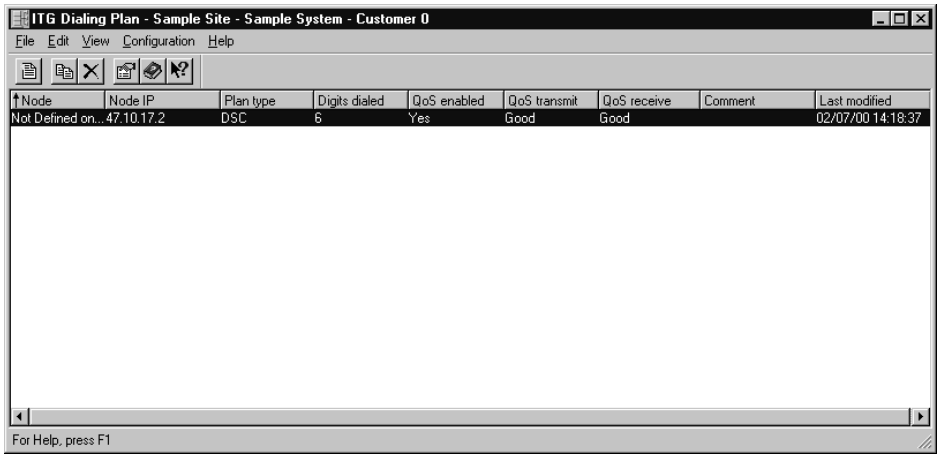
If the destination ITG node does not appear in the node pull-down list, select “Not defined on this MAT PC,” and type in the Node IP address in the “Node IP” field. Type in the site, system, and customer number and in the “Comments” field.

10 If *Fallback to circuit-switched voice facilities* will be configured, check the “Enable Quality of Service (QoS) monitoring” box. Appropriate alternate routes must be added in the RLB for the outgoing ITG calls on the Meridian 1 system.

11 From the “Receive fall back threshold” pull-down list, select the “Excellent, Good, Fair, or Poor” parameters according to network engineering guidelines. The default Quality of Service setting is “Good.”

12 From the “Transmit fall back threshold” pull-down list, select the “Excellent, Good, Fair, or Poor” parameters according to network engineering guidelines. The default Quality of Service setting is “Good.”

13 Click **OK**. The newly added dialing plan entry appears in the window.



14 Repeat the previous steps for each dialing plan entry that is required for the ITG network.

15 When you have completed all dialing plan entries, click the Close icon (X) in the right corner of the window.

Note: Some destination ITG nodes may have multiple dialing plan entries.

What to do next?

Once you have completed the configuration of the node properties and the MAT ITG dialing plan, there are two ways to proceed:

1 If the ITG cards are on site, you should proceed with "Install the ITG cards in the Meridian 1" on page 139, and then proceed to transmit the ITG node properties and dialing plan table information from MAT to the newly installed ITG cards. After the node properties are successfully transmitted, you will find it easier to configure and verify the card properties on MAT, before transmitting the card properties from MAT to the ITG cards.

2 If the ITG cards are not on site, you can proceed now to "Configure the properties of each ITG card" on page 149. After the ITG cards arrive on site, and have been physically installed in the Meridian 1 system, you can then proceed to transmit the ITG node properties, card properties, and dialing plan table.

Install the ITG cards in the Meridian 1

Physical placement of the cards

The ITG cards that have been added in MAT should now be installed in the Meridian 1. ITG cards require two card slots in the Meridian 1 IPE shelf, and may be installed in any position where there are two adjacent physical slots. Only the left slot requires connection to the Meridian 1 IPE backplane.

Option 11C Class A EMC guidelines

The NTCW80CA is approved for CISPR 22 Class A (and FCC Part 15 Class A) limits and approved to CISPR 22 Class B limits, resulting in compliance to CISPR 22 Class A by default.

You can install up to four boards total for the combined main and expansion cabinets (main cabinet code NTDK50GA or equivalent) - Class A Option 11. This can be expanded to four cards for the main cabinet and four each for any of the expansion cabinets, provided that the physical distance between each of the cabinets is a minimum of ten meters. Cards can be installed in any of the available IPE slots.

Option 11C Class B EMC guidelines

You can install up to two boards total for the combined main and expansion cabinet (main cabinet code NTDK50GA or equivalent) - Class A Option 11. This can be expanded to two cards for the main cabinet and two each for any of the expansion cabinets, provided that the physical distance between each of the cabinets is a minimum of ten meters. Cards can be installed in any of the available IPE slots.

Option 21 to Option 81, Class A and Class B

There are no limitations for Class A limitations. Four cards per system maximum for Class B installations. This can be expanded to four cards per column provided that the physical distance between each of the cabinets is a minimum of ten metres.

The ITG card can be configured as an EXUT card in slots 0 to 6 and 8 to 15 in an IPE shelf. The ITG card cannot be configured as an EXUT card in slot 7 of the IPE module, as this slot can only accommodate single-width cards and slots 7 and 8 are separated by the XPEC card. In Option 11E/11C systems, the ITG card can be provisioned in the main or expansion cabinets. In an Option 11 main cabinet the ITG card cannot be configured as an EXUT card in slots 9 or 10 if the Meridian Mail Card Option is present in card slot 10.

In order to accommodate the maximum number of ITG cards per module, each card should preferably be installed such that the left slot is an even-numbered slot and the ITG card is configured as an EXUT card in the even-numbered slot.

The ITG card may be configured as an EXUT card in an odd-numbered slot, if the maximum ITG card density per module is not required.

> ***Note:*** In some older IPE shelves only 16 tip and ring pairs are supported for most card slots. Since the ITG requires 24 tip and ring pairs in the left-hand card slot, the ITG card can only be configured as an EXUT card in slots 0, 4, 8, and 12 in these older shelves. Kits are available to modify the older shelves in order to bring out 24 tip and ring pairs per card slot.

Note: It is not necessary to install all ITG cards that belong to the same node in the same IPE shelf. For multi-card ITG nodes, it is recommended that the cards be provisioned in separate IPE shelves. This is to avoid total loss of IP trunking capability in case of the failure of a single IPE shelf.

CAUTION

Do not install an ITG card into an IPE card slot if that card slot has been configured for a central office trunk card. Before you insert the card into the card slot, disconnect the cable connecting this card slot to the MDF. Central office trunk cards may receive ringing voltage or other foreign voltage, which, when applied to the ITG card, may damage the card.

1 Identify the IPE card slots selected for the ITG card(s).

Note: Refer to and update the ITG card TNs on the ITG Installation Summary Sheet.

2 Remove any existing I/O panel cabling associated with any card formerly installed in the selected card slot.

3 Pull the top and bottom locking devices away from the ITG faceplate.

4 Insert the ITG card into the card guides and gently 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 remains lit until the card is configured and enabled in software, at which point in turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the ITG faceplate maintenance display to see start-up selftest results and status messages. A display of the type “F:xx” indicates a failure. Some failures indicate that the card must be replaced. “F:10” indicates Security Device test failure: check for presence of Security Device on the card. Refer to “ITG faceplate maintenance display codes for card reset” on page 220 for a listing of display codes.

Install cables

This section explains how to install the NTMF94DA E-LAN, T-LAN and serial interface and how to connect the NTAG81CA maintenance cable.

The NTMF94DA cable provides the E-LAN, T-LAN and serial interface for the ITG 1.0 card. Refer to "Cabling" on page 255 for pinouts and technical specifications. You must plug all ITG card T-LAN interfaces belonging to the same ITG node into the same T-LAN hub. Plug all ITG card E-LAN interfaces belonging to the same ITG node into the same E-LAN hub.

You must use Shielded Category 5 cable to connect to the E-LAN, T-LAN ports on the NTMF94DA cable. To conduct a ground loop test, turn to page 261 and follow the test procedure.

1 On large systems, connect the NTMF94DA E-LAN, T-LAN, and RS232 Serial Maintenance I/O cable to the I/O panel connector for the left hand card slot. If you have an Option 11, connect the cable to the I/O connector in the cabinet that corresponds to the ITG card slot (see Figure 26).

2 Connect a shielded Category 5 cable from the customer LAN/WAN equipment to the port labeled "T-LAN".

3 Connect a shielded Category 5 cable from the customer LAN/WAN equipment to the port labeled "E-LAN".

Install the NTAG81CA serial cable

You can install the NTAG81CA serial cable (shown in Figure 27) into the faceplate Maint port or in the serial port of the NTMF94DA interface cable. If required, use the NTAG81BA maintenance extender cable (see Figure 28).

WARNING

The serial maintenance ports presented at the faceplate and at the backplane are identical. Do not connect a terminal to both access points simultaneously. This will result in incorrect and unpredictable operation of the ITG card.

Note 1: The hub LEDs and the faceplate link LEDs light when you connect the card to the WAN/LAN through the E-LAN and T-LAN ports.

Note: Refer to the *Engineering Guidelines* section for more details about engineering and connecting the LAN/WAN.

Figure 26
NTMF94DA E-LAN, T-LAN and serial cable

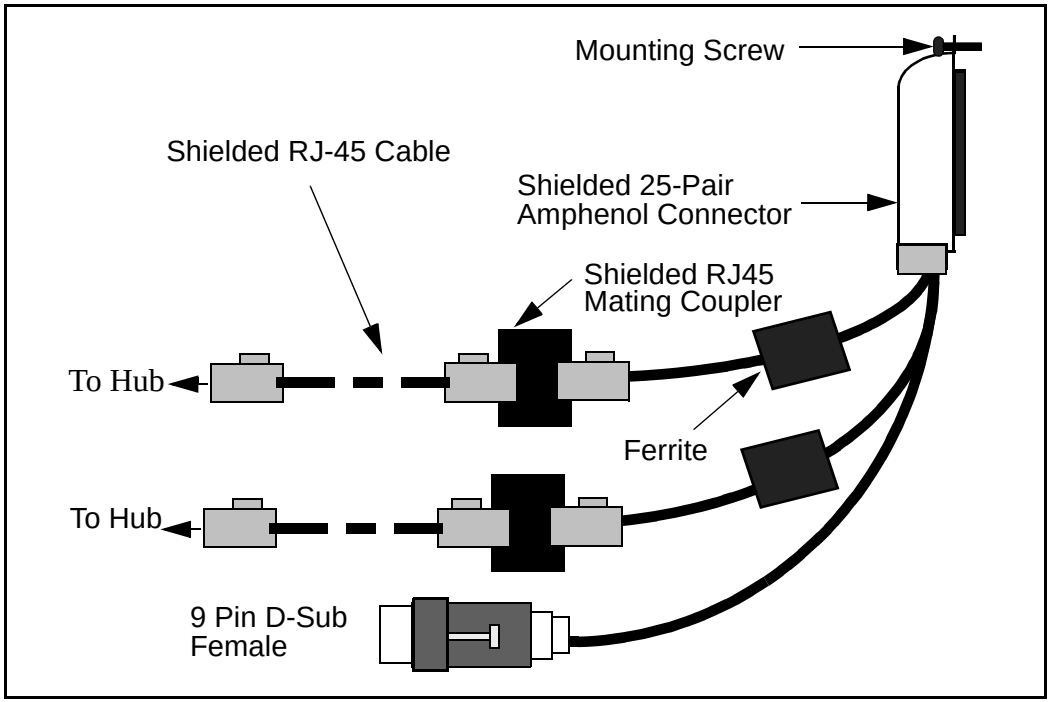


Figure 27
NTAG81CA Maintenance cable

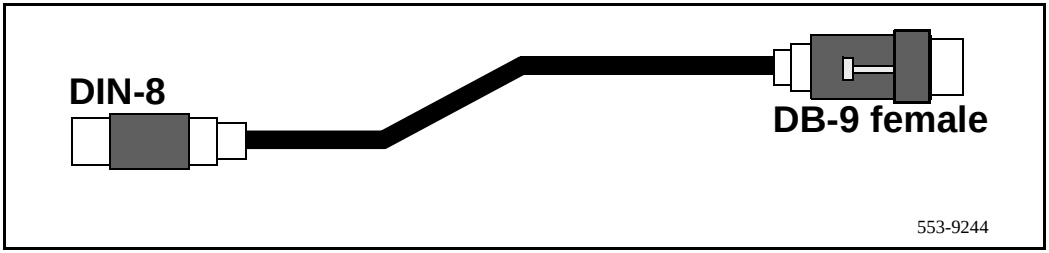
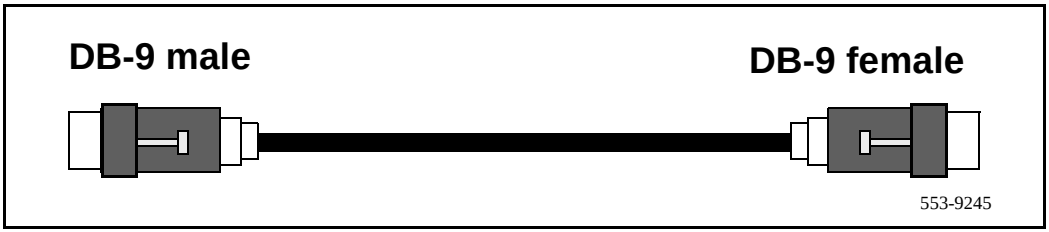


Figure 28
NTAG81BA Extender cable



Transmit ITG configuration information from MAT

Transmitting ITG configuration information from MAT to the ITG cards starts with configuration of the Leader 0, and proceeds to transmitting the node properties, transmitting the card properties and dialing plan, and verifying that the ITG cards have the correct software.

Set the Leader 0 IP address

1 Connect the MAT PC com port to the RS-232 serial maintenance port of the ITG Leader card via an NTAG81CA Faceplate Maintenance cable.
If required, use an NTAG81BA Maintenance Extender cable to provide an extension between the NTAG81CA Faceplate Maintenance cable and the MAT PC. Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTMF94DA I/O Panel Ethernet and Serial Adaptor cable to create a more permanent connection to the ITG card maintenance port.

2 Use the following communication parameters for the TTY terminal emulation on the MAT PC: 9600 baud, 8 bits, no parity bit, one stop bit.

When a new ITG card 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 **+++** and then press **Enter** to bring up the ITG shell command line prompt:

...+++

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:
setLeader "xx.xx.xx.xx","yy.yy.yy.yy","zz.zz.zz.zz", and press **Enter**.

Where:

- "xx.xx.xx.xx" is the IP address of the management interface on Leader 0,
- where "yy.yy.yy.yy" is the Gateway IP address for the management interface on Leader 0. If the MAT PC will be connected directly to the LAN, then the Gateway IP address is "0.0.0.0".
- and where "zz.zz.zz.zz" is the subnet mask for the management interface on Leader 0.

"setLeader" parameters description

All ITG shell commands are case-sensitive. The three parameters must each be enclosed in quotes, and that there must be a comma and no spaces between the "xx.xx.xx.xx" and "yy.yy.yy.yy" parameters and between the "yy.yy.yy.yy" and "zz.zz.zz.zz" parameters.

The **Gateway IP address** is used on reboot to create IP route table default network route only if 1) there is no active leader that has this card's MAC address in its bootp.1 file, and 2) this card's bootp.1 file is empty (size 0 Kb).

IP addresses and subnet masks must be entered in dotted decimal format.

The **subnet mask** may be expressed in Classless Inter-Domain Routing (CIDR) format, appended to the IP address. For example 10.1.1.1/20. To convert subnet mask from CIDR format to dotted decimal format refer to *Appendix C*.

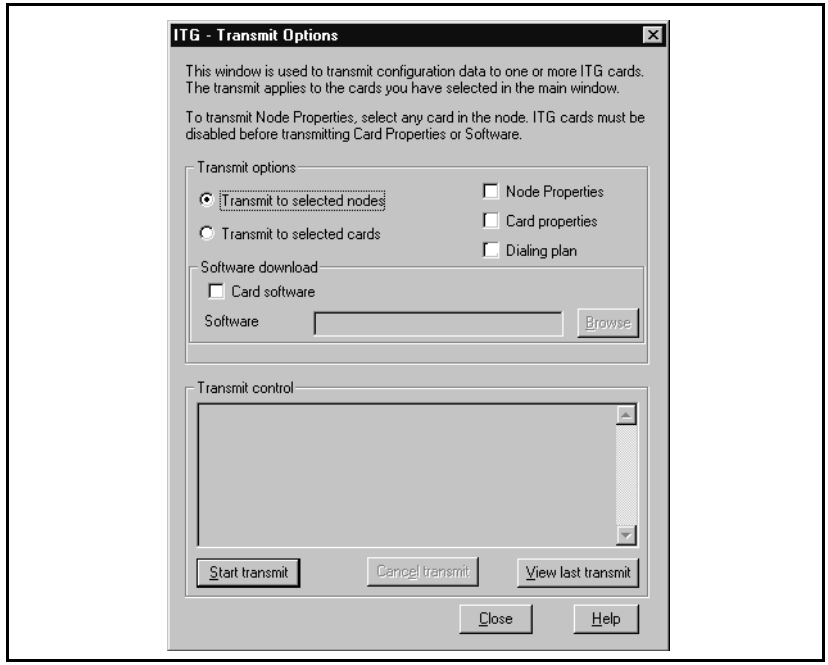
Leader 1 card will automatically be set as a leader after node properties are successfully transmitted.

5 Reboot the Leader 0 ITG card.

After the reboot, the Leader 0 card will be in a state of “backup leader”. It cannot yet be in a state of “active leader”, because it is missing the node properties (bootp.1 bootp table file). After MAT successfully transmits the node properties to Leader 0 card, it can enter the state of the “active leader”.

Transmit node properties

1. Launch the Meridian Administration Tools application on the MAT PC.
2. From the “MAT Navigator” window, double-click the **ITG M1 IP Trk** icon from the “Services” folder. The “IP Telephony Gateway” window opens.
3. In the “IP Telephony Gateway” window, select Leader 0 or any card from the node.
4. Click **Configuration** | **Synchronize** | **Transmit.** The “ITG - Transmit Options” window appears.



5 Leave the radio button default setting of “Transmit to selected nodes”. Check the “Node Properties” check box only.

Note: Card Properties and Dialing Plan will be transmitted in “Transmit Card Properties and Dialing Plan” on page 156.

ITG cards are delivered with software pre-installed in the onboard flash memory, so a transmitting new card software may not be required during installation. After the Node Properties have been transmitted and MAT has established communication with the ITG card, you will verify the software on the cards. To re-install or upgrade to a new version, refer to the *Administration and maintenance* chapter.

6 Click the **Start Transmit** button. Monitor progress in the “Transmit Control” window. Confirm that the node properties are transmitted successfully.

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

8 Reboot the Leader 0 ITG card.

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 Leader 1 card is now auto-configured, reboots automatically, and enters the state of “backup leader”. Any follower cards are now auto-configured with their IP addresses. MAT ITG should now be in communication with all cards in the ITG node.

1 From the MAT “IP Telephony Gateway” main window, select **View|Refresh**, and verify that the card status is showing “unequipped”. If any cards still show “not responding”, verify the management interface cable connection to the E-LAN, and verify the management interface MAC addresses that were entered previously on the “Configuration” tab of the Node Properties, while adding the ITG node on MAT.

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 “IP Telephony Gateway” main window, and select **Configuration|Node|Properties** from the drop-down menus. Compare the values displayed on the “General” tab and “Configuration” tab with those on the ITG Installation Summary Sheet.

What to do next?

Once you have successfully transmitted the node properties, there are two ways to proceed.

1. If you have previously configured the card properties of each ITG card in the node, you should proceed to "Transmit Card Properties and Dialing Plan" on page 156.
2. If you chose to configure the card properties of each ITG card in the system after you physically installed the ITG cards in the Meridian 1 system, you may now proceed to "Configure the properties of each ITG card" on page 149.

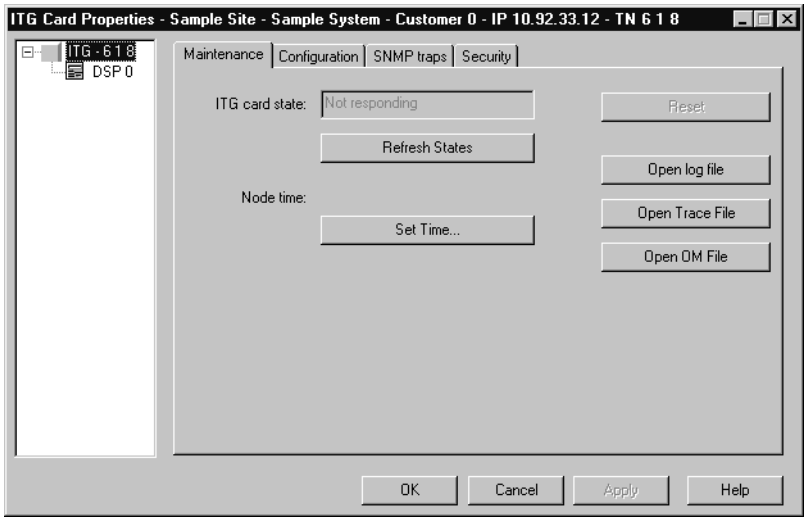
Configure the properties of each ITG card

This procedure may be used before or after you physically install the ITG cards in the Meridian 1. The appearance of the MAT ITG "Card Properties" will differ depending on whether the cards are present and responding, or not yet physically installed:

- If the cards are present and responding, DSP 0 and DSP 1 will both appear in the left side of the window. On the "Maintenance" tab, "ITG card state" will show "Unequipped." On the Configuration tab, the "S/W release" and "Security Device (NT_SDID)" will show the values actually read from the card.
- If the cards have not yet been physically installed, only DSP 0 will appear in the left side of the window. On the "Maintenance" tab, "ITG card state" will show "Not responding." On the Configuration tab, the "S/W release" and "Security Device (NT_SDID)" will show nothing.

To configure the ITG cards, do the following:

1. In the "IP Telephony Gateway" window, double-click on an ITG card to display the "ITG Card Properties" window. Leave the ITG card icon selected in the left side of the window.
2. If the ITG Leader 0 card is present and responding, you should set the time on the "Maintenance" tab of.the card properties for Leader 0. If not, you must remember to come back and set the time on the Leader 0 card after the card is physically installed.



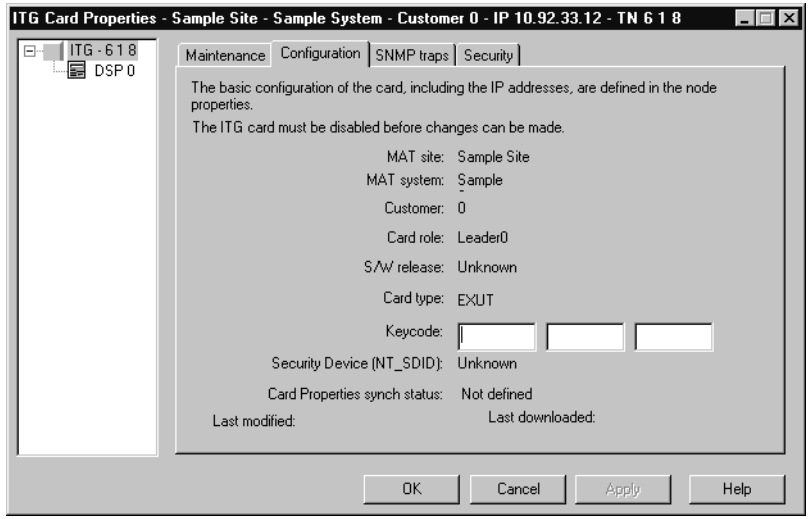
3 Click the **Configuration** tab.

4 Verify that all cards in the same ITG node are running the same software version, and that the “S/W release” shows the latest recommended software version.

- If the software needs to be updated, refer to “Upgrade ITG card software (if required)” on page 158.
- If the cards are not present and responding, you must remember to come back and verify the software version.

5 Enter the keycode into the keycode field. Refer to the Software License document for the keycode. The keycode is 24 digits, consisting of 3 groups of 8 alphanumeric characters. Optionally, the keycode can be copied from a file and pasted into the first field. If the cards are present and responding, compare the keycode and “Security Device NT_SDID” displayed with the ITG Installation Summary Sheet.

6 Click the **SNMP traps** tab.

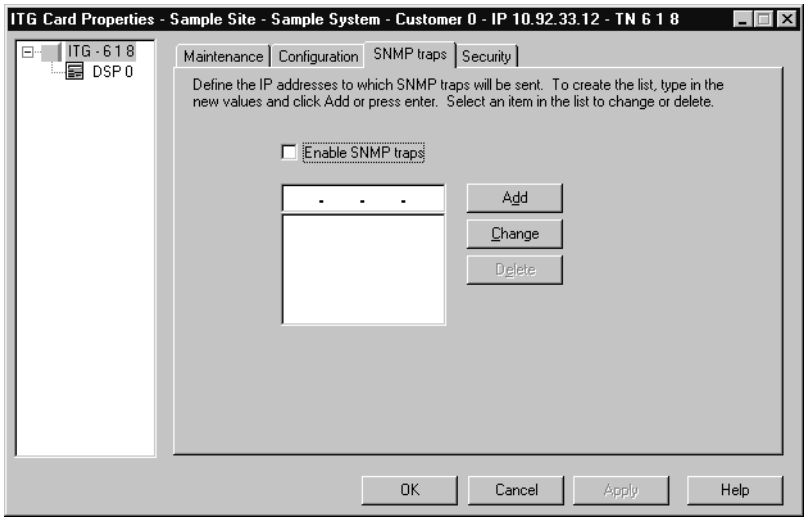


Note 1: The term “SNMP trap” refers to the sending of ITG error messages to the locations specified by the SNMP Manager IP addresses. Checking the “Enable SNMP traps” box will enable sending of SNMP traps to the SNMP managers that appear in the list.

Note 2: Refer to “Activate SNMP traps for ITG” on page 170 to configure MAT Alarm Notification to monitor SNMP traps for ITG cards.

7 To add an SNMP Manager IP address, type the address in the entry field, and click **Add**. You should add SNMP Manager IP addresses for:

- the local MAT PC
- PPP IP address configured in the Bay Networks Netgear RM356 Modem Router, or equivalent, on the E-LAN for the remote support MAT PC
- the SNMP manager for remote alarm monitoring via SEB2 and IRIS nGEN (if present).
- Any remote MAT PCs on the customer’s IP network.



Change SNMP community name

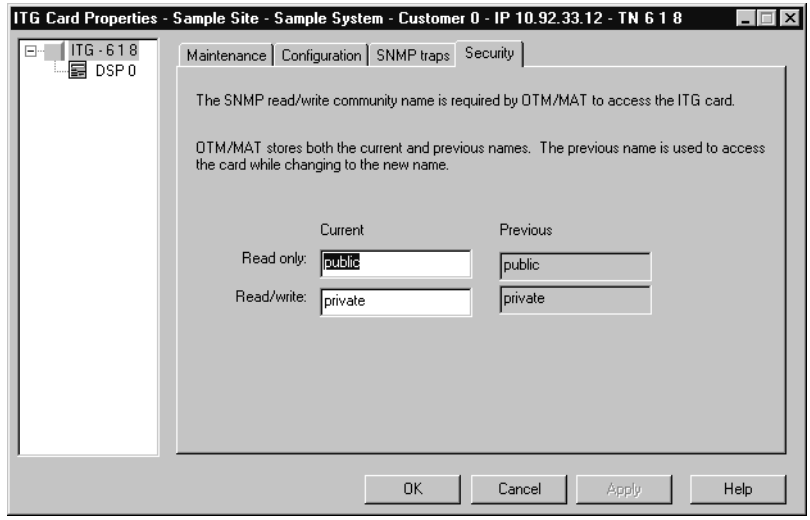
SNMP community name is equivalent to a password. The community names should be changed from the defaults in order to provide better security for the ITG node. This SNMP community name is used by MAT ITG to refresh the node status, and to control the transmitting and retrieving of files.

1 Click the **Security** tab and enter the new “Read only” and “Read/write” card SNMP community name. MAT will use the previous community names to transmit the card properties and thereafter the current and previous fields will both show the new community names,

2 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 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.

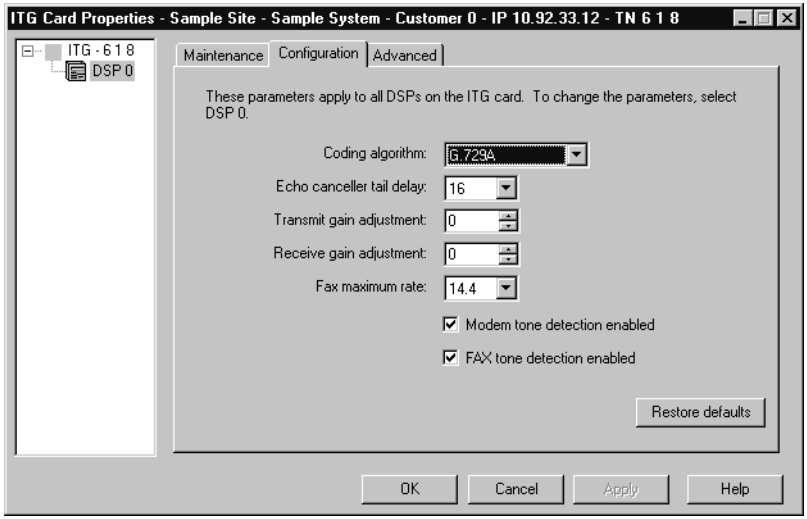
Configure ITG card DSP properties

Note: The properties of all DSPs on an ITG card are modified by configuring the properties for "DSP 0" on an ITG card. The "Restore defaults" button can be used to restore all default values including restoring the coding algorithm to G.729A.

CAUTION

The default DSP parameters for each codec are suitable for most applications. If you are not an expert in voice over IP, do not modify them. Refer to the *Administration* section for more details.

1 Click to select the **DSP 0** icon underneath the ITG card. Click the **Configuration** tab.



2 Select the "Coding algorithm" (codec) according to your ITG network engineering plan. Refer to the *Engineering Guidelines* section.

The "DSP coding algorithm", or codec, pull-down menu has the following options: "G.711 A-law", "G.711 Mu-law", "G.729", "G.729A" (default),"G.723.1 5.3K," and "G.723.1 6.3K."Click **Apply** then **OK**.

3 Repeat the previous steps to configure the card and DSP properties for each ITG card.

Disable or enable silence suppression (Voice Activity Detection (VAD))

Silence suppression must be disabled or enabled according to your ITG network engineering plan. Refer to “Silence suppression or Voice Activity Detection” on page 57 in the Engineering Guidelines section.

Silence suppression or VAD must be enabled or disabled on a card by card basis similar to other card properties.

After changing the configuration of silence suppression from enabled to disabled, or vice versa, the card properties must be retransmitted from MAT in order to apply the silence suppression changes to the ITG cards.

Disabling silence suppression *approximately doubles* LAN/WAN bandwidth usage. Do not change this unless instructed by the IP network engineer.

1 In the MAT ITG window, select the first card for which silence suppression configuration needs to be changed.

2 Right-click the ITG card and select **Telnet to card**.

3 When the “VxWorks login:" prompt appears, enter the default user name, **itgadmin**.

4 When the “password” prompt appears, enter the default password, **itgadmin**.

5 If the login is unsuccessful, then check that you have the correct user name and password.

6 At the “>” prompt enter **itgVADShow**.

The output appears as this:

Voice Activity Detection configured: ENABLED (DISABLED)
Voice Activity Detection currently on DSP: ENABLED (DISABLED)

7 If the silence suppression (or VAD) must be DISABLED then enter the command **itgSetVAD 0** (0 equals OFF).

The output of this command will be the same as the 'itgVADShow' command, except that the value at the end of the first line will reflect the configuration setting changed, and the second line will show that the setting of the DSP has not changed.

8 If the silence suppression (or VAD) must be ENABLED according to the IP network engineer, then enter the command **itgSetVAD 1** (1 equals ON).

The output of this command will be the same as the 'itgVADShow' command, except that the value at the end of the first line will reflect the configuration setting changed, and the second line will show that the setting of the DSP has not changed.

What to do next?

Once you have completed the configuration of the card properties, you will proceed to "Transmit Card Properties and Dialing Plan" on page 156.

Transmit Card Properties and Dialing Plan

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

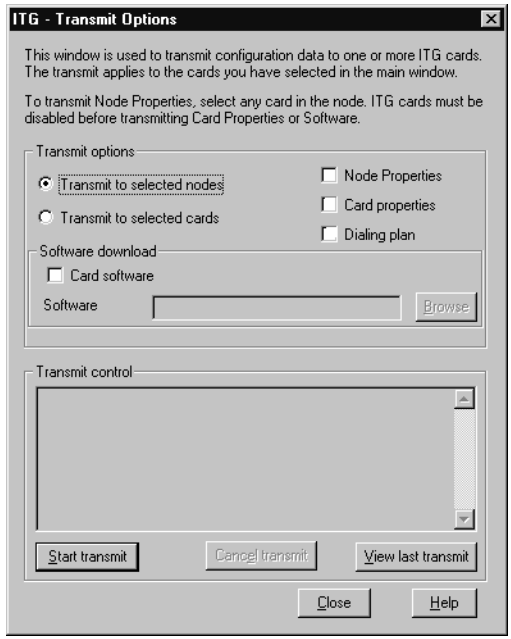
> ***Note:*** It is not necessary to disable ITG cards when transmitting a dialing plan alone.

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" main window, select **View | Refresh** and verify that the card status is showing "Disabled" or "Unequipped." Cards without a valid keycode will show "Unequipped."

1 In the "IP Telephony Gateway" window, select Leader 0 or any card from the node

2 Click **Configuration** | **Synchronize** | **Transmit.** The "ITG - Transmit Options" window appears.

3 Leave the radio button defaulted to "Transmit to selected nodes". Check the "Card properties" and "Dialing plan" boxes only.



4 Click the **Start Transmit** button.

The transmission status is displayed in the “Transmit control” box. Confirm that card properties and dialing plan are transmitted to all cards successfully.

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

6 Use the overlay 32 ENLC command to re-enable the ITG cards.

7 In the “IP Telephony Gateway” main window, select **View | Refresh**. The card status should now show “Enabled.”

8 Verify the TN, management interface MAC address, IP addresses, the NT-SDID, and keycode for each ITG card. The NT_SDID and keycode are verified by double-clicking each ITG card in the MAT "IP Telephony Gateway" main window and clicking the “Configuration” tab of the Card Properties. Compare the displayed values with those 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 as soon as the Meridian 1 PBX has been configured with route data blocks and trunk data blocks and the destination ITG nodes are configured to a similar stage.

Verify card software

In the IP Telephony Gateway window, starting with the Leader 0 ITG card, double-click each ITG card to open the ITG Card Properties window. Leave the default selection of the ITG card in the Card Properties window, and click the "Configuration" tab. The software release is displayed on this tab.Verify the software release from each card is the latest recommended software release for ITG. The website URL to check the latest recommended ITG software release is "http://www.nortel.com/secure/cgi-bin/itg/enter.cgi" If any of the cards require a software upgrade, refer to the next procedure, *Upgrading ITG card software*.

Upgrade ITG card software (if required)

1 Download the MAT ITG software from the World Wide Web (WWW) to the MAT PC hard drive. Open a browser on the MAT PC and connect to WWW address:
http://www.nortel.com/secure/cgi-bin/itg/enter.cgi

Once connected to the site, enter the username and password. Select the latest recommended software version and select the location on the MAT PC hard drive where it is to be downloaded. Record the MAT PC hard drive location for use later in the procedure.

2 Open MAT and launch the "**ITG M1 IP Trk**" application, if not already opened.

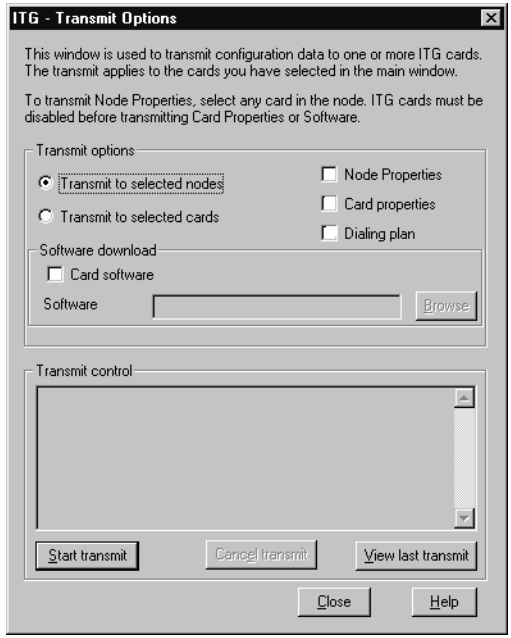
3 Verify the current software version of the ITG cards to be upgraded. To check the software version, double-click a card and click the "Configuration" tab where "S/W version" displays the current software version as read from the ITG card.

4 Select the cards from the main card list view that are to be upgraded. Upgrade all the cards in the node together, unless you are installing a spare card that has older software.

5 Disable all ITG cards to be upgraded. Use the Meridian 1 overlay 32 DISI command from 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 verify that the card status is showing “Disabled.”

7 Select **Configuration | Synchronize | Transmit**. The “ITG - Transmit Options” dialog box is displayed.



8 In the “Transmit Options” group box, select the radio button “Transmit to selected cards.”

9 In the “Software Download” group box check “Card software.”

10 Click on the **Browse** button to locate the ITG card software that was downloaded earlier from the website. Select the software file and click **Open** to save the selection. The path and file name of the ITG card software appears in the edit box next to the “Browse” button.

11 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 progress in the “Transmit Control” window. Confirm that the card software is transmitted successfully to all cards. Note any error messages, investigate, correct any problems, and repeat card software transmission until it is completed successfully on each ITG card. The cards continue to run the old software until they are rebooted.

12 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 successfully rebooted and are responding again to the MAT ITG status refresh (disabled: active; disabled: backup; disabled).

These cards should be remain in the “Disabled” state after the upgrade, so that the craftsperson can issue a “Reset” command from the Maintenance menu or the “Maintenance” tab in the “ITG Card Properties” window to each card to reboot them. Alternatively, the cards can be reset by pressing the “Reset” button on the card faceplate using a pointed object.

13 Double-click each upgraded card and verify the software version on the “Configuration” tab of the Card Properties.

14 Use the overlay 32 ENLC command to re-enable the ITG cards.

The software upgrade procedure is complete.

Add ITG configuration data on a Meridian 1

Configure ITG trunk routes

The Meridian 1 must be configured with new trunk routes for the ITG TIE trunks, via the MAT System Passthru terminal, ESN MAT application, or via a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1.

Read all **Notes** in this section before configuring ITG Route Data Blocks.

LD 16 – Configure the new trunk routes.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	RDB	Route Data Block.
CUST	0-99	Customer number.
ROUT	0-511	Route number.
DES	IP TELEPHONY GWY	16 character description is “IP TELEPHONY GWY,” or “ITG” and a specific description if more than one ITG route exists.
...	...	...
TKTP	TIE	Trunk type.
SAT	YES	Required for ITG *Fallback to circuit-switched voice facilities* feature. *See Note 1.*
...	...	...
DTRK	NO	Not for a digital trunk route.
ICOG	IAO	Incoming and outgoing route.
SRCH	LIN	Linear search method. *See Note 2.*
ISDN	NO	No ISDN support.

...	...	...
SIGO	STD	Standard signaling arrangement. *See Note 3.*
CNTL	YES	Changes to controls or timers.
NEDC	ETH	Near End Disconnect Control: either end.
FEDC	ETH	Far End Disconnect Control: either end.

Note 1: Satellite link control should be enabled to allow *Fallback to circuit-switched voice facilities* to use the next available entry in the Route List Block. Satellite link control will also prevent tandem connections of ITG trunks.

Note 2: SIGO (outgoing signaling protocol) should be set to STD (no proprietary protocol signaling). ITG 1.0 does not support Meridian 1 network signaling such as ESN5.

Note 3: SRCH (outgoing search method) should be set to LIN (linear) to minimize glare conditions on ITG routes carrying incoming and outgoing traffic. The Meridian 1 will search from the highest route member to the lowest for an idle outgoing trunk.

Configure CPND name for ITG route ACOD

A descriptive name should be configured for the ITG route access code (ACOD) to take the place of the Calling Line ID (CLID) and Call Party Name Display (CPND). ITG 1.0 provides non-ISDN tie trunks, therefore the Meridian 1 MCDN features CLID and CPND are not available for calls that are routed by ITG tie trunks between Meridian 1 PBXs.

LD 95 – Call Party Name Display.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	NAME	
CUST	xx	The customer number for the ITG node.
DIG	<CR>	

DN	x...x	The ITG tie route ACOD.
NAME	IP Telephony Gwy	Recommended name for ITG route.
...	<CR>	Repeat <CR> response until 'REQ.'

The CPND name "IP Telephony Gwy" will be displayed on Meridian Modular Terminal telephone sets when calls are received that have been routed over the ITG trunks. This will help the called parties to understand why they have not received the CLID and Call Party Name Display, and will help in isolating telephony problems that may or may not be related to the ITG tie trunks.

For outgoing ITG tie trunk calls "IP Telephony Gwy" will be displayed on Meridian Modular Terminal telephone sets when a call has been placed on 'Hold' and then retrieved. Again this will help in isolating problems that may or may not be related to the ITG tie trunks.

Configure the ITG cards and trunk units

LD 14 – Configure the ITG cards.

Prompt	Response	Description
REQ	NEW 8 NEW 4	Add new data. Configure 8 units on the EXUT ITG card. Add new data. Configure 4 units on the ITG card (G.729). *See Note 2.*
TYPE	TIE	TIE trunk.
TN	l s c u	TN of the trunk.
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 1-7 the ITG card management IP address.
XTRK	EXUT	Trunk type emulated by the ITG card.
...	...	...
CUST	0-99	Customer number.

NCOS	0-99	For *Fallback to circuit-switched voice facilities*, FRL of NCOS must be greater than FRL in alternate routing entries of ESN Route List Block.
RTMB	rrr mmm	Route and member number. *See Note 3.*
SIGL	LDR	Loop dial repeating trunk signaling.
STRI	WNK	Start arrangement incoming.
STRO	WNK	Start arrangement outgoing.
SUPN	YES	Answer and disconnect supervision.
CLS	DTN	Digitone class of service.

Note 1: Use the "NEW 8" 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 MAC address, see the ITG information entry sheet. MAC addresses are labeled on the ITG card faceplate.

Note 2: When using the G.729 only four DSP channels are supported, and only trunk units 0, 1, 4, and 5 must be configured.

Note 3: Assign route member numbers to cards in the same order as the default order in the MAT ITG window (i.e, Leader 0 is members 1-8; Leader 1 is members 9-16; first follower is members 17-24).

Note 4: Only Wink Start arrangement is supported.

Note 5: Digitone class of service is recommended for faster call setup. Dial pulse (DIP) class of service is also supported.

Configure the Meridian 1 ESN dialing plan for the ITG network

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 dialing plan information (as configured in "Add an ITG node on MAT by retrieving an existing node" on page 128) must correspond.

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.

> ***Note:*** *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*. 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.

When a Meridian 1 PBX 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 excessively low audio level, silence suppression should be disabled using the ITG shell command 'itgSetVAD 0'.

Disabling silence suppression *approximately doubles* LAN/WAN bandwidth usage. Disabling silence suppression consumes more real-time on the ITG card. To avoid real-time capacity problems on the ITG card when silence suppression has been disabled, you should set the voice payload to 20 ms or 30 ms for the G.711 and G.729A codec types. This restriction is not required for other codecs types.

> ***Note:*** When silence suppression is disabled, if the craftsperson happens to set a payload size of 10 ms for the G.711 or G.729A codec types, the ITG card software will automatically reject the settings and use a 20 ms payload size instead.

LD 86 – ESN configuration.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in overlay 15.
FEAT	ESN	Electronic Switched Network.
...	...	...
CDP	YES	Coordinated Dialing Plan feature.
...	...	...
AC1	xx	NARS/BARS Access Code 1.
AC2	xx	NARS/BARS Access Code 2.
...	...	...

LD 86 – Route List Index configuration.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in overlay 15.
FEAT	RLB	Route List Data Block.
RLI	xxx	Route List Index.
ENTR	xxx	Route List Entry for the ITG route.
...	...	...
ROUT	0-511	ITG tie trunk route number.
DMI	xxx	Digit manipulation table to insert ESN AC1 or AC2 (see note). **Not required for CDP steering codes**.
ENTR	xxx	Route List Entry for the Fallback route.
ROUT	0-511	Alternate route for “Fallback to circuit-switched trunk facilities”
FRL		NCOS of ITG tie trunks must have FRL equal to or greater than the FRL of the alternate route.

Note: Digit manipulation table for ITG tie trunk entry in the RLB must only insert AC1 or AC2, depending on the network translations that point to this RLI. Any digit manipulation for a specific destination node must be done in the ITG card dialing plan entry.

LD 87 – Coordinated Dialing Plan configuration.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in overlay 15.
FEAT	CDP	Coordinated Dialing Plan.
TYPE	LSC DSC	Local Steering Code. Distant Steering Code.
...	...	...
RLI	xxx	Route list index created in overlay 86.
...	...	...

LD 90 – Network translation table configuration.

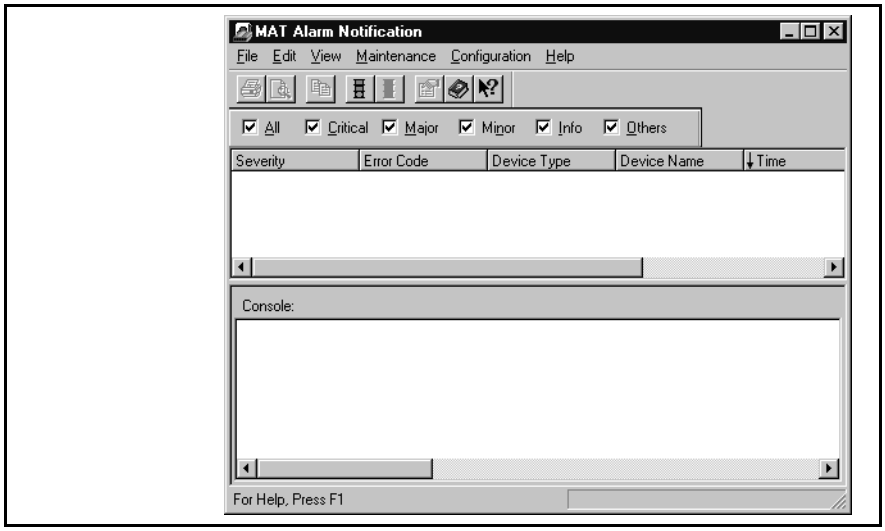
Prompt	Response	Description
REQ	NEW PRT	Add new data. Print data block.
CUST	xx	Customer number as defined in overlay 15.
FEAT	NET	Network translation tables.
TRAN	AC1 AC2 SUM	Access Code 1 (NARS/BARS) Access Code 2 (NARS) Summary of Network Translations (allowed when REQ=PRT)
TYPE	NPA NXX LOC	Numbering Plan Area code translation data block. Central Office Code Translation data block. ESN Location Code translation data block.
...	...	...
RLI	xxx	Route list index created in overlay 86.
...	...	...

Note: After making changes to the network translation table, then make a new set of test calls using the ESN translation.

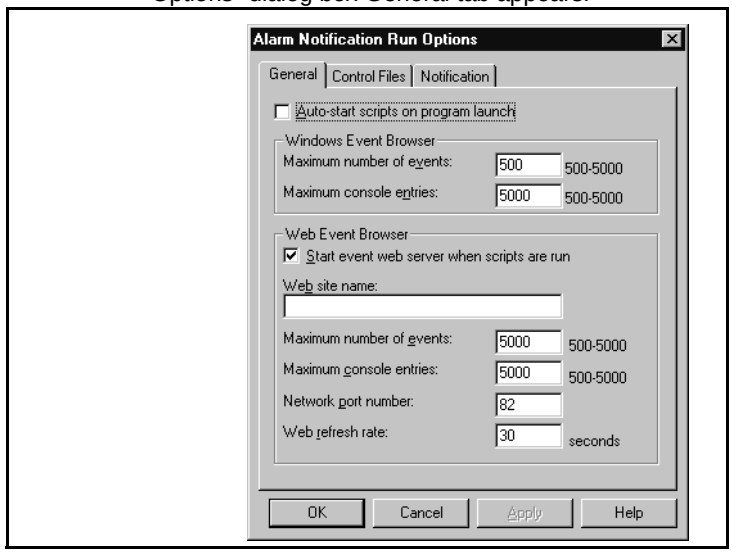
Activate SNMP traps for ITG

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

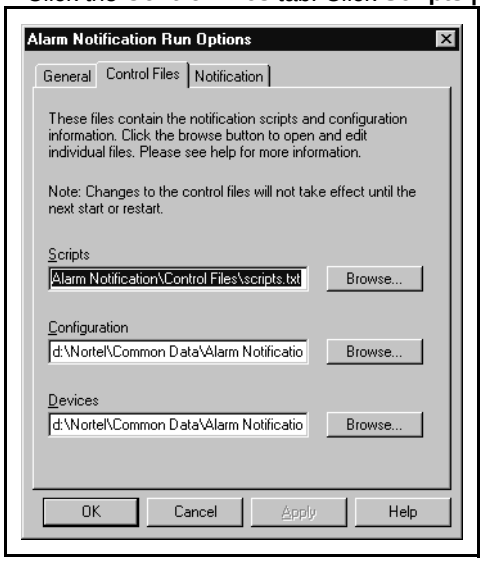
.



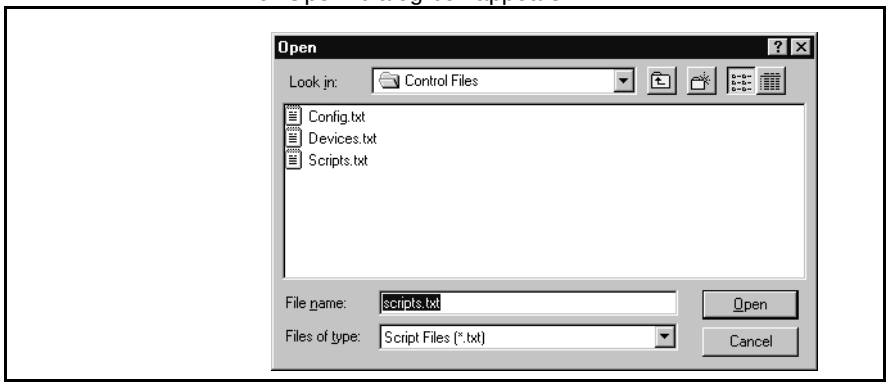
2 Select **Configuration|Run|Options**. The "Alarm Notification Run Options" dialog box General tab appears.



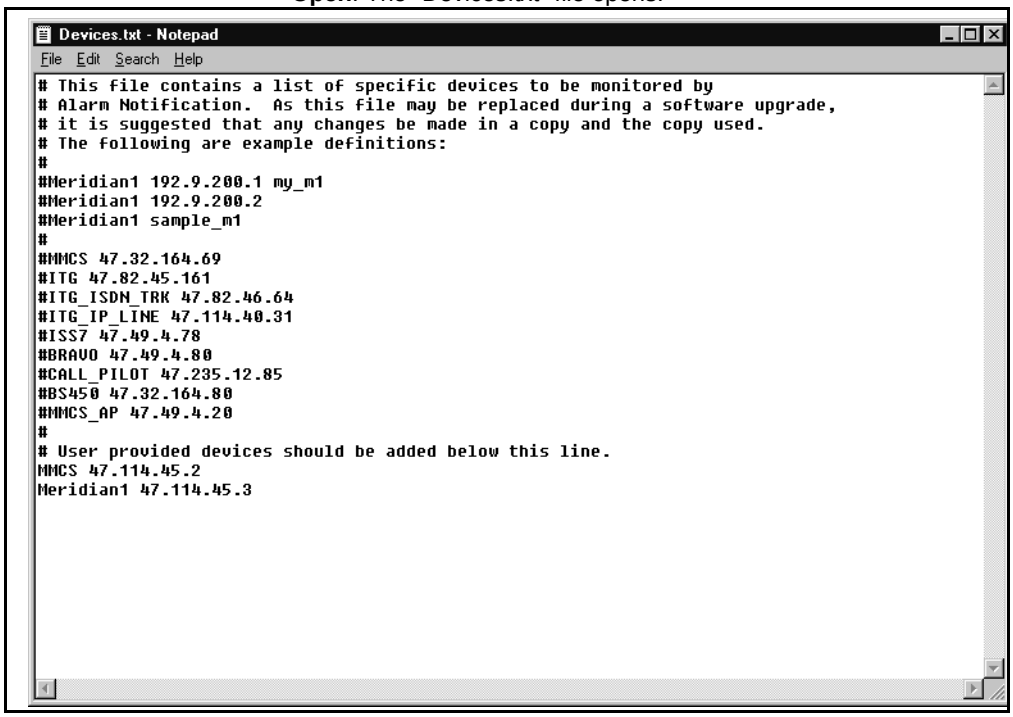
3 Click the **Control Files** tab. Click **Scripts | Browse**.



The "Open" dialog box appears.



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



5 For each ITG card in each monitored ITG node, add a line consisting of three fields separated by spaces. Enter the first line beginning underneath the last line that begins with a "#".,

Table 23
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

6 Click **File|Save**.

7 In the "Alarm Notification Run Options" window, click **Apply** then **OK**.

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

8 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.

9 If MAT Alarm Notification is not running (i.e., green traffic light showing on the tool bar), start it by clicking on the green traffic light to change it to red.

10 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.

Enable the ITG cards in LD32

1 Use LD 32 via the TTY or MAT overlay passthru to enable the ITG cards with the following command: **ENLC l s c**.

2 Repeat the above step for each ITG card.

Make test calls to the remote ITG nodes

Make test calls to ensure that the ITG system can process calls from each node to remote node, and that quality of service, as defined within the Dialing Plan window, is acceptable. Check the ITG operational report, as described in the *Administration* chapter.

Administration

ITG Trunk 1.0 administration tasks are performed in MAT, through a Command Line Interface and through the Meridian 1 Overlays.

MAT Administration Tools

The majority of ITG commands are performed through MAT, and specific tasks are described in “ITG MAT OA&M tasks” on page 183. The MAT ITG application is accessed by clicking the “ITG M1 IP Trk” icon in the “MAT Navigator” window in the “Services” folder. For basic information, refer also to “Basic interface of common MAT ITG windows” on page 176.

Command Line Interface

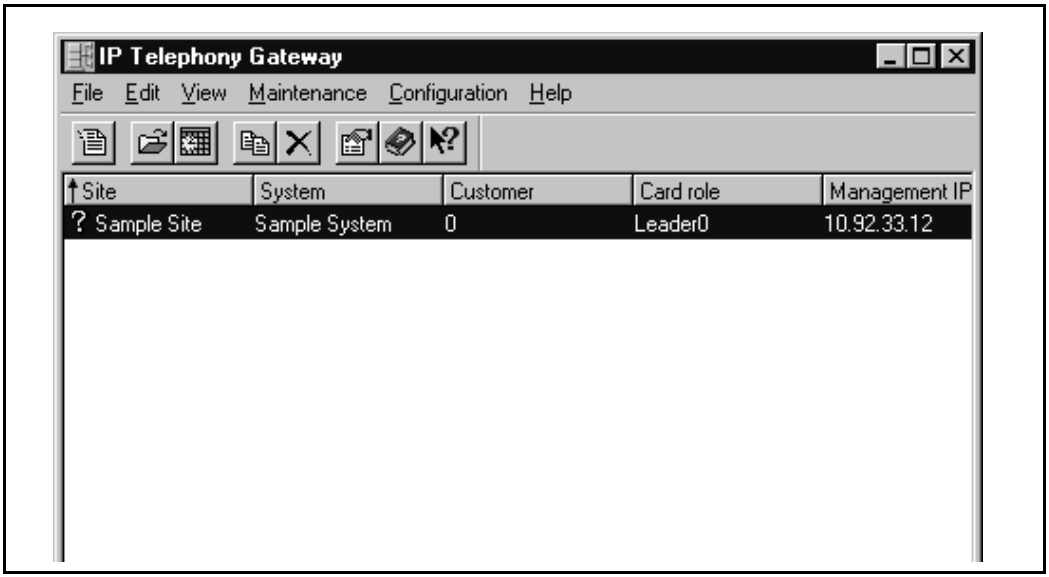
The RS-232 MMI port on an ITG card, which is connected directly to a VT-100 type terminal or to a PC running a terminal emulation program. Once connected, a command-line interface referred to as the ITG shell is available. ITG shell commands are described in “ITG shell command-line interface access via Telnet or maintenance port” on page 206, and a ITG shell commands are listed in the *Maintenance* section. Use the following parameters on the TTY: 9600 baud, 8 bits, no parity bit, one stop bit.

Meridian 1 system commands

- Meridian 1 system commands as described on page 213.
  The ITG card uses the existing commands and messages used for the NT8D14 Universal Trunk (EXUT) card.

Basic interface of common MAT ITG windows

When the “ITG M1 IP Trk” icon is clicked from the “Services” folder in the “MAT Navigator” window, the window that first opens is the “IP Telephony Gateway” window.



The “IP Telephony Gateway” window contains a list of all ITG cards defined by the user. Information stored about the ITG cards includes their associated Site, System, Customer, IP/MAC addresses, TN, synch status, and the SNMP community name.

When the window is launched, the application attempts to get the status of each ITG card. This involves sending an SNMP “get” message to the ITG card using the SNMP community name stored for each card. If the SNMP “get” message is successful, it retrieves the card and fallback states and displays this information is the list. If the “get’ message is not successful, the card state field indicates this condition, the fallback state is set to “unknown”, and an alarm icon is displayed in the first column.

"IP Telephony Gateway" window column definitions

Site The site name defined in MAT Common Services.

Card role Leader 0 (Leader), Leader 1 (Backup Leader), or Follower as defined in the Node properties.

Management IP Management IP address as defined in the Node properties.

TN Terminal number of the trunk portion of the ITG card.

Card state Card state received from the card from SNMP.

Nodes in fallback The number of remote ITG nodes that are in a fallback to PSTN routing state due to Quality of Service thresholds. For example, if there are 10 nodes in the network and a Leader card puts calls to 2 remote nodes into fallback routing, then the number 2 is put in this column for the active Leader. The screen must be refreshed to show the current status.

Node synch status The status of the node properties between MAT and the ITG node. The status can be:

- "Undefined": a new ITG card has been added in "ITG node properties," but the card properties have not been configured.
- "Transmitted": the node properties has been downloaded to the Leader card from MAT successfully.
- "New": a new ITG card has been added in the "ITG node properties" window, but not downloaded to the Leader card.
- "Changed": an IP/MAC address has changed, but a card has been deleted, but not download to the Leader card has occurred.
- "Deleted": an ITG card has been deleted from the "ITG Node Properties" window, but not download to the Leader card has occurred.

Dial plan synch status The status of the dialing plan between MAT and the ITG node. The status can be:

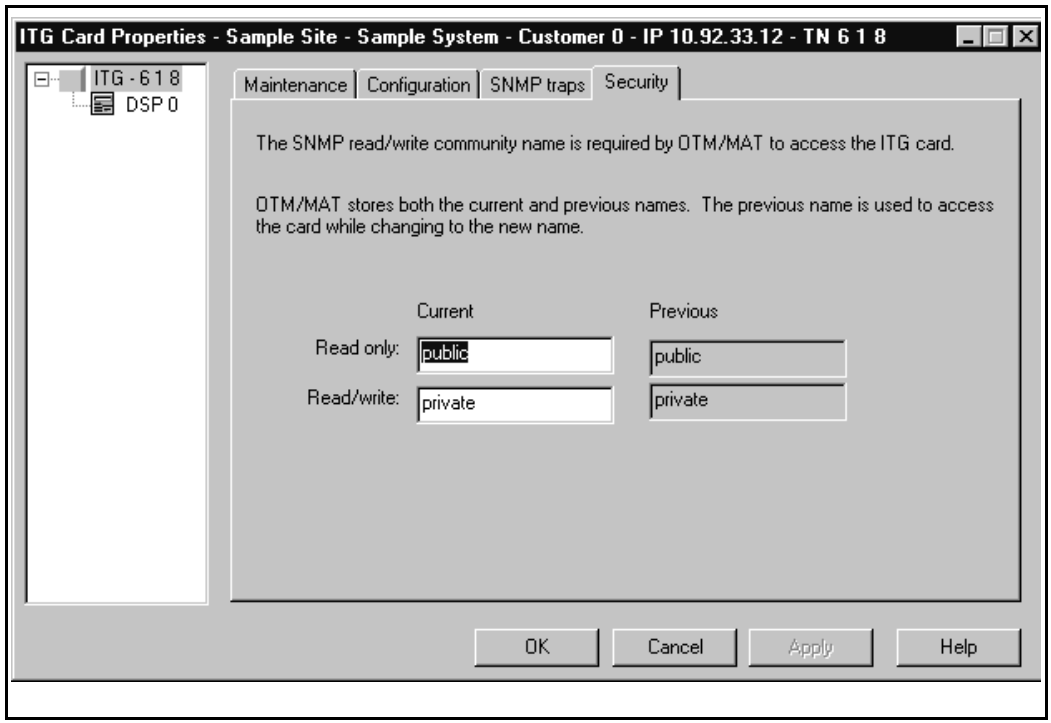
- "Not defined": the dialing plan has not been created for the node.
- "Changed" (dialing plan changes have not been transmitted to the card.
- "New" (dialing plan has never been transmitted to the card.
- "Transmitted": transmitted/retrieved to/from the node).

Card synch status The status of the card properties between MAT and the ITG card. The status can be:

- "Not defined": card has been added via the node properties, or by retrieving the node properties from a Leader, but the user has never opened the card properties and made a change.
- "New": once the user opens a card with the state of "Not defined" and makes a change, the status changes to "New".
- "Changed": card properties have been changed but not transmitted to the card.
- "Transmitted": card properties have been transmitted/retrieved to/from the card. When the card is deleted from the "ITG Node Properties" window, the card is removed from the "IP Telephony Gateway" window, and the "Node synch status" is set to "Changed."

Change the SNMP Community Names to maintain MAT ITG access security

Good security policy requires changing passwords periodically. The MAT ITG SNMP community names function as the passwords for MAT ITG access to cards in the ITG node. MAT ITG SNMP community names must be changed on a card by card basis.



1 Click the **Security** tab and enter the new "Read only" and "Read/write" card SNMP community name. MAT will use the previous community names to transmit the card properties and thereafter the current and previous fields will both show the new community names.

After you transmit the card properties for all cards, the current and previous fields will both reflect the new community names.If MAT ITG cannot refresh the status or transmit and retrieve configuration files to or from a particular ITG card, and if you can ping the card from the MAT ITG PC, then the community names may be mismatched between the

MAT ITG and the ITG cards. Call your Nortel Networks technical support representative for assistance.

If a failed card has been replaced with a spare card try the default community names. The default "Read only" community name is **public**. The default "Read/write" community name is **private**. (MAT ITG only uses the "Read/write" community name).

Remote Access

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, Bay 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 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.

Figure 29
Remote access with full access to the customer's LAN/WAN network

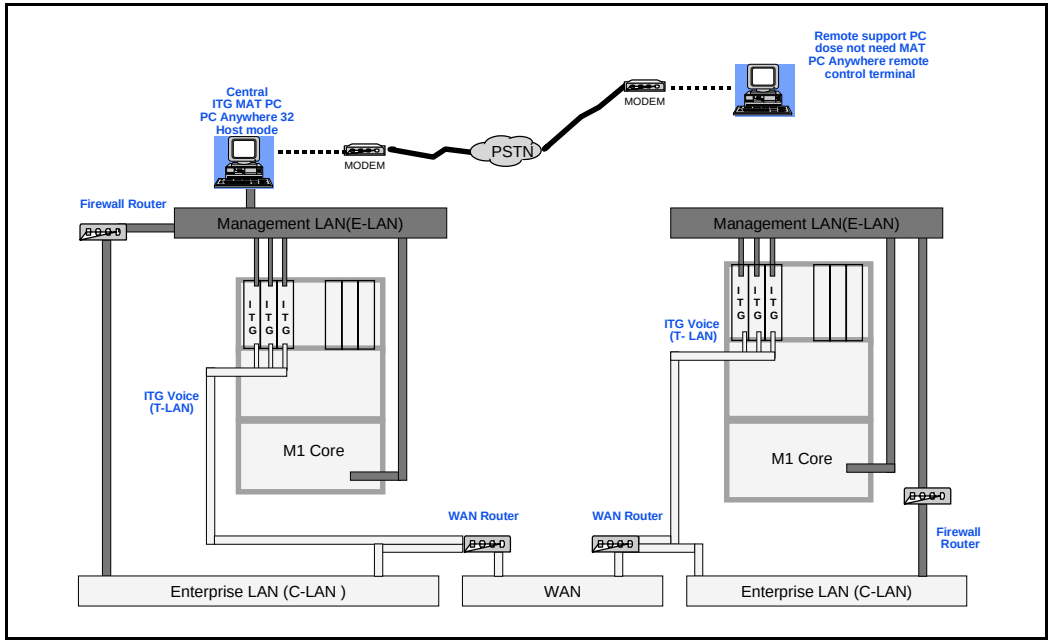
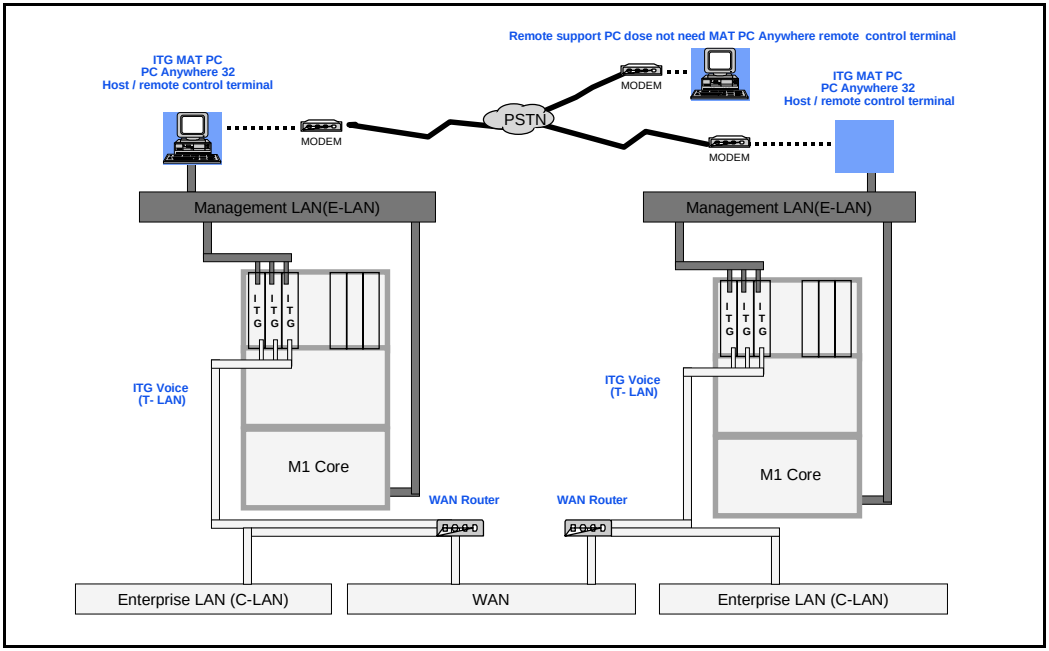


Figure 30
Remote access with no access to the customer's LAN/WAN network



ITG MAT OA&M tasks

The MAT ITG application provides most of the ITG administration commands.

The following commands are described:

ITG operational measurement (OM) report scheduling and generation

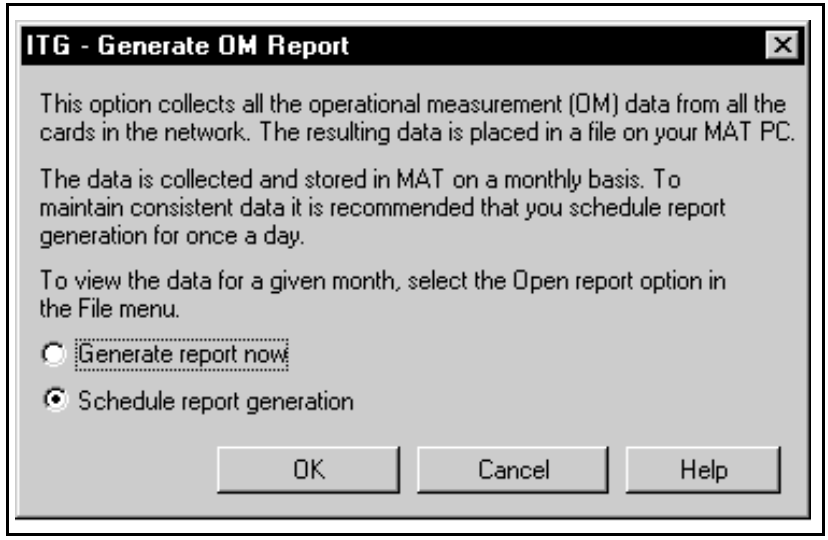
The purpose of Operational Measurement (OM) is to give some important statistics/traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file will apply only to the calls routed over the IP network via ITG. It will also give a quantitative view of how the system has performed.

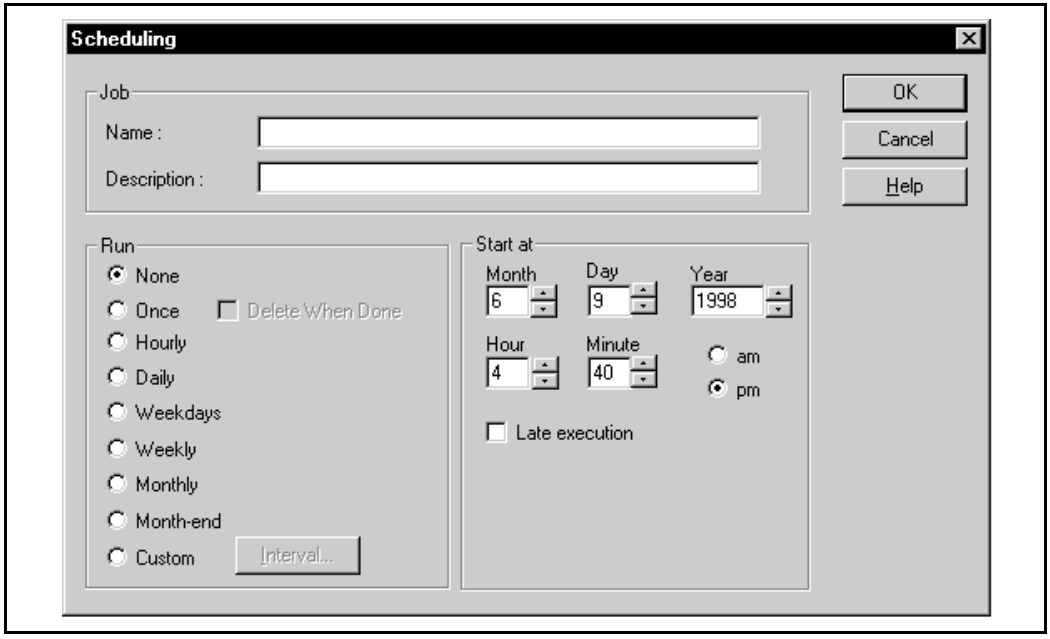
The OM reports are a collection of data from all the ITG cards in the network. On an hourly basis, the OM data is written to a file. At midnight, the OM file will be copied to a backup file and the new day will start with a clean file.

The user can generate a report on demand or schedule reports. Each time a report is generated, the application retrieves the latest OM data from each ITG card that is 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 data is collected. The files are named as "itg_mm_yyyy.csv," where "mm" = the month, and "yyyy" = the year. For example: **itg_12_1998.csv**.

It is recommended that the user schedule report generation once a day.
To schedule a report:

1. In the ITG Main window, click the **File** menu and select **Report,** then **Generate**.
2. In the "ITG - Generate Report" window, select the **Schedule report generation** radio button.
3. Click **OK**. The Scheduling window appears:
4. In the "Job" text box, enter the name and description of the schedule.
5. In the "Run" box, click the radio button that indicates the frequency of report generation.
6. In the "Start at" box, enter the month, day, year, hour, and minute of the start of the report period. Select the "am" or "pm" radio button.
7. Click **Apply** then **OK**.


ITG - Generate OM Report
This option collects all the operational measurement (OM) data from all the cards in the network. The resulting data is placed in a file on your MAT PC.
The data is collected and stored in MAT on a monthly basis. To maintain consistent data it is recommended that you schedule report generation for once a day.
To view the data for a given month, select the Open report option in the File menu.
Generate report now
Schedule report generation
OK
Cancel
Help


Scheduling
Job
Name :
Description :
OK
Cancel
Help
Run
None
Once
Delete When Done
Hourly
Daily
Weekdays
Weekly
Monthly
Month-end
Custom
Interval...
Start at
Month
Day
Year
6
9
1998
Hour
Minute
4
40
am
pm
Late execution

To generate a report

1. In the “IP Telephony Gateway” window, click the **File** menu and select **Report**, then **Generate**.In the “ITG - Generate Report” window, select the **Generate OM report now** radio button.
2. Click **OK**.

View the ITG error log through the MAT ITG application

To view ITG error conditions that are abnormal events, but not severe enough to raise an alarm:

1. In the “MAT Navigator” window, select the **ITG M1 IP Trk** icon from the “Services” folder.
2. In the “IP Telephony Gateway” window, click the right mouse button and select **Card | Properties** from the pop-up menu.
3. Click the **Open log file** button.

The file is transferred via FTP from the ITG card to the PC and opened in the WordPad application.

The ITG Error log file displays error information, including the date/time of the error, the originating module (ITG node), and the specific error data.

Back up and restore MAT ITG data

The MAT Backup Wizard is used to backup and restore any or all of MAT PC based data, including ITG MAT data. All of the ITG data is stored in an Access database file on the MAT PC or Server. This file is only backed up when the user selects the “Disaster Recovery” option. This option backs up all MAT data and can only be used to restore all data

For more information on using the MAT Backup Wizard, see the *Common Services User Guide* in the *MAT 6 User Guides.*

Update ITG node properties

In MAT, perform the following to update the ITG node properties:

1. In the MAT Navigator window, select the **ITG M1 IP Trk** icon from the "Services" folder. The system displays the "IP Telephony Gateway" screen.
2. Click the right mouse button on a card and select **Node | Properties** from the pop-up menu.
3. Perform all required updates to the ITG Node "General" tab parameters.
4. Configure the Node Location parameters: "MAT site, MAT system, and Customer."
5. Configure the "Network connections" parameters: "Node IP, Voice gateway IP, Management gateway IP, Voice subnet mask, and Management subnet mask." See your network administrator for assignment of these IP addresses.
6. If ITG cards are to be added or deleted from the node or changed (refer to the Maintenance section for the procedure to replace an ITG card), then use one of the following procedures:
   - "Add an ITG card to the node" on page 187
   - "Delete an ITG card from the node" on page 194
   - "Change an IP address" on page 195

Add an ITG card to the node

To add a new ITG card to the node, follow the steps that begin on page 126 in the Install and configure the ITG node chapter.

1. In the "MAT Navigator" window select the **ITG M1 IP Trk** icon from the "Services" folder.
2. In the "IP Telephony Gateway" window, select **Node | Properties** from the popup menu. The ITG Node Properties window is displayed.
3. Click the "Configuration" tab.

4 To add a card:

- Enter the “Management IP”, “Management MAC”, “Voice IP”, and “Card TN” fields. These fields are mandatory. The “Management MAC” address is labeled on the faceplate on the ITG card.
- Refer to and update the ITG card MAC and IP addresses on the ITG Installation Summary Sheet.
- Select “Leader 1”, or “Follower” from the “Card role” pull-down menu.

5 Click the **Add** button.

6 Click **Apply** then **OK**.

7 Add the ITG TIE trunks via the MAT System Passthru terminal, ESN MAT application, or via a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1. Use the overlay 14 **NEW** command.

Physical card installation

1 Identify the IPE card slots selected for the new ITG card.

Note: Refer to and update the ITG card TNs on the ITG Installation Summary Sheet.

2 Remove any existing I/O panel cabling associated with any card formerly installed in the selected card slot.

3 Pull the top and bottom locking devices away from the ITG faceplate.

4 Insert the ITG card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

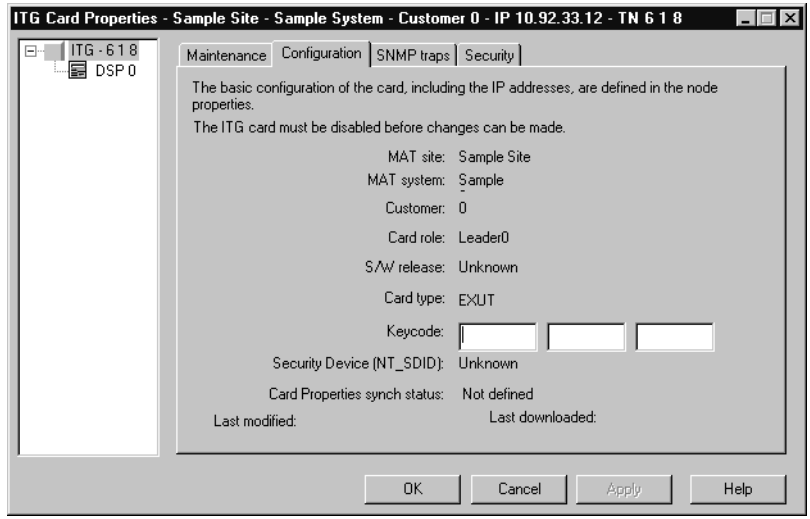
Note 1: When ITG cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in software, at which point in turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the ITG faceplate maintenance display to see start-up selftest results and status messages. A display of the type "F:xx" indicates a failure. Some failures indicate that the card must be replaced. "F:10" indicates Security Device test failure: check for presence of Security Device on the card. Refer to "ITG faceplate maintenance display codes for card reset" on page 220 for a listing of display codes.

Configure the properties of the ITG card

To configure the new ITG card, do the following:

1 In the "IP Telephony Gateway" window, double-click on the new ITG card to display the "ITG Card Properties" window. Leave the ITG card icon selected in the left side of the window.



2 Click the **Configuration** tab.

3 Verify that the new ITG card is running the same software version as the existing cards in the ITG node, and that the “S/W release” shows the latest recommended software version.

- If the software needs to be updated, refer to “Upgrade ITG card software (if required)” on page 158.
- If the cards are not present and responding, you must remember to come back and verify the software version.

4 Enter the keycode into the keycode field. Refer to the Software License document for the keycode. The keycode is 24 digits, consisting of 3 groups of 8 alphanumeric characters. Optionally, the keycode can be copied from a file and pasted into the first field. If the cards are present and responding, compare the keycode and “Security Device NT_SDID” displayed with the ITG Installation Summary Sheet.

5 Click the **SNMP traps** tab.

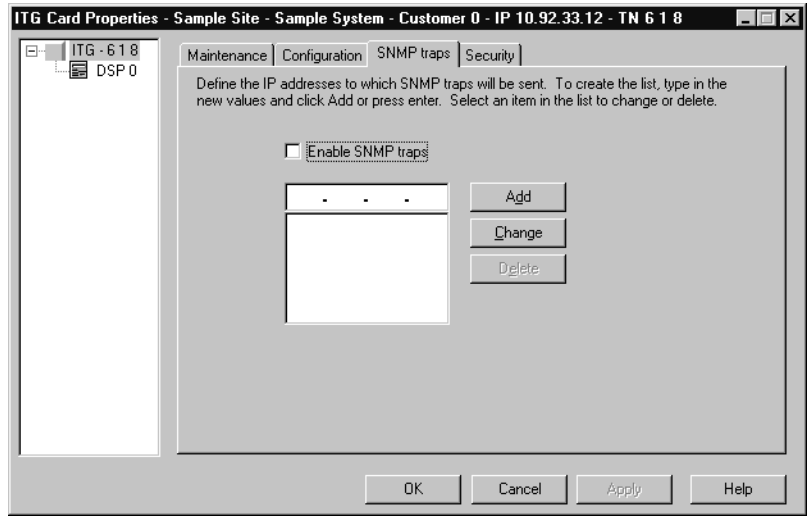
Note: The term “SNMP trap” refers to the sending of ITG error messages to the locations specified by the SNMP Manager IP addresses. Checking the “Enable SNMP traps” box will enable sending of SNMP traps to the SNMP managers that appear in the list.

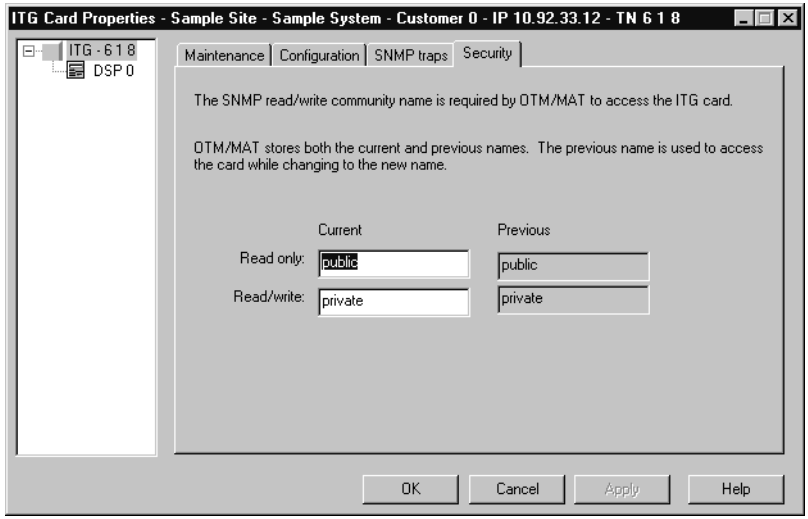
6 To add an SNMP Manager IP address, type the address in the entry field, and click **Add**. You should add SNMP Manager IP addresses for:

- the local MAT PC
- PPP IP address configured in the Netgear RM356 Modem Router, or equivalent, on the E-LAN for the remote support MAT PC
- the SNMP manager for remote alarm monitoring via SEB2 and IRIS nGEN (if present).
- Any remote MAT PCs on the customer’s IP network.

SNMP community name is equivalent to a password. The community names should be changed from the defaults in order to provide better security for the ITG node. This SNMP community name is used by MAT ITG to refresh the node status, and to control the transmitting and retrieving of files.

7 Click the **Security** tab and enter the “Card SNMP community name” .


ITG Card Properties - Sample Site - Sample System - Customer 0 - IP 10.92.33.12 - TN 6 1 8
ITG - 6 1 8
DSP 0
Maintenance
Configuration
SNMP traps
Security
Define the IP addresses to which SNMP traps will be sent. To create the list, type in the new values and click Add or press enter. Select an item in the list to change or delete.
Enable SNMP traps
Add
Change
Delete
OK
Cancel
Apply
Help


ITG Card Properties - Sample Site - Sample System - Customer 0 - IP 10.92.33.12 - TN 6 1 8
ITG - 6 1 8
DSP 0
Maintenance
Configuration
SNMP traps
Security
The SNMP read/write community name is required by OTM/MAT to access the ITG card.
OTM/MAT stores both the current and previous names. The previous name is used to access the card while changing to the new name.
Current
Previous
Read only:
public
public
Read/write:
private
private
OK
Cancel
Apply
Help

Configure ITG card DSP properties

Note: The properties of all DSPs on an ITG card are modified by configuring the properties for "DSP 0" on an ITG card. The "Restore defaults" button can be used to restore all default values including restoring the coding algorithm to G.729A.

CAUTION

The default DSP parameters for each codec are suitable for most applications. If you are not an expert in voice over IP, do not modify them. Refer to the *Administration* section for more details.

1. Click to select the **DSP 0** icon underneath the ITG card.
2. Click the **Configuration** tab.
3. Select the "Coding algorithm" (codec) according to your ITG network engineering plan. Refer to the *Engineering Guidelines* section.

   The "DSP coding algorithm", or codec, pull-down menu has the following options: "G.711 A-law", "G.711 Mu-law", "G.729", "G.729A" (default),"G.723.1 5.3K," and "G.723.1 6.3K."
4. Click **Apply** then **OK**.

Transmit the card properties

1. In the "IP Telephony Gateway" window, select the newly added card from the node.
2. Click **Configuration** | **Synchronize** | **Transmit.**

   The "ITG - Transmit Options" window appears

   Leave the radio button defaulted to "Transmit to selected nodes". Check the "Card properties" box only.
3. Click the **Start Transmit** button.

   The transmission status is displayed in the "Transmit control" box. Confirm that card properties and dialing plan are transmitted to all cards successfully.
4. When the transmission is complete, click the **Close** button.
5. Use the overlay 32 ENLC command to re-enable the ITG cards.

6 In the “IP Telephony Gateway” main window, select **View | Refresh**. The card status should now show “Enabled.”

7 Verify the TN, management interface MAC address, IP addresses, the NT-SDID, and keycode for each ITG card. The NT_SDID and keycode are verified by double-clicking each ITG card in the MAT "IP Telephony Gateway" main window and clicking the “Configuration” tab of the Card Properties. Compare the displayed values with those on the ITG Installation Summary Sheet.

Configure the new trunks for the ITG card in the Meridian 1

LD 14 – Configure the ITG card.

Prompt	Response	Description
REQ	NEW 8 NEW 4	Add new data. Configure 8 units on the EXUT ITG card. Add new data. Configure 4 units on the ITG card (G.729). *See Note 2.*
TYPE	TIE	TIE trunk.
TN	l s c u	TN of the trunk.
DES	 hhhh:hh:hh:hh:hh xxx.xxx.xxx.xxx	16 character descriptive designator for the ITG card. See Note 1. For unit 0. the ITG card management MAC address. For units 1-7 the ITG card management IP address.
XTRK	EXUT	Trunk type emulated by the ITG card.
...	...	...
CUST	0-99	Customer number.
NCOS	0-99	For *Fallback to circuit-switched voice facilities*, FRL of NCOS must be greater than FRL in alternate routing entries of ESN Route List Block.
RTMB	rrr mmm	Route and member number. *See Note 3.*
SIGL	LDR	Loop dial repeating trunk signaling.
STRI	WNK	Start arrangement incoming.
STRO	WNK	Start arrangement outgoing.

SUPN	YES	Answer and disconnect supervision.
CLS	DTN	Digitone class of service.

Note 1: Use the "NEW 8" 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 MAC address, see the ITG information entry sheet. MAC addresses are labeled on the ITG card faceplate.

Note 2: When using the G.729 only four DSP channels are supported, and only trunk units 0, 1, 4, and 5 must be configured.

Note 3: Assign route member numbers to cards in the same order as the default order in the MAT ITG window (i.e, Leader 0 is members 1-8; Leader 1 is members 9-16; first follower is members 17-24).

Note 4: Only Wink Start arrangement is supported.

Note 5: Digitone class of service is recommended for faster call setup. Dial pulse (DIP) class of service is also supported.

The procedure is complete.

Delete an ITG card from the node

1. In the "MAT Navigator" window select the **ITG M1 IP Trk icon** from the "Services" folder.
2. If the ITG card to be deleted is a Leader 0 or Leader 1, then:
   - Telnet to the card.
   - Enter the **clearLeader** command from the ITG shell.
3. In the "IP Telephony Gateway" window, select **Node | Properties** from the popup menu. The ITG Node Properties window is displayed.
4. Click the "Configuration" tab.
5. Select the ITG card to be deleted from the list.
6. Click the **Delete** button.

7 Click **Apply** then **OK**.

8 Remove the ITG TIE trunks via the MAT System Passthru terminal, ESN MAT application, or via a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1. Use the overlay 14 **OUT** command.

Change an IP address

1 To change the IP address of ITG card(s): Click **Configuration|Node|Properties**. Update the ITG card IP addresses as required.

2 When all updates to the IP addresses have been made, click **Apply** then **OK** in the "ITG Node Properties" window. Or click **Cancel**, if you do not wish to save the changes. Transmit the node properties to the Leader 0 card:

3 Select the ITG Leader 0 card in the IP Telephony Gateway window.

4 Click the **Configuration** menu, then **Synchronize**, then **Transmit**.

5 Click the "Transmit to selected nodes" radio button.

6 Click the "Node Properties" check box.

7 Click the **Start Download** button.

The results of the download appear in the "Transmit control" box.

8 Click **Close**.

9 If you have changed IP addresses of any cards, restart the cards for the changes to take effect.

Update the ITG dialing plan

To add, delete, or change the properties of a dialing plan entry:

1 Make the appropriate changes to the Meridian 1 dialing plan in overlays 86, 87, and 90. Refer to "Configure the Meridian 1 ESN dialing plan for the ITG network" on page 165.

2 In the MAT ITG application, go to the "ITG Dialing Plan Properties" screen.

3 Click the **General** tab.

4 Add, delete, or change the properties of the dialing plan, as required.

5 Click **Apply** then **OK**.

6 In the “Dialing Plan Entry Properties” screen, make sure each ITG Leader card is associated with a “set of dialed digits.”

7 Click **Apply** then **OK**. Transmit the updated dialing plan to the Leader 0 card:

8 Select the ITG Leader 0 card in the IP Telephony Gateway window.

9 Click the **Configuration** menu, then **Synchronize**, then **Transmit**.

10 Click the “Transmit to selected cards” radio button.

11 Click the “Dialing Plan” check box.

12 Click the **Start Download** button. The results of the download appear in the “Transmit control” box.

13 Click **Close**.

Update ITG card properties

Some basic ITG card configuration, including IP address configuration, must be performed from the ITG Node Properties window, as described in “Update ITG node properties” on page 187.

1 In the “MAT Navigator” window, select the **ITG M1 IP Trk icon** from the “Services” folder.

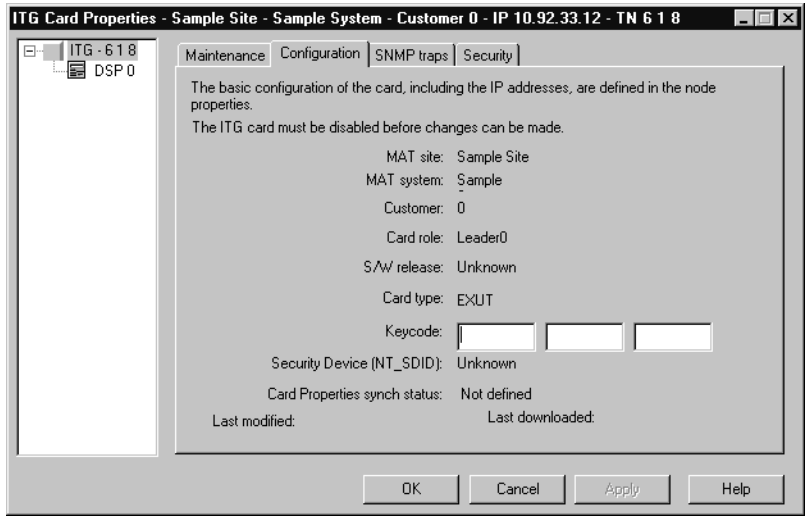
2 In the “IP Telephony Gateway” window, select the ITG card to be modified.

3 Select the ITG card to be updated and click the right mouse button to select **Cards | Properties** from the pop-up menu. The “ITG Card Properties” window appears. The “Configuration, SNMP traps, and Security” tabs are described following step 3.

4 Make the required changes to the ITG card configuration. Click **Apply** then **OK**.

The following pages describe the various card properties tabs.

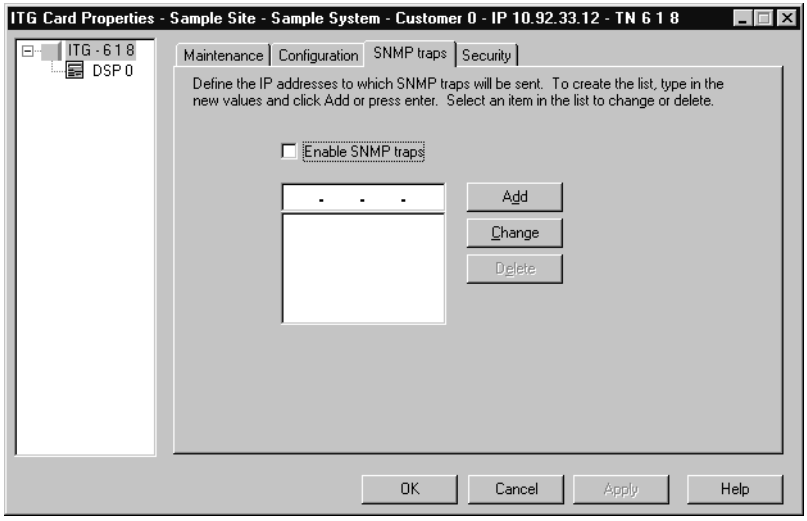
Configuration tab



The Configuration tab shows ITG card information and allows the ITG card Keycode to be updated. The ITG card must be disabled before changes can be made.

To update the keycode, enter the new keycode as three sets of eight characters each in the “Keycode” fields.

SNMP traps tab



The SNMP traps tab is used to define the IP addresses to which SNMP traps will be sent.

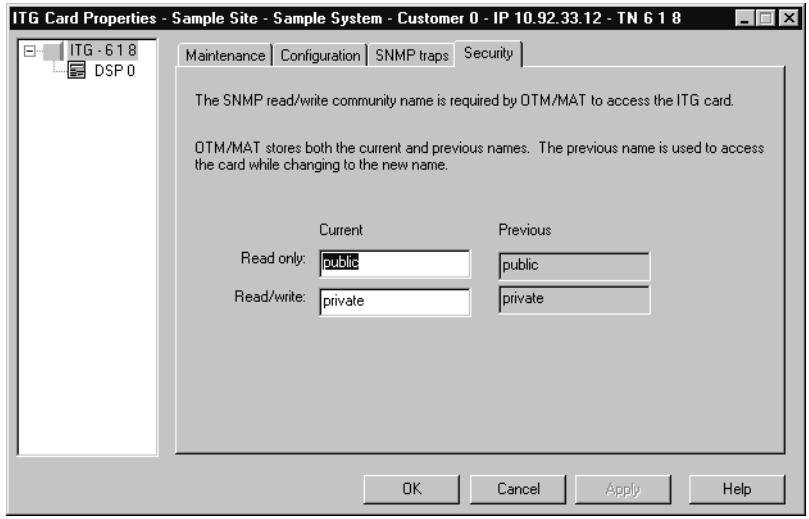
To enable the sending of SNMP traps to receive alarms (error messages) to the hosts specified by the IP addresses in the list, check the “Enable SNMP traps” box.

To add an IP address to receive SNMP traps, type the address in the entry field, and click “Add.”

To delete an IP address, select the address from the list, and click “Delete.”

To change an IP address, select the address from the list. Type the new address in the entry field, then click “Change.”

Security tab



This tab allows the user to change the SNMP community names of the ITG card. This name is used with all SNMP communication between MAT and the card.

Update ITG card DSP properties

Note: The properties of all DSPs on an ITG card are modified by configuring the properties for "DSP 0" on an ITG card. The "Restore defaults" button can be used to restore all default values including restoring the coding algorithm to G.729A.

CAUTION

The default DSP parameters for each codec are suitable for most applications. If you are not an expert in voice over IP, do not modify them.

1. In the "MAT Navigator" window select the **ITG M1 IP Trk icon** from the "Services" folder.
2. In the "IP Telephony Gateway" window select the ITG card that will have its DSP properties modified.
3. Click the right mouse button on the card and select **Card | Properties** from the popup menu. The "ITG Card Properties" window appears.
4. Click the **DSP 0** icon underneath the ITG card.
5. Click the **Configuration** tab.

Configuration tab parameters description

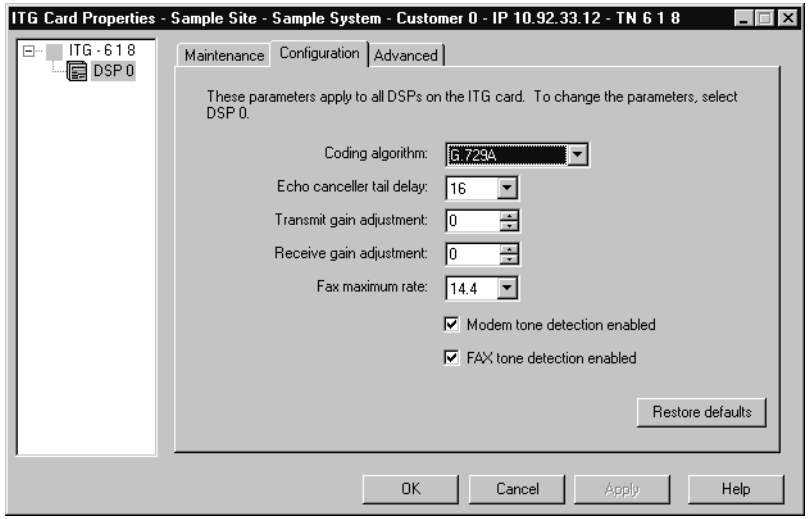
Note: In the following parameter descriptions, values in parenthesis are default values.

The "DSP coding algorithm", or codec, pull-down menu has the following options: "G.711 A-law", "G.711 Mu-law", "G.729", "G.729A," "G.723.1 5.3K," and "G.723.1 6.3K."

The "Echo canceller tail delay" parameter range is: 8-16-(32) ms for the G.729 DSP coding algorithm, and 8-(16) for all other codecs.

The "Transmit gain adjustment" parameter range is -14 to +14 dB. The default is 0 dB.

The "Receive gain adjustment" parameter range is -14 to +4 dB. The default is 0 dB.



The “Fax maximum rate” parameter options are: “2400,” “4800,” 7200,” “9600,” “12000,” and (“14400,”), displayed in Kbps (2.4, 4.8, etc...).

The defaults are checked boxes for “V.25 FAX/Modem tone detection enabled” and “V.21 FAX tone detection enabled.”

6 Configure the parameters in the “Configuration” tab as required.

7 Click the **Advanced** tab.

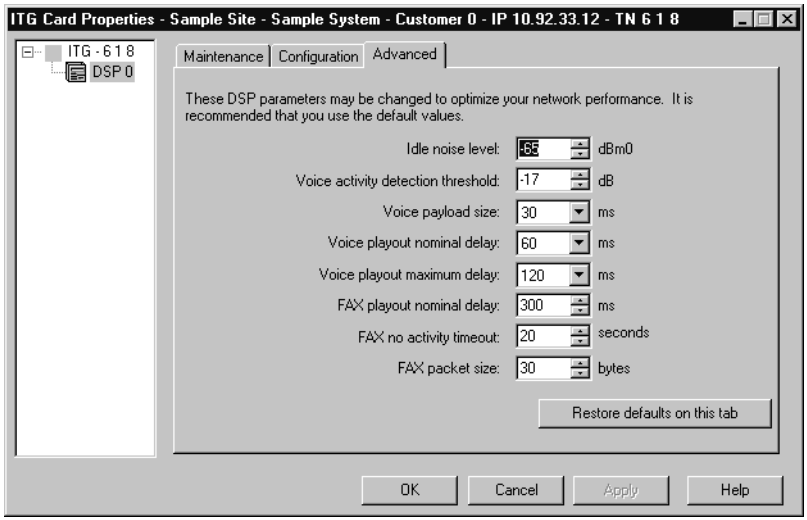
Advanced tab parameters description

The Advanced tab contains parameters that should only be modified by experienced users:

> ***Note:*** In the following parameter descriptions, values in parenthesis are default values.

The “Idle noise level” parameter range is -327 to +327 dBm0.
The default is -65.

The “Voice Activity Detection (VAD) threshold” parameter range is -20 to +10dB. The default is -17 dB.



The “Voice payload size” parameter range is 10-80ms in increments of 10. Allowed values depend on the selected “DSP coding algorithm”:

- G.711 A-law, G.711 Mu-law range is: (10)-30 ms.
- G.723.1 5.3K, and G.723.1 6.3K: only allowed value is 30 ms.
- G.729, and G.729A range is: 10-(30)-80 ms.

The “Voice playout nominal delay (ND)” parameter values are as follows, where PT is the Voice payload size:

- PT * 2 to PT * 10, subject to a maximum of 320 ms, in steps of PT. Default is 40 when PT=10, 60 when PT=20, or else the default is PT*2. The upper bound for G.711 is 160 ms.

The “Voice playout maximum delay (MD)” values are:

- (Voice playout nominal delay + (PT * 2)) to a maximum of 500 ms, in steps of PT. The default is 100 when PT=10, 120 when PT=20, or else the default is Voice playout nominal delay*2. The upper bound for G.711 is 160 ms.

The “Fax playout nominal delay” parameter range is 0-(100)-300 ms.

The ‘Fax no-activity timeout” parameter range is 10-(20)-32000 seconds.

The “Fax packet size” parameter range is 20-(30)-48 bytes.

8 Configure the parameters in the “Advanced” tab as required. Click **Apply** then **OK**.

Transmit the card properties to the updated ITG card

1 Select the updated ITG card in the IP Telephony Gateway window.

2 Click the **Configuration** menu, then **Synchronize**, then **Transmit**.

3 Click the “Transmit to selected cards” radio button and click the “Card Properties” check box.

4 Click the **Start Download** button. The results of the download appear in the “Transmit control” box.

5 Click Close.

Delete an ITG node

1 In the “MAT Navigator” window select a specific **ITG M1 IP Trk icon** from the “Services” folder.

2 In the “IP Telephony Gateway” window select the Leader 0 ITG card from the node that is to be deleted.

3 Click the right mouse button on the card and select **Node | Delete** from the popup menu. Upon clicking **Yes** to confirm the deletion of the ITG node, the ITG node and all associated ITG cards will be deleted.

Display ITG node properties

1 In the “MAT Navigator” window select the **ITG M1 IP Trk icon** from the “Services” folder.

2 In the “IP Telephony Gateway” window, select **Node | Properties** from the popup menu. The ITG Node Properties window will be displayed.

Display ITG card properties

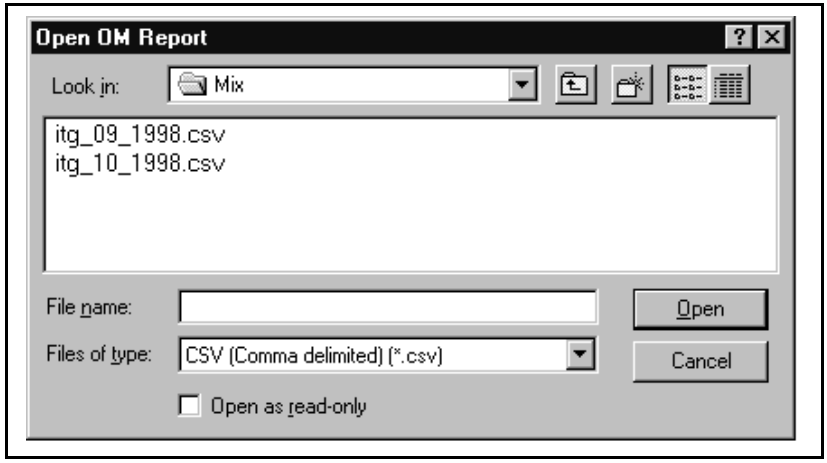
1. In the “MAT Navigator” window select the **ITG M1 IP Trk icon** from the “Services” folder.
2. In the “IP Telephony Gateway” window, select the ITG card for which information is to be displayed.
3. Click the right mouse button on the card, and select **Card | Properties** from the popup menu. The ITG Card Properties window will be displayed.

   The card properties displays the card software, the time and date, the NT_SDID, and keycode, the SNMP manager addresses, and the SNMP community names.

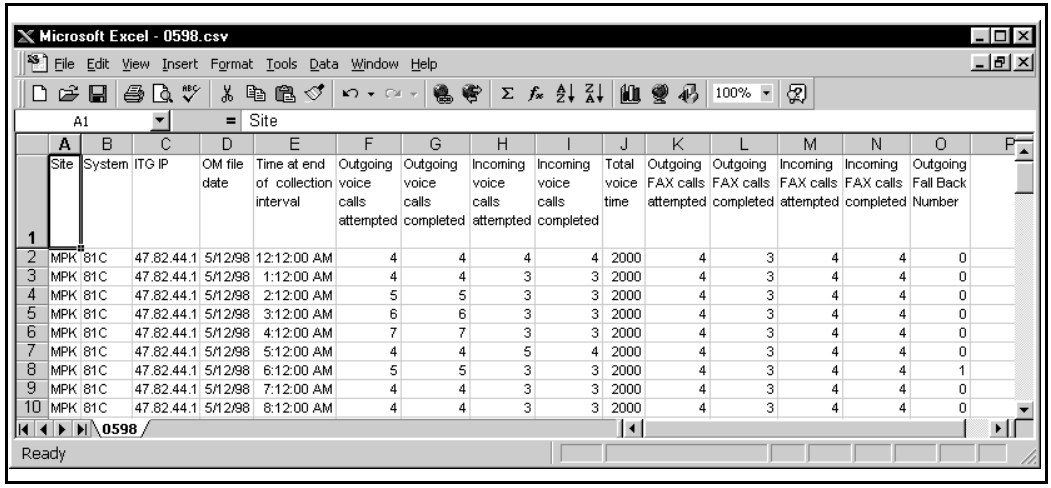
   If you select **DSP 0**, the DSP parameters of the ITG card are displayed.

Open an Operational Measurement (OM) report

1. In the “IP Telephony Gateway” window, click **File | Report | Open**.
2. Select an “ITG_mm_yyyy.csv” file to be opened and click **Open**.



The selected report is opened:



Microsoft Excel - 0598.csv

File Edit View Insert Format Tools Data Window Help

A1 = Site

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Site	System	ITG IP	OM file date	Time at end of collection interval	Outgoing voice calls attempted	Outgoing voice calls completed	Incoming voice calls attempted	Incoming voice calls completed	Total voice time	Outgoing FAX calls attempted	Outgoing FAX calls completed	Incoming FAX calls attempted	Incoming FAX calls completed	Outgoing Fall Back Number	
2	MPK	81C	47.82.44.1	5/12/98	12:12:00 AM	4	4	4	4	2000	4	3	4	4	0	
3	MPK	81C	47.82.44.1	5/12/98	1:12:00 AM	4	4	3	3	2000	4	3	4	4	0	
4	MPK	81C	47.82.44.1	5/12/98	2:12:00 AM	5	5	3	3	2000	4	3	4	4	0	
5	MPK	81C	47.82.44.1	5/12/98	3:12:00 AM	6	6	3	3	2000	4	3	4	4	0	
6	MPK	81C	47.82.44.1	5/12/98	4:12:00 AM	7	7	3	3	2000	4	3	4	4	0	
7	MPK	81C	47.82.44.1	5/12/98	5:12:00 AM	4	4	5	4	2000	4	3	4	4	0	
8	MPK	81C	47.82.44.1	5/12/98	6:12:00 AM	5	5	3	3	2000	4	3	4	4	1	
9	MPK	81C	47.82.44.1	5/12/98	7:12:00 AM	4	4	3	3	2000	4	3	4	4	0	
10	MPK	81C	47.82.44.1	5/12/98	8:12:00 AM	4	4	3	3	2000	4	3	4	4	0	

0598

Ready

Use the Retrieve command

The Retrieve command sends information from the ITG cards to the MAT ITG node. The Retrieve command can be used for:

- a remote MAT user to download a node or card configuration

  Note: This can also be performed by doing the “Add ITG Node” command and selecting the “Retrieve the active configuration from an existing node” option.

- for copying node information from one node to another
- for restoring accidentally changed MAT information, and
- for downloading information to a fictitious “dummy” node that has been created for this purpose, in order to view the configuration of the ITG cards and node.

To use the Retrieve command:

1 In the “IP Telephony Gateway” window, select the card(s) from which to retrieve information.

2 Click **Configuration | Synchronize | Retrieve**.

3 Configure whether to retrieve “Node properties” or “Card properties.” Click one or more of the check boxes.

4 Click **Start Retrieve**. The results of the Retrieve command are displayed in the “Retrieve control” box.

ITG shell command-line interface access via Telnet or maintenance port

Connect the MAT PC com port to the RS-232 serial maintenance port of the ITG Leader card via an NTAG81CA Faceplate Maintenance cable.
If required, use an NTAG81BA Maintenance Extender cable to provide an extension between the NTAG81CA Faceplate Maintenance cable and the MAT PC. Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTMF94AA I/O Panel Ethernet and Serial Adaptor cable to create a more permanent connection to the ITG card maintenance port.

Alternatively, the ITG shell can be accessed from the MAT PC. Refer to “Telnet to an ITG card” on page 207.

The following administration commands may be performed from the ITG shell:

- “Telnet to an ITG card” on page 207.
- Changing the default ITG Telnet password to maintain access security
- “Download the ITG operational measurements through the ITG shell” on page 208
- “Reset the operational measurements” on page 208.
- “Display the number of DSPs” on page 208.
- “Disabling or enabling silence suppression (also known as Voice Activity Detection (VAD))” on page 208.
- “Displaying ITG Node Properties” on page 209.
- “Transferring files via the command-line interface” on page 210.
- “IP configuration commands” on page 212.
- “Download the ITG error log” on page 212.

Telnet to an ITG card

To access the command line on an ITG card from the MAT PC:

1. In the "MAT Navigator" window select the **ITG M1 IP Trk icon** from the "Services" folder.
2. In the "IP Telephony Gateway" window click the right mouse button on the ITG card that you wish to access and select **Card | Telnet to ITG card** from the popup menu.
3. The default user name and password are **itgadmin**.

The MAT PC opens a Telnet window and automatically connects to the ITG card by using the management IP address. After entering a username and password, the ITG shell command-line interface is accessed from the MAT PC.

Telnet and FTP Security

Good security policy requires changing user names and passwords periodically. The ITG user name and password protects 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 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.

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:

At the ITG shell prompt, type: **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 will reset all operational measurement (OM) parameters that have been collected since 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**

Enter this command to set the Voice Activity Detection to enabled or disabled: **itgSetVAD**

Enter this command to show the VAD configuration and the current DSP setting: **itgVADShow**

Disabling or enabling silence suppression (also known as Voice Activity Detection (VAD))

Silence suppression must be disabled or enabled according to your ITG network engineering plan. Refer to “Silence suppression or Voice Activity Detection” on page 57 in the Engineering Guidelines section.

Silence suppression or VAD must be enabled or disabled on a card by card basis similar to other card properties.

After changing the configuration of silence suppression from enabled to disabled, or vice versa, the card properties must be retransmitted from MAT in order to apply the silence suppression changes to the ITG cards.

Disabling silence suppression *approximately doubles* LAN/WAN bandwidth usage. Do not change this unless instructed by the IP network engineer.

1. In the MAT ITG window, select the first card for which silence suppression configuration needs to be changed.
2. Right-click the ITG card and select **Telnet to card**.
3. When the "VxWorks login:" prompt appears, enter the default user ID, **itgadmin**.
4. When the "password" prompt appears, enter the default password, **itgadmin**.
5. If the login is unsuccessful, then check that you have the correct user ID and password.
6. At the ">" prompt enter **itgVADShow**. The output appears as this:

   Voice Activity Detection configured: ENABLED (DISABLED)
   Voice Activity Detection currently on DSP: ENABLED (DISABLED)
7. If the silence suppression (or VAD) must be DISABLED then enter the command **itgSetVAD 0** (0 equals OFF).

   The output of this command will be the same as the 'itgVADShow' command, except that the value at the end of the first line will reflect the configuration setting changed, and the second line will show that the setting of the DSP has not changed.
8. If the silence suppression (or VAD) must be ENABLED according to the IP network engineer, then enter the command **itgSetVAD 1** (1 equals ON).

   The output of this command will be the same as the 'itgVADShow' command, except that the value at the end of the first line will reflect the configuration setting changed, and the second line will show that the setting of the DSP has not changed.

Displaying ITG Node Properties

At the ITG shell, enter the following command to display information about an ITG node: **IPInfoShow**

The following ITG node information will be displayed 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

Transferring files via the command-line interface

To transfer a file from the ITG card to the MAT PC or from the MAT PC to the ITG card, perform the one of the following commands at the ITG shell command-line, depending on what type of file transfer is to occur. These commands are from the perspective of the ITG card: that is, commands containing “Get” as part of the command refer to file transfer from the MAT PC to the ITG card, while commands containing “Put” as part of the command refer to file transfer from the ITG card to the MAT PC:

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 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.

Note 1: These commands are *case-sensitive*. The parameters following the command must each be enclosed in quotes, and that there must be a comma and no spaces between the parameters.

Note 2: Refer to the *Maintenance* section for a complete description of the various ITG shell file transfer commands.

Note 3: *Hostname* refers to the either IP address of the FTP host, or the ITG card itself or another ITG card when a PC card in the A: drive or C: drive (the swDownload command must only use the A: drive), of the ITG card contains the software binary file.

- swDownload <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>

This command updates the software on the ITG card with the binary file received from an FTP server or ITG card (from the drive A: PC card) 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 verify 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.

- DPAddrTGet <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- configFileGet <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- bootPFileGet <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- SNMPConfFileGet <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- hostFileGet <*hostname*> <*username*> <*password*> <*directory path*> <*filename*> <*ITGFileName*> <*listener*>
- 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*>
- DPAddrTPut <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- configFilePut <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- bootPFilePut <*hostname*> <*username*> <*password*> <*directory path*> <*filename*>
- hostFilePut <*hostname*> <*username*> <*password*> <*directory path*> <*filename*> <*ITGFileName*>

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 info in NVRAM and set the boot method to use bootp, thus, making the card a follower:

- clearLeader

Enter this command to print the values of the IP parameters that reside in NVRAM.

- NVRIPShow

Download the ITG error log

The ITG error log contains error conditions as well as normal events. Some of the error conditions may be severe enough to raise an alarm through SNMP traps.

The following commands are used to download an ITG error log:

- currLogFilePut
- prevLogFilePut

Meridian 1 system commands - LD 32

The following Meridian 1 system administration commands can be performed:

- "Disable the specified ITG card" on page 215.

The ITG card must be disabled before card properties can be transmitted from the MAT ITG application to the card.

The card reset button is only available in the MAT ITG application when the card is disabled.

Disabling the ITG card in overlay 32 does not disable the active leader or backup leader functions.

"Disable the specified ITG card when idle" on page 215.

This will temporarily prevent the ITG node from seizing the port from incoming calls.

- "Disable a specified ITG port" on page 215.
- "Enable a specified ITG card" on page 216.
- "Enable a specified ITG port" on page 216.
- "Display ITG card ID information" on page 216.

Note 1: This command will display the PEC (Product Engineering Code) for the card. The ITG PEC is NTCW80CA.

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 216.
- "Displaying ITG card port status" on page 217.

A summary list of ITG Meridian 1 system commands is shown in Table 24 on page 214.

Table 24 summarizes the Meridian 1 system administration commands available in overlay 32.

Table 24
Overlay 32 - ITG maintenance commands

Command	Function
DISC l s c	Disable the specified card, where: l = loop, s = shelf, c = card
DISI l s c	Disable the specified 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 specified unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the specified card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, where: l = loop, s = shelf, c = card

Table 24
Overlay 32 - ITG maintenance commands

Command	Function
STAT l s c	Print the Meridian 1 software status of the specified card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 software status of the specified unit, where: l = loop, s = shelf, c = card, u = unit

Disable the specified ITG card

To disable the specified ITG card in LD 32, use the following command:

DISC l s c	Disable the specified ITG card, where: l = loop, s = shelf, c = card

Disable the specified ITG card when idle

To disable the specified ITG card when idle in LD 32, use the following command:

DISI l s c	Disable the specified ITG card when idle, where: l = loop, s = shelf, c = card

Disable a specified ITG port

To disable a specified ITG port in LD 32, use the following command:

DISU l s c u	Disable the specified ITG unit (port), where: l = loop, s = shelf, c = card, u = unit

Enable a specified ITG card

To enable a specified ITG card in LD 32, use the following command:

ENLC l s c	Enable the specified ITG card, where: l = loop, s = shelf, c = card

Enable a specified ITG port

To enable a specified ITG port in LD 32, use the following command:

ENLU l s c u	Enable the specified 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 specified ITG card in LD 32, use the following command:

STAT l s c	Display the status of the specified ITG card, where: l = loop, s = shelf, c = card

Displaying 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 specified ITG port, where: l = loop, s = shelf, c = card, u = unit.

Identify ITG routes and cards in the Meridian 1 system

The overlay 16 RDB "DES" prompt should be used to identify the IP Telephony Gateway route.

ITG card management interface MAC address and IP address

The overlay 14 "DES" prompt is used to identify the management interface MAC address and IP address.

Print the ITG route and trunk designators in Meridian 1

The overlay 21 "LTM" (List Trunk Members) response to the REQ prompt can be used to list the ITG route designator and the individual ITG trunk designators to show the MAC addresses and IP addresses. Whenever cards are added, deleted, or changed you must update the trunk designators.

Maintenance

Introduction

This section provides information on maintenance functions of the ITG card:

ITG faceplate maintenance display codes for card reset

The ITG card faceplate four character display provides feedback to the craftsperson on the diagnostic status of the card during power-up and on its operational state when in service. Table 25 gives a list of display messages.

Table 25
ITG faceplate maintenance display code messages (Part 1 of 3)

Hex display code	Message
T:00	Initialization.
T:01	Testing Internal RAM.
T:02	Testing ALU.
T:03	Testing address modes.
T:04	Testing Boot ROM.
T:05	Testing timers.
T:06	Testing watchdog.
T:07	Testing external RAM.
T:08	Testing Host DPRAM.
T:09	Testing DS30 DPRAM.
T:10	Testing Security Device.
T:11	Testing flash memory.
T:12	Programming PCI FPGA.
T:13	Programming DS30 FPGA.
T:14	Programming CEMUX FPGA.
T:15	Programming DSP FPGA.

Table 25
ITG faceplate maintenance display code messages (Part 2 of 3)

Hex display code	Message
T:16	Testing CEMUX interface.
T:17	Testing EEPROM.
T:18	Booting processor, waiting for response with selftest information.
T:19	Waiting for application start-up message from processor.
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.
T:21	CardLAN operational, A07 enabled, display now under host control. ITG > shell is available for manual card configuration.
T:22	The ITG card is attempting to start the ITG application.
LDR	Card is running active leader tasks.
BLDR	Card has detected existing active leader, and is running backup leader tasks, or the card is configured as a leader and is missing its node properties. Transmit node properties from MAT.

Table 25
ITG faceplate maintenance display code messages (Part 3 of 3)

Hex display code	Message
FLR	Card has detected the active leader, and is running Follower tasks.

If the internal RAM test, ALU test, address mode test, Boot ROM test, timer test, or external RAM test fails, the card will enter a maintenance loop, as no further processing will be possible. A failure message will be printed on the display to indicate which test failed. For example, if the timer test fails, “F:05” will be displayed.

If any of the other tests fail (up to and including the EEPROM test), a message will be displayed to indicate this for three seconds. If more than one test fails, the message displayed will indicate the first failure. If verbose mode has been selected (by the test input pin on the backplane), the three second failure message will not be displayed.

If the maintenance display shows a persistent T:20 indicating an ITG software failure and if this occurs after the card was reset during a software download procedure, then call your Nortel Network technical support for assistance in attempting to download new software onto the card.

ITG system error messages (alarms)

When an error or specific event occurs, SNMP sends an alarm trap to MAT or any SNMP manager that is configured in the SNMP Manager’s list in the ITG card properties; it also puts the system error message into the error log file containing error messages, which is available through the MAT ITG card properties by clicking on the ’Open Log File’ button on the "Maintenance" tab of the ITG card properties. You can also view the log file in any text browser after uploading it to an FTP host using the **currLogFilePut** or **prevLogFilePut**. Events of the type **ITG4XX** will be written to the ITG face plate maintenance display, in the form "**I:4xx**", where "xxx" are the last three digits of the message. Table 26 lists the ITG messages by severity.

Table 26
ITG system error messages (alarms) (Part 1 of 3)

Alarm Clearance - No intervention required	
ITG0100	Successful bootup. All alarms cleared.
ITG0101	Exit from QoS fallback. Normal operation restored.
ITG0102	Ethernet voice port restored to normal operation.
ITG0103	Ethernet management port restored to normal operation.
ITG0104	DSP successfully reset.
ITG0105	Exit from card fallback. Leader card restored.
Minor Alarms - No intervention required	
ITG0200	Voice Ethernet buffer exceeded. Packet(s) discarded.
ITG0201	Management Ethernet buffer exceeded. Packet(s) discarded.
ITG0202	Card recovered from software reboot.
ITG0203	Fallback to PSTN activated.
ITG0204	DSP device reset.
ITG0205	Not used.
ITG0206	Invalid A07 message received. Message discarded.
ITG0207	Unknown H.323 message received. Message discarded/rejected.
ITG0208	Backup leader has been activated (i.e., has promoted itself to active leader) because the active leader is no longer responding to ping on the T-LAN.
ITG0250	Invalid X12 message received. Message discarded.
Major Alarms - Intervention required but not immediately	
ITG0300	Memory allocation failure.
ITG0301	Channel not responding. Channel is disabled.

Table 26
ITG system error messages (alarms) (Part 2 of 3)

ITG0302	DSP device failure. Operating on reduced capacity.
ITG0303	DSP subsystem failure. Initiating card reboot.
ITG0304	Cannot write to file. I/O write error.
ITG0305	Can't open configuration file. Using default settings.
ITG0306	Meridian Messaging error threshold exceeded.
ITG0307	Not used.
ITG0308	Address Translation failure. Call is released.
ITG0309	Unexpected DSP channel closed. Channel is unusable.
ITG0310	Can't open DSP channel.
ITG0311	Unable to get response from Follower card.
ITG0312	Unable to push BOOTP tab file to backup leader.
ITG0313	Keycode failed validation. Configuration file ignored.
Major Alarms - Immediate Intervention Required	
ITG0400	Fatal self-test failure. Card is out of service.
ITG0401	Reboot threshold exceeded. Manual intervention required.
ITG0402	Ethernet voice port failure.
ITG0403	Ethernet management port failure.
ITG0404	Can't open address translation file.
ITG0405	Keycode file failed validation during bootup.
ITG0406	Start-Up memory allocation failure. Card reboot initiated.
ITG0407	Unable to get response from leader card.
ITG0408	Bad address translation file. Reverting to previous version (if any).
ITG0409	Bad config file. Reverting to previous version (if any).

Table 26
ITG system error messages (alarms) (Part 3 of 3)

ITG0410	Remote leader not responding.
ITG0411	Failed to start UDP server for intercard messaging.
ITG0412	Failed to start UDP client for intercard messaging.
ITG0413	Failed to register with Leader card. Defaulting to fallback mode.
ITG0414	No response from Leader card.
ITG0415	Task spawn failed. Attempting a reboot.
ITG0416	Failed to start QOS / Network Probing Timer
ITG0417	Failed to Send Fallback Update to Followers
ITG0418	H.323 stack failed to initialize.
ITG0452	Meridian-1 messaging failure. Unable to process calls.

Replacing an ITG card

The ITG card should be replaced when the following conditions occur:

- If, following a reboot, the ITG card displays a code of the form “F:xx” on the faceplate LED display, this indicates an unrecoverable hardware failure and the card will not register with the Meridian 1. The exception is the "F:10" code, which may indicate that the Security Device is missing from the card.
- If the management Ethernet interface or the voice Ethernet interface on the ITG card has failed. This may be indicated by failure to show a link pulse on the voice IP interface status LED, or on the hub, or if the maintenance port continuously prints ’lnIsa0 Carrier Failure’ messages, after proving that the hub port and T-LAN cable are good.
- If a voice channel on the ITG card has a consistent voice quality fault, such as persistent noise or lack of voice path, even after resetting the card and retransmitting the card properties.
- Or, If the card cannot detect a known good Security Device.

The card should first be removed for 2-3 seconds and then reseated in the IPE shelf in order to perform a power-on reset. If the failure persists, there is no option but to replace the card. Use the following procedure to replace a faulty ITG card:

1 Locate the faulty card in the MAT ITG database by the TN, MAC address, and IP address.

2 Disable the faulty ITG card in overlay 32 with the **DISI** command. The Meridian 1 outputs "NPR011" when the card has been completely disabled by the DISI command.

3 Disconnect the T-LAN Ethernet cable from the faceplate of the faulty ITG card in the Meridian large system IPE module or the Option 11 cabinet. Label the cable to identify the LAN connection so that it can later be attached to the replacement ITG card.

WARNING

In the Option 11 cabinet the T-LAN cable is hidden behind the faceplate of the ITG card. The card or cable can be damaged if you attempt to remove the cable without using the correct procedure.

Note: Refer to Appendix A for detailing instructions on connecting the T-LAN cable to the ITG card in the option 11 cabinet.

4 Remove the faulty ITG card from the Meridian 1.

5 Remove the Security Device from the faulty ITG card. The Security Device is located on the top of the motherboard under the top edge of the daughterboard. The Security Device has a tab attached to it to facilitate removal and insertion on the motherboard.

Note: Be careful not to bend the Security Device retaining clip when removing or inserting the Security Device. If the replacement card cannot read the Security Device later in this procedure, gently bend the spring clip down, to increase contact pressure between the spring clip and the Security Device.

6 Select Leader 0 or any ITG card in the node.

7 Click **Configuration | Node | Properties** in the "IP Telephony Gateway" window.

8 Click the **Card Configuration** tab in the "ITG Node Properties" window.

9 In the "Card Configuration" tab, select the faulty ITG card from the list of cards in the node.

10 Change the "Management MAC" to the MAC address of the replacement ITG card. The MAC address is labeled on the faceplate of the replacement ITG card.

11 Click **OK**.

12 Select Leader 0 or any ITG card in the node.

13 Use the **Configuration | Synchronize | Transmit** command to transmit the Node Properties from MAT to the active leader card (Leader 0 or Leader 1) of the ITG node. Leave the default radio button selection "Transmit to Selected Nodes". Check the **Node Properties** box, and then click **Start Transmit**. This will update the node properties on the active leader card with the MAC Address of the replacement ITG card.

14 Install the Security Device that was removed from the faulty ITG card into the replacement ITG card.

Note: Be careful not to bend the Security Device retaining clip when removing or inserting the Security Device. If the replacement card cannot read the Security Device later in this procedure, gently bend the spring clip down, to increase contact pressure between the spring clip and the Security Device.

15 Install the replacement ITG card into the card slots in the Meridian 1 IPE module or option 11 cabinet:

Note: Refer to Appendix A for detailing instructions on connecting the T-LAN cable to the ITG card in the Option 11 cabinet.

- Pull the top and bottom locking devices away from the ITG faceplate.
- Insert the ITG card into the card guides and gently 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 remains lit until the card is configured and enabled in software, at which point in turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the ITG faceplate maintenance display to see startup selftest results and status messages. A display of the type "F:xx" indicates a failure. Some failures indicate that the card must be replaced. "F:10" indicates Security Device test failure: check for presence of Security Device on the card. Refer to "Prior to communication with the Meridian 1, the 8051XA controller will download FPGA data files and perform tests to ensure correct programming of the FPGA." on page 250 for a listing of display codes.

16 In the Meridian 1 large system IPE module, attach the T-LAN Ethernet cable to the faceplate of the replacement ITG card.

Note: Refer to Appendix A for detailing instructions on connecting the T-LAN cable to the ITG card in the Option 11 cabinet.

Note: When connecting the ITG card to the T-LAN, the link status LED on the ITG 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.

17 In the MAT "IP Telephony Gateway" main window, select **View | Refresh** and verify that the replacement ITG card status is showing "Unequipped."

Verifying card software

1 In the "IP Telephony Gateway" window, double-click the replacement ITG card to open the “Card Properties”. Leave the default selection of the ITG card in the "Card Properties" window, and click the “Configuration” tab.

2 Verify that the “S/W release” shows the latest recommended ITG card software version.

The website URL to check the latest recommended ITG software release is “https://www.nortel.com/secure/cgi-bin/itg/enter.cgi.”

The default user name is **usa**. The default password is **usa**. See your Nortel Network representative to register for a new default name and password if the default does not work.

If the replacement card requires a software upgrade, refer to the next procedure, *Upgrading ITG card software*.

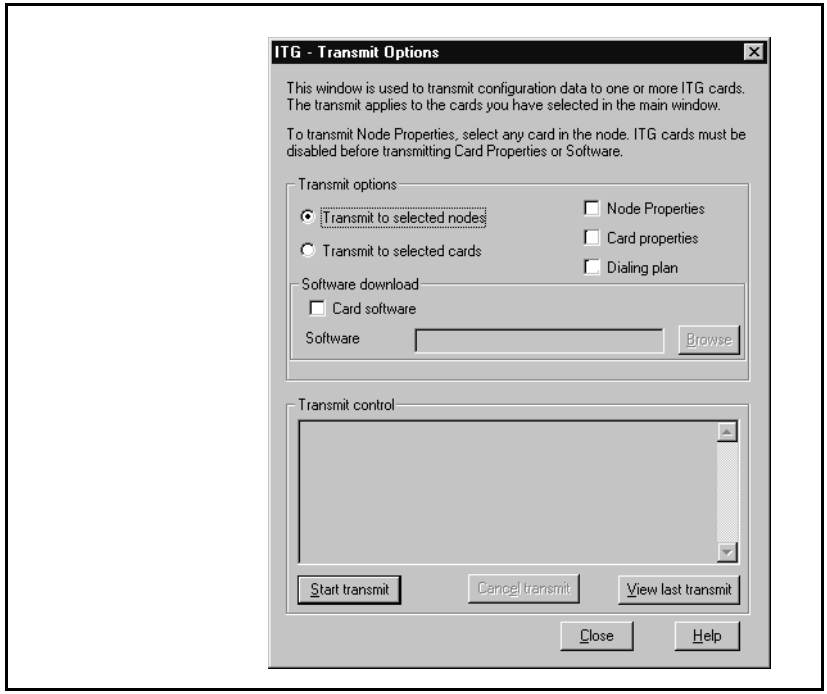
Transmitting Card Properties and Dialing Plan

Note: 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 **Configuration** | **Synchronize** | **Transmit.**

The "ITG - Transmit Options" window appears.



3 Select the radio button "Transmit to selected cards". Check the "Card properties" and "Dialing plan" boxes only.

4 Click the **Start Transmit** button.

The transmission status is displayed in the "Transmit control" box. Confirm that card properties and dialing plan are transmitted successfully.

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

6 Use overlay 14 to update the DES (description) of unit 0 of the replaced ITG card with the new MAC address.

7 Use the overlay 32 ENLC command to re-enable the ITG card.

8 In the “IP Telephony Gateway” main window, select **View | Refresh**. The card status should now show “Enabled.”

9 Update the Installation Summary Sheet with the new MAC address.

10 Verify the TN, management interface MAC address, IP addresses, the NT-SDID, and keycode for each ITG card. The NT_SDID and keycode are verified by double-clicking each ITG card in the MAT "IP Telephony Gateway" main window and clicking the “Configuration” tab of the "Card Properties." Compare the displayed values with those on the ITG Installation Summary Sheet.

Resolving problems with card replacement

Make test calls on the new card to verify good DSP channel performance.

If the card status is still unequipped after downloading the card properties, verify that the ITG card is able to read the Security Device and verify that the keycode in the "Card Properties" has been entered correctly according to the NT_SDID.

Consult the software license document that accompanied the original failed ITG card, or call your Nortel Networks representative and obtain the correct keycode for the NT_SDID that is read from the Security Device. The NT_SDID can be read from the MAT ITG "Card Properties" "Configuration" tab or from the ITG shell using the command **dongleIDShow**.

Meridian 1 system level maintenance of the ITG card

The ITG card system level maintenance can be performed in overlay 32, in the same manner as with the NT8D14 Universal Trunk card. Table 27 lists the commands supported on the ITG card.

Table 27
Overlay 32 - ITG maintenance commands

Command	Function
DISC l s c	Disable the specified card, where: l = loop, s = shelf, c = card
DISI l s c	Disable the specified card when idle, where: l = loop, s = shelf, c = card
DISU l s c u	Disable the specified unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the specified card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, where: l = loop, s = shelf, c = card
STAT l s c	Print the Meridian 1 software status of the specified card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 software status of the specified unit, where: l = loop, s = shelf, c = card, u = unit

Equivalent information to that provided by the STAT command can be accessed from the command line on the card, as described in “ITG shell commands” on page 233.

ITG shell commands

The ITG shell commands are accessed by connecting a TTY to the MMI port on the ITG card faceplate. Alternatively, the MAT ITG “Telnet” command can be used to access the ITG shell. Commands are grouped into six categories are shown in Tables 28 through 35.

Table 28
ITG Shell Commands (Part 1 of 4)

Command	Description
General-Purpose Commands:	
shellPasswordSet	Change the default ITG shell password.
itgCardShow	Show card info.
itgChanStateShow	Show state of channels. eg. busy or idle.
itgHelp	Shows the complete command list. "?" also shows the list.
ldrResTableShow	Show backup leader and followers for a given leader.
h323SessionShow	Show h323 session info for each channel
itgMemShow	Show memory usage
ifShow	Show detailed IP information, including MAC addresses.
IPInfoShow	Prints IP information.
numNodesInFallbackShow	Lists the IP addresses of node that are in Fallback.
cardRoleShow	Prints card role i.e Leader, Backup leader, follower.
cardStateShow	Prints card state i.e. Unequipped, Disabled, Enabled.
dongleIDShow	Prints out dongle ID.

Table 28
ITG Shell Commands (Part 2 of 4)

Command	Description
serialNumShow	Prints out card serial number.
firmwareVersionShow	Prints out firmware version number.
numChannelsShow	Prints out number of available channels.
swVersionShow	Prints out software version.
resetOm	Resets the operational measurement file timer.
logFileOn	Turns on logging.
logFileOff	Turns off logging.
logStatus	Shows whether logging is on or off.
emodelSim	Allows user to interactively determine QoS score.
File Transfer Commands:	
swDownload	Loads new version of s/w from MAT PC to ITG card.
DPTableGet	Sends an updated address table from MAT to ITG.
configFileGet	Sends an updated config.ini file from MAT to ITG.
bootpFileGet	Sends an updated bootptab file from MAT to ITG.
SNMPConfFileGet	Sends an updated snmp configuration file from MAT to ITG.
hostFileGet	Transfers any file from MAT to ITG.
currOmFilePut	Sends the current OM file from ITG to MAT.

Table 28
ITG Shell Commands (Part 3 of 4)

Command	Description
prevOmFilePut	Sends the previous OM file from ITG to MAT.
traceFilePut	Sends the trace file from ITG to MAT.
currLogFilePut	Sends the current log file from ITG to MAT.
prevLogFilePut	Sends the previous log file from ITG to MAT.
bootPFilePut	Sends the bootptab file from ITG to MAT.
hostFilePut	Transfers any file from ITG to MAT.
IP Configuration Commands:	
NVRIPSet	Sets the IP address in NVRAM.
NVRGWSet	Sets the default gateway address in NVRAM.
NVRSMSet	Sets the subnet mask in NVRAM..
NVRShow	Prints the values of the IP parameters that reside in NVRAM.
nvramLeaderSet	Sets the leader bit in NVRAM.
nvramLeaderClr	Clears the leader bit in NVRAM, but does not erase the IP parameters in NVRAM
NVRClear	Clears IP parameters in NVRAM.
setLeader	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..

Table 28
ITG Shell Commands (Part 4 of 4)

Command	Description
clearLeader	The one command that does all the necessary actions to clear the leader info in NVRAM and set the boot method to use bootp, thus, making the card a follower.
Card Commands:	
itgSetVAD	Sets the Voice Activity Detection to enabled or disabled.
itgVADShow	Shows the VAD configuration and the current DSP setting.
cardReset	Warm reboot of ITG card.
DSP Commands:	
DSPReset	Resets the specified DSP
DSPselfTest	Runs selftest on the DSP.
DSPNumShow	Prints number of DSPs on ITG card.
DSPPcmLpbkTestOn	Starts pcm loopback test on the specified DSP.
DSPPcmLpbkTestOff	Stops pcm loopback test on the specified DSP.
DSPSndLpbkTestOn	Starts Send loopback test on the specified DSP.
DSPSndLpbkTestOff	Stops Send loopback test on the specified DSP.
DSPRcvLpbkTestOn	Starts Receive loopback test on the specified DSP.
DSPRcvLpbkTestOff	Stops Receive loopback test on the specified DSP.

Table 29
General-Purpose Commands (Part 1 of 4)

Synopsis:	**itgCardShow**
Description:	Show card info.
Synopsis:	**ldrResTableShow**
Description:	Show backup leader and followers for a given leader.
Synopsis:	**itgChanStateShow**
Description:	Show state of channels. eg. busy or idle.
Synopsis:	**h323SessionShow**
Description:	Show h323 session info for each channel
Synopsis:	**itgMemShow**
Description:	Show memory usage
Synopsis:	**ifShow**
Description:	Show detailed IP information, including MAC addresses.
Synopsis:	**IPinfoShow**
Description:	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 mask (for both management and voice networks) • SNMP manager • gatekeeper
Synopsis:	**cardRoleShow**
Description:	Prints card role i.e Leader, Backup leader, follower.

Table 29
General-Purpose Commands (Part 2 of 4)

Synopsis:	**cardStateShow**
Description:	card state i.e. Unequipped, Disabled, Enabled.
Synopsis:	**itgHelp**
Description:	Displays the ITG commands and a short description. ITG>? **itgHelp**: Show complete command list. ? will also show command list. **itgCardShow:** Show card information. l**drResTableShow** Display Leader card's resource Table. **itgChanStateShow** Show Channel States. **h323SessionShow** Show H.323 session states. **itgMemShow** Show status of ITG memory usage. **IPInfoShow** Shows IP info for management and voice ports **cardStateShow** Prints cardState i.e. Unequipped, Disabled,Enabled **dongleIDShow** Prints out Dongle ID. **serialNumShow** Prints our card serial number **firmwareVersionShow** Prints out firmware version number. **numChannelsShow** Prints out number of available channels. **numNodesInFallbackShow** Prints out number of nodes in fallback to PSTN state. **swVersionShow** Prints out software version. **swDownload** Load a new software version to flash **DPFileGet** Updates the address table on the ITG card. **configFileGet** Updates the configuration file on the ITG card. **bootPFileGet** Updates the bootptab file on the ITG card. **hostFileGet** Gets any file from the host and puts to the specified location on the ITG card. Type <CR> to continue, Q<CR> to stop:
Synopsis:	**shellPasswordSet**

Table 29
General-Purpose Commands (Part 3 of 4)

Description:	Change the current user name and password.
Synopsis:	**dongleIDShow**
Description:	Prints out dongle ID.
Synopsis:	**serialNumShow**
Description:	Prints our card serial number. Command displays the same ITG card serial number that is displayed from the Meridian 1 IDC command.
Synopsis:	**firmwareVersionShow**
Description:	Prints out firmware version number.
Synopsis:	**numChannelsShow**
Description:	Prints out number of available channels.
Synopsis:	**swVersionShow**
Description:	Prints out software version.

Table 29
General-Purpose Commands (Part 4 of 4)

Synopsis:	**resetOm**
Description:	Resets the operational measurement file timer.
Synopsis:	**logFileOn**
Description:	Turns on logging.
Synopsis:	**logFileOff**
Description:	Turns off logging.
Synopsis:	**logStatus**
Description:	Shows whether logging is on or off.
Synopsis:	**emodelSim**
Description:	Allows user to interactively determine QoS score.

Table 30
File Transfer Commands (Part 1 of 4)

Synopsis:	**swDownload** hostname, username, password, directory path, filename
Description:	Updates 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 verify 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 the either 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”
Synopsis:	**DPFileGet** hostname, username, password, directory path, filename

Table 30
File Transfer Commands (Part 2 of 4)

Description:	Updates the address table on the ITG card with the address table file on the specified host, account and path. The ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.
Example:	ITG> DPFileGet “ngals042”, “anonymous”, ”guest”, “/dialPlan”, ”dialingPlan.txt"
Synopsis:	**configFileGet** hostname, username, password, directory path, filename
Description:	Updates the config.ini file on the ITG card with the config.ini file on the specified host, account and path. The configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.
Example:	ITG> ConfigFileGet “ngals042”, “anonymous”, ”guest”, “/configDir”, ”config.ini”
Synopsis:	**bootPFileGet** hostname, username, password, directory path, filename
Description:	Updates the bootptab file on the ITG card with the bootptab file on the specified host, account and path. The bootpFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.
Example:	ITG> bootpFileGet “ngals042”, “anonymous”, ”guest”, “/bootpDir”, ”bootptab”
Synopsis:	**SNMPConfFileGet** hostname, username, password, directory path, filename
Description:	Updates the snmp configuration file on the ITG card with the snmp configuration file on the specified host, account and path. The SNMPConfFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system.
Example:	ITG> SNMPConfFileGet “ngals042”, “anonymous”, ”guest”, “/snmpDir”, ”agent.cnf”
Synopsis:	**hostFileGet** hostname, username, password, directory path, filename, ITGFileName, listener

Table 30
File Transfer Commands (Part 3 of 4)

Description:	Gets 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
Synopsis:	**currOmFilePut** hostname, username, password, directory path, filename
Description:	The omFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card’s operational measurements file to the specified location on the host.
Example:	ITG> currOmFilePut “ngals042”, “anonymous”, ”guest”, “/currDir”, ”omFile”
Synopsis:	**prevOmFilePut** hostname, username, password, directory path, filename
Description:	The omFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card’s operational measurements file to the specified location on the host.
Example:	ITG> prevOmFilePut “ngals042”, “anonymous”, ”guest”, “/prevDir”, ”omFile”
Synopsis:	**traceFilePut** hostname, username, password, directory path, filename
Description:	The traceFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card’s call trace file to the specified location on the host.
Example:	ITG> traceFilePut “ngals042”, “anonymous”, ”guest”, “/trcDir”, ”trcFile”
Synopsis:	**currLogFilePut** hostname, username, password, directory path, filename
Description:	The logFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card’s logfile the to specified location on the host.
Example:	ITG> currLogFilePut “ngals042”, “anonymous”, ”guest”, “/currDir”, ”logFile”
Synopsis:	**prevLogFilePut** hostname, username, password, directory path, filename

Table 30
File Transfer Commands (Part 4 of 4)

Description:	The logFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card's logfile the to specified location on the host.
Example:	ITG> prevLogFilePut “ngals042”, “anonymous”, ”guest”, “/currDir”, ”logFile”
Synopsis:	**bootPFilePut** hostname, username, password, directory path, filename
Description:	The bootpFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG card's bootp file the to specified location on the host.
Example:	ITG> bootpFilePut “ngals042”, “anonymous”, ”guest”, “/bootpDir”, ”bootpFile”
Synopsis:	**hostFilePut** hostname, username, password, directory path, filename, ITGFileName
Description:	Transfers any file on the ITG card from location ITGFileName and does a put via FTP to the host specified by hostname, username, password and directory path. Note: ITGFileName is the full path, i.e. 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 31
IP Configuration Commands (Part 1 of 3)

Synopsis:	**numNodesInFallbackShow**
Description:	Lists the IP addresses of the nodes that are in Fallback.
Example:	ITG> numNodesInFallbackShow 47.82.xx.xxx xx.xx.xx.xxx
Synopsis:	**NVRIPSet** “IP address”

Table 31
IP Configuration Commands (Part 2 of 3)

Description:	Sets the IP address in NVRAM.
Example:	ITG> NVRRIPSet “47.23.34.19”
Synopsis:	**NVRGWSet** “IP gateway”
Description:	Sets the default gateway address in NVRAM.
Example:	ITG> NVRRGWSet “47.0.0.1”
Synopsis:	**NVRSMSet** ”subnet mask”
Description:	Sets the subnet mask in NVRAM..
Example:	ITG> NVRRSMSet “255.255.240.0”
Synopsis:	**NVRIPShow**
Description:	Prints the values of the IP parameters that reside in NVRAM.
Example:	ITG> NVRIPShow
Synopsis:	**nvramLeaderSet** “IP address”, “IP gateway”, ”subnet mask”
Description:	Sets the leader bit in NVRAM.
Example:	ITG> nvramLeaderSet
Synopsis:	**nvramLeaderClr**
Description:	Clears the leader bit in NVRAM, but does not erase the IP parameters in NVRAM
Example:	ITG> nvramLeaderClr
Synopsis:	**NVRClear**
Description:	Clears IP parameters in NVRAM.

Table 31
IP Configuration Commands (Part 3 of 3)

Example:	ITG> NVRClear
Synopsis:	**setLeader** “IP address”, “IP gateway”, ”subnet mask”
Description:	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”
Synopsis:	**clearLeader**
Description:	The one command that does all the necessary actions to clear the leader info in NVRAM and set the boot method to use bootp, thus, making the card a follower.
Example:	ITG> clearLeader

Table 32
Card Commands

Synopsis:	**itgSetVAD**
Description:	Sets the Voice Activity Detection to disabled (0) or enabled (1). After setting this, you must download the card properties so the new settings take effect. If VAD is turned off, the voice payload size of 10ms is not supported for G.711 a/u law and G.729A codecs. The voice payload size for these codecs should be set to at least 20ms in MAT. In the event that the codec is configured for 10ms with VAD disabled, the call processing software will automatically select a minimum voice payload size of 20ms during call setup via codec negotiation procedures.
Example:	ITG> itgSetVAD 0 Disables the VAD ITG> itgSetVAD 1 Enables the VAD
Synopsis:	**itgVADShow**
Description:	Shows the VAD configuration and the current DSP setting. If the configured voice activity setting is correct and different from the setting currently on the DSP, then transmit the card properties from MAT ITG in order to update the setting on the DSP. If the DSP setting is correct, then use the ITGSetVAD command to change the configured settings to be the same as the setting currenty on the DSP.
Example:	ITG> itgVADShow
Synopsis:	**cardReset**
Description:	Performs a warm reboot of the ITG card. The card has to be in OOS state to be able to use this command.

Table 33
DSP Commands (Part 1 of 3)

Synopsis:	**DSPReset** DSP Number
Description:	Resets specified DSP
Example:	ITG>DSPReset 0

Table 33
DSP Commands (Part 2 of 3)

Synopsis:	**DSPSelfTest** DSP Number
Description:	Runs selftest on specified DSP: DSPSelfTest <DSP#>
Example:	ITG>DSPSelfTest 0
Synopsis:	**DSPNumShow**
Description:	Prints number of DSPs on ITG card.
Example:	ITG>DSPNumShow
Synopsis:	**DSPPcmLpbkTestOn**
Description:	Starts pcm loopback test on specified DSP.
Example:	ITG>DSPPcmLpbkTestOn
Synopsis:	**DSPPcmLpbkTestOff**
Description:	Stops pcm loopback test on specified DSP.
Example:	ITG> DSPPcmLpbkTestOff
Synopsis:	**DSPSndLpbkTestOn**
Description:	Starts sendloopback test on the specified DSP.
Example:	ITG> DSPSndLpbkTestOn
Synopsis:	**DSPSndLpbkTestOff**
Description:	Stops sendloopback test on specified DSP.
Example:	ITG> DSPSndLpbkTestOff

Table 33
DSP Commands (Part 3 of 3)

Synopsis:	**DSPRcvLpbkTestOn**
Description:	Starts receive loopback test on specified DSP.
Example:	ITG> DSPRcvLpbkTestOn
Synopsis:	**DSPRcvLpbkTestOff**
Description:	Stops receive loopback test on specified DSP.
Example:	ITG> DSPRcvLpbkTestOff

Table 34
Operational Measurement Queries

Synopsis:	**resetOM**
Description:	Resets the OM counter to collect data every hour from when command is issued.

Table 35
Log File Commands

Synopsis:	**logFile** on/off
Description:	turn on/off the log file
Synopsis:	**logFileShow**
Description:	Show whether logging is on or off.

ITG card selftests

During power-up, the ITG card performs diagnostic tests to ensure correct operation. The faceplate RS-232 port on the ITG card can be used to monitor the progress of these tests. Messages indicating the completion of each phase of testing as well as any detected faults will be echoed on this port.

Additionally, the ITG card has a hex LED 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 progress of the selftest, and an indication of the first failure detected.

At power-up, the 8051XA controller on the ITG card takes control of the system and ensures that the 486 processor is initially held in a reset state. The 8051XA controller will take control of one of the RS-232 ports and will use it to communicate to a maintenance terminal in order to display the results of the power-up selftest and diagnostics. The initial tests to be performed include:

- 8051XA controller self-test, including ROM checksum, onboard RAM, and timer tests, and
- external data/program RAM, and dual port memory tests.

Following the successful completion of these tests, the 8051XA controller will then attempt to bring up the 486 processor by clearing the reset, and entering a timing loop in anticipation of receiving a message from the 486 processor. If this loop times out, it will output an error to the RS-232 port. It will attempt to bring up the 486 processor two more times before indicating an unrecoverable card failure.

Similarly, if a message is received from the 486 processor, but the message indicates a failure of one or more of the circuit elements connected to the 486 processor, up to two more resets will be attempted before entering the unrecoverable failure state. This ensures that failures due to erratic power-up or reset conditions do not cause unnecessary failure of the card. The failures are logged to the RS-232 faceplate port, however, to provide information to the maintenance technician that there may be a problem with the card.

Once the 486 processor responds correctly, the 8051XA controller will switch its serial port to provide Card LAN communication and connect the 486 processor with the external RS-232 port.

Card LAN

The ITG card will support the backplane Card LAN interface for the purposes of communicating selftest errors and allowing maintenance access including resetting the card remotely.

BIOS selftest

The ITG card contains its own VxWorks based BIOS. At power-up, the BIOS will perform 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 selftest

The ITG card base code will perform the following tests:

- flash integrity test
- PGA read/write test
- PCMCIA controller test (also tests the PCI bus)
- Timer and DMA tests
- DSP test

FPGA testing

Prior to communication with the Meridian 1, the 8051XA controller will download FPGA data files and perform tests to ensure correct programming of the FPGA.

Troubleshooting a software load failure

Symptoms

MAT cannot establish connection with ITG card. The faceplate LCD display reads "BIOS."

Problem

the ITG card has booted the BIOS load.

Diagnosis

in the event of a failure to load and run the ITG software, the ITG card will default to the BIOS load. This load consists of a prompt that allows commands to reload the ITG software and reboot (see below).

Three known reasons can cause the failure to load the ITG software:

- Not enough memory due to a faulty or missing SIMM.
- Corruption of the ITG software image in flash memory.
- The escape sequence to boot from the BIOS has been inadvertently sent down the serial line due to noise.

To determine which of the three causes caused the ITG load failure, reboot and monitor the booting sequence through the serial port. Capture the booting sequence to aid in communication with technical support personnel.

Examples of booting sequences:

Case 1: The following excerpt from the booting sequence indicates the amount of memory onboard.

```
Memory Configuration
Onboard: 4MB
SIMM: 16MB
Total: 20MB
```

In the absense or failure of the SIMM, the total memory would be 4MB, which is not enough to support the ITG application.

Case 2: The following excerpt from the booting sequence indicates the ITG card locating and loading the ITG software from flash memory:

```
Cookie array value: 0x111111100

Checksum Validation at Bank Address: 0xF9800000
Checksum in ROM = 35582602
Length of bank = 0004FEF8
Calculated Checksum = 35582602

Checksum array value: 0x11111100

Loading code from address: F9800010
Verifying ROM to RAM copy...
ROM to RAM copy completed OK
Jumping to VxWorks at 0x00E00000
EIP = 0x00E0011E
Jumping to romStart at 0x00E00300
```

In the event of a software load failure, the boot sequence indicates that the BIOS is being loaded:

```
Cookie array value: 0x11111111
Booting from BIOS ROM
```

Case 3: The boot sequence indicates that the "xxx" sequence has been entered and the BIOS is being loaded:

Solutions

Case 1: In the case of a missing SIMM, install a 16MB SIMM into the SIMM slot which is found underneath the ITG daugherboard. If the SIMM is present, check that the SIMM is properly seated. Otherwise, the SIMM may be faulty and need replacement.

Case 2: Reattempt a software download from the MAT host. Use the following commands:

```
upgradeErase
upgrade "hostname","hostAccount","hostPassword",
         "hostDirectoryPath","hostSWFilename"
```

After the software loads to flash, reboot the card:

```
sysReboot
```

If the failure to load the ITG software into RAM persists, then the flash device is faulty. Replace the ITG card.

Case 3: The escape sequence "xxx" is rarely transmitted. Reboot the card.

Warm rebooting the ITG card

The following ITG shell command performs a warm reboot of an out-of-service ITG card: **cardReset**

Testing the ITG card DSPs

At the ITG shell, the following two tests can be performed on the ITG DSPs:

- To run a selftest on the DSP daughterboard: **DSPselfTest**

Note: If the DSP self test fails, the ITG card must be replaced.

- To run a PCM loopback test, a Send loopback test, or a Receive loopback test on the DSP daughterboard, respectively:

DSPPcmLpbkTestOn ("DSPPcmLpbkTestOff" to stop the test)
DSPSndLpbkTestOn ("DSPSndLpbkTestOff" to stop the test)
DSPRcvLpbkTestOn ("DSPRcvLpbkTestOff" to stop the test)

Note: The DSPs and all associated ports must be disabled before performing these tests.

Working with alarm and log files

Alarm and log file ouput is turned on via the ITG shell. The following commands may be performed at the ITG shell prompt:

- to turn on/off the error log file, type: **logFileOn** or **logFileOff**.
- to display the modes of all log files/alarms, type: **logFileShow**.

Appendix A: Cabling

ITG cabling configuration and requirements are the same for Option 11 and large systems. ITG supports both separate E-LAN (Management LAN) and T-LAN (Telephony LAN) subnets and common E-LAN and T-LAN subnet. The final connection from ITG to the customer's Intranet should be adjusted based on the desired configuration.

The ITG requires separate cables to connect to the voice and management LANs. In addition, a serial cable may be required to connect to the faceplate Serial Port for maintenance purposes (including Leader card configuration). Alternatively, access to the serial maintenance port is also available at the I/O panel via the DB-9 female connector of the NTMF94DA cable assembly, presenting an external interface connection point and obviating the requirement for the faceplate connection.

WARNING

The serial maintenance ports presented at the faceplate and at the backplane are identical. Do not connect a terminal to both access points simultaneously. This will result in incorrect and un-predictable operation of the ITG Assembly.

NTAG81CA Maintenance Cable

This cable is required to connect a PC or terminal to the ITG via the maintenance port connector on the faceplate for administration. This cable may be connected directly to the 9-pin D-type RS232 input on a standard PC.

Figure 31
Maintenance cable

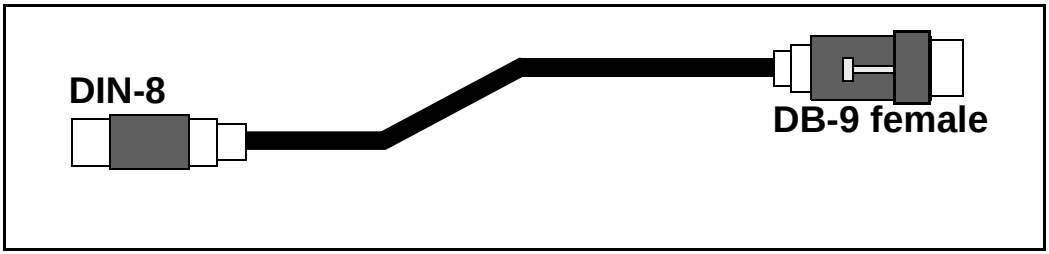


Table 36
NTAG81CA Maintenance cable pin description

Signals (MIX Side)	8-pin Mini-DIN (MIX 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

This three-meter cable connects the NTAG81CA cable to a PC or terminal. It has a nine-pin D-type connector at both ends, one male, one female. It can also be used to extend the serial port presented by the NTMF94DA I/O panel cable.

Figure 32
Maintenance Extender cable

Table 37
Maintenance 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

NTMF94DA Management Port & Serial I/O Cabling

The NTMF94DA provides the E-LAN, T-LAN ports that provide the interface from the ITG card to the customer's network equipment, and one DB9 serial port that provides serial connection between the card and the customer PC or TTY (see Figure 33). Table 38 describes the NTMF94DA cable pins.

It is very important to use the mounting screw provided to secure the top of the NTMF94DA cable 25-pair Amphenol connector to the Meridian 1. The screw ties the LAN cable shield to the Meridian 1 frame ground for EMC compliance.

The NTMF94DA cable provides a factory installed, shielded, RJ45 to RJ45 coupler at the end of both the E-LAN and T-LAN ports. An unshielded coupler is provided to prevent ground loops (if required). Turn to page 261 for a test that helps you decide if you have to use the unshielded coupler. Both ends of the RJ45 ports of the cables are labeled as to which is the T-LAN and which is the E-LAN. The ports provide the connection point to the customer's E-LAN and T-LAN equipment. You must use shielded Category 5 cable to connect to the customer's equipment. To improve EMC performance, use standard cable ties to bundle all LAN cables as they route out of the system.

> ***Note:*** To avoid damage to Category 5 cable, do not overtighten cable ties.

Figure 33
NTMF94DA E-LAN, T-LAN & RS-232 Serial Maintenance I/O cable

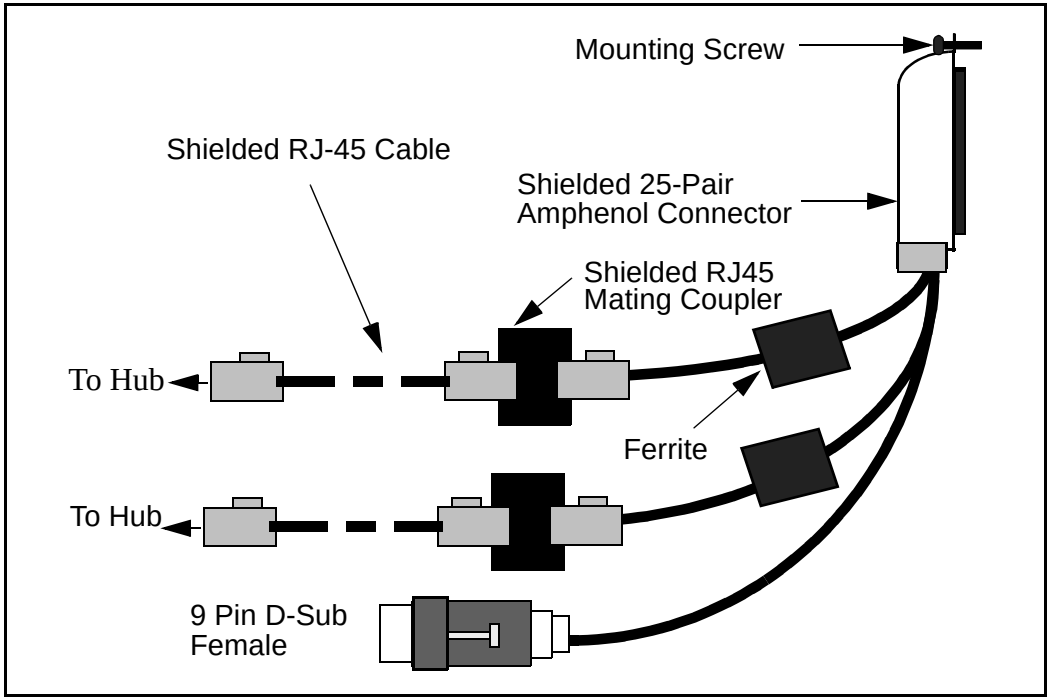


Table 38
NTMF94DA cable pin description (Part 1 of 2)

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

Table 38
NTMF94DA cable pin description (Part 2 of 2)

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RXDB+	P4-3	GRN/WHT
P1-19	TXDB+	P4-1	ORG/WHT
P1-43	RXDB-	P4-6	WHT/GRN
P1-44	TXDB-	P4-2	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
P1-25	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.

Appendix B: Product integrity

This chapter presents information about Meridian Integrated IP Telephony Gateway (ITG) card reliability, environmental specifications, and electrical regulatory standards.

Reliability

Reliability is measured by the Mean Time Between Failures (MTBF).

Mean time between failures (MTBF)

The ITG card Mean Time Between Failure (MTBF) is 36.95 years.

Environment specifications

Measurements of performance in regards to temperature and shock were made under test conditions as described in the following table.

Temperature-related conditions

Refer to Table 39 for a display of acceptable temperature and humidity ranges for the ITG card.

Table 39
ITG environmental specifications

Specification	Minimum	Maximum
Normal Operation		
Recommended	15° C	30° C
Relative humidity	20%	55% (non-condensing)
Absolute	10 ° C	45° C
Relative humidity	20% to	80% (non-condensing)
Short Term (less than 72 hr)	–40° C	70° C
Rate of change	Less than 1° C per 3 minutes	
Storage		
Recommended	–20° C	60° C
Relative Humidity	5%	95% (non-condensing
	-40° C to 70° C, non-condensing	
Temperature Shock		
In 3 minutes	-40° C	25° C
In 3 minutes	70° C	25° C
	-40° to 70° C, non-condensing	

Electrical regulatory standards

The following three tables list the safety and electro-magnetic compatibility regulatory standards for the ITG card, listed by geographic region. Specifications for the ITG card meet or exceed the standards listed in these regulations.

Safety

Table 40 provides a list of safety regulations met by the ITG card, along with the type of regulation and the country/region covered by each regulation.

Table 40
Safety regulations

Regulation Identifier	Regulatory Agency
UL 1459	Safety, United States, CALA
CSA 22.2 225	Safety, Canada
EN 41003	Safety, International Telecom
EN 60950/IEC 950	Safety, International
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
AS3260, TS001 - TS004, TS006	Safety/Network (Australia)
JATE	Safety/Network (Japan)

Electro-magnetic compatibility (EMC)

Table 41 lists electro-magnetic emissions regulations met by the ITG card, along with the country's standard that lists each regulation.

Table 41
Electro-Magnetic 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
EN55022/CISPR 22 CLASS B	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 42 lists electro-magnetic immunity regulations met by the ITG card, along with the country's standard that lists each regulation.

Table 42
Electro-Magnetic Immunity

Regulation Identifier	Regulatory Agency
CISPR 22 Sec. 20 Class B	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 3548	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Appendix C: Convert from CIDR to dotted decimal format

Subnet masks may 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 in order 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. Therefore, a typical CIDR format subnet mask will be 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 decimal 255 represents binary 1111 1111.

To convert the subnet mask from CIDR format to dotted decimal format:

1 Divide the CIDR format value by 8. The quotient (the number of times that eight divides into the CIDR format value) equals the number of dotted decimal fields containing 255.

In the example above, the subnet mask is expressed as /20. Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.

2 If there is a remainder, refer to Table 43, to obtain the dotted decimal value for the field following the last field containing “255”. In the example of /20 above, the remainder is four. In Table 43, a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next and last field is 240. Therefore the first three 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. Therefore, in the example of /20, the complete subnet mask in dotted decimal format is 255.255.240.0.

Table 43
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: Estimate QoS Level

Table 44 estimates the ITG QoS level based on QoS measurements of the intranet. The packet loss and one-way delay values are tabulated in increments of 1% and 10ms respectively.

Table 44
QoS Levels (Part 1 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
0	50	excellent	excellent	excellent
0	60	excellent	excellent	excellent
0	70	excellent	excellent	excellent
0	80	excellent	excellent	excellent
0	90	excellent	excellent	excellent
0	100	excellent	excellent	excellent
0	110	excellent	excellent	excellent
0	120	excellent	excellent	excellent
0	130	excellent	excellent	excellent
0	140	excellent	excellent	excellent
0	150	excellent	excellent	excellent

Table 44
QoS Levels (Part 2 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
0	160	excellent	excellent	excellent
0	170	excellent	excellent	excellent
0	180	excellent	excellent	excellent
0	190	excellent	excellent	excellent
0	200	excellent	excellent	excellent
0	210	excellent	excellent	good
0	220	excellent	excellent	good
0	230	good	excellent	good
0	240	good	excellent	good
0	250	good	excellent	good
0	260	good	excellent	good
0	270	good	excellent	good
0	280	good	excellent	good
0	290	good	excellent	good
0	300	good	excellent	good
0	310	good	excellent	good
0	320	good	excellent	good
0	330	good	excellent	good
0	340	good	good	good
0	350	good	good	good

Table 44
QoS Levels (Part 3 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
0	360	good	good	good
0	370	good	good	fair
0	380	good	good	fair
0	390	fair	good	fair
0	400	fair	good	fair
0	410	fair	good	fair
0	420	fair	good	fair
0	430	fair	good	fair
0	440	fair	good	fair
0	450	fair	good	fair
0	460	fair	good	fair
0	470	fair	good	fair
0	480	fair	good	fair
0	490	fair	good	fair
0	500	fair	good	fair
0	510	fair	good	fair
0	520	fair	good	fair
0	530	fair	good	fair
0	540	fair	good	fair
0	550	fair	good	fair

Table 44
QoS Levels (Part 4 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
0	560	fair	good	fair
0	570	fair	good	fair
0	580	fair	good	fair
0	590	fair	good	fair
0	600	fair	good	fair
0	610	fair	good	fair
0	620	fair	good	fair
0	630	fair	fair	fair
0	640	fair	fair	fair
0	650	fair	fair	fair
0	660	fair	fair	fair
0	670	fair	fair	fair
0	680	fair	fair	fair
0	690	fair	fair	fair
0	700	fair	fair	fair
0	710	fair	fair	fair
0	720	fair	fair	fair
0	730	fair	fair	fair
0	740	fair	fair	fair
0	750	fair	fair	fair

Table 44
QoS Levels (Part 5 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
0	760	fair	fair	fair
0	770	fair	fair	fair
0	780	fair	fair	fair
0	790	fair	fair	poor
1	50	excellent	excellent	good
1	60	excellent	excellent	good
1	70	excellent	excellent	good
1	80	excellent	excellent	good
1	90	excellent	excellent	good
1	100	excellent	excellent	good
1	110	excellent	excellent	good
1	120	excellent	excellent	good
1	130	excellent	excellent	good
1	140	excellent	excellent	good
1	150	excellent	excellent	good
1	160	excellent	excellent	good
1	170	excellent	excellent	good
1	180	excellent	excellent	good
1	190	good	excellent	good
1	200	good	excellent	good

Table 44
QoS Levels (Part 6 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
1	210	good	good	good
1	220	good	good	good
1	230	good	good	good
1	240	good	good	good
1	250	good	good	good
1	260	good	good	good
1	270	good	good	good
1	280	good	good	good
1	290	good	good	good
1	300	good	good	good
1	310	good	good	good
1	320	good	good	good
1	330	good	good	fair
1	340	good	good	fair
1	350	fair	good	fair
1	360	fair	good	fair
1	370	fair	fair	fair
1	380	fair	fair	fair
1	390	fair	fair	fair
1	400	fair	fair	fair

Table 44
QoS Levels (Part 7 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
1	410	fair	fair	fair
1	420	fair	fair	fair
1	430	fair	fair	fair
1	440	fair	fair	fair
1	450	fair	fair	fair
1	460	fair	fair	fair
1	470	fair	fair	fair
1	480	fair	fair	fair
1	490	fair	fair	fair
1	500	fair	fair	fair
1	510	fair	fair	fair
1	520	fair	fair	fair
1	530	fair	fair	fair
1	540	fair	fair	fair
1	550	fair	fair	fair
1	560	fair	fair	fair
1	570	fair	fair	fair
1	580	fair	fair	fair
1	590	fair	fair	fair
1	600	fair	fair	fair

Table 44
QoS Levels (Part 8 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
1	610	fair	fair	fair
1	620	fair	fair	fair
1	630	fair	fair	fair
1	640	fair	fair	poor
1	650	fair	fair	poor
1	660	fair	fair	poor
1	670	fair	fair	poor
1	680	fair	fair	poor
1	690	fair	fair	poor
1	700	poor	fair	poor
1	710	poor	fair	poor
1	720	poor	fair	poor
1	730	poor	fair	poor
1	740	poor	fair	poor
1	750	poor	fair	poor
1	760	poor	fair	poor
1	770	poor	fair	poor
1	780	poor	fair	poor
2	50	good	good	good
2	60	good	good	good

Table 44
QoS Levels (Part 9 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
2	70	good	good	good
2	80	good	good	good
2	90	good	good	good
2	100	good	good	good
2	110	good	good	good
2	120	good	good	good
2	130	good	good	good
2	140	good	good	good
2	150	good	good	good
2	160	good	good	good
2	170	good	good	good
2	180	good	good	good
2	190	good	good	good
2	200	good	good	good
2	210	good	good	good
2	220	good	good	good
2	230	good	good	good
2	240	good	good	good
2	250	good	good	good
2	260	good	good	good

Table 44
QoS Levels (Part 10 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
2	270	good	good	good
2	280	good	good	fair
2	290	good	good	fair
2	300	good	good	fair
2	310	good	fair	fair
2	320	good	fair	fair
2	330	fair	fair	fair
2	340	fair	fair	fair
2	350	fair	fair	fair
2	360	fair	fair	fair
2	370	fair	fair	fair
2	380	fair	fair	fair
2	390	fair	fair	fair
2	400	fair	fair	fair
2	410	fair	fair	fair
2	420	fair	fair	fair
2	430	fair	fair	fair
2	440	fair	fair	fair
2	450	fair	fair	fair
2	460	fair	fair	fair

Table 44
QoS Levels (Part 11 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
2	470	fair	fair	fair
2	480	fair	fair	fair
2	490	fair	fair	fair
2	500	fair	fair	fair
2	510	fair	fair	fair
2	520	fair	fair	poor
2	530	fair	fair	poor
2	540	fair	fair	poor
2	550	fair	fair	poor
2	560	fair	fair	poor
2	570	fair	fair	poor
2	580	fair	fair	poor
3	50	good	good	good
3	60	good	good	good
3	70	good	good	good
3	80	good	good	good
3	90	good	good	good
3	100	good	good	good
3	110	good	good	good
3	120	good	good	good

Table 44
QoS Levels (Part 12 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
3	130	good	good	good
3	140	good	good	good
3	150	good	good	good
3	160	good	good	good
3	170	good	good	good
3	180	good	good	good
3	190	good	good	good
3	200	good	good	good
3	210	good	good	good
3	220	good	good	good
3	230	good	good	good
3	240	good	good	good
3	250	good	good	good
3	260	good	good	fair
3	270	fair	fair	fair
3	280	fair	fair	fair
3	290	fair	fair	fair
3	300	fair	fair	fair
3	310	fair	fair	fair
3	320	fair	fair	fair

Table 44
QoS Levels (Part 13 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
3	330	fair	fair	fair
3	340	fair	fair	fair
3	350	fair	fair	fair
3	360	fair	fair	fair
3	370	fair	fair	fair
3	380	fair	fair	fair
3	390	fair	fair	fair
3	400	fair	fair	fair
3	410	fair	fair	fair
3	420	fair	fair	fair
3	430	fair	fair	fair
3	440	fair	fair	fair
3	450	fair	fair	fair
3	460	fair	fair	fair
3	470	fair	fair	poor
3	480	fair	fair	poor
3	490	fair	fair	poor
4	50	good	good	good
4	60	good	good	good
4	70	good	good	good

Table 44
QoS Levels (Part 14 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
4	80	good	good	good
4	90	good	good	good
4	100	good	good	good
4	110	good	good	good
4	120	good	good	good
4	130	good	good	good
4	140	good	good	good
4	150	good	good	good
4	160	good	good	good
4	170	good	good	good
4	180	good	good	good
4	190	good	good	good
4	200	good	good	good
4	210	good	good	fair
4	220	good	good	fair
4	230	good	good	fair
4	240	good	good	fair
4	250	fair	fair	fair
4	260	fair	fair	fair
4	270	fair	fair	fair

Table 44
QoS Levels (Part 15 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
4	280	fair	fair	fair
4	290	fair	fair	fair
4	300	fair	fair	fair
4	310	fair	fair	fair
4	320	fair	fair	fair
4	330	fair	fair	fair
4	340	fair	fair	fair
4	350	fair	fair	fair
4	360	fair	fair	fair
4	370	fair	fair	fair
4	380	fair	fair	fair
4	390	fair	fair	fair
4	400	fair	fair	poor
4	410	fair	fair	poor
4	420	fair	fair	poor
4	430	fair	fair	poor
4	440	fair	fair	poor
5	50	good	good	good
5	60	good	good	good
5	70	good	good	good

Table 44
QoS Levels (Part 16 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
5	80	good	good	good
5	90	good	good	good
5	100	good	good	good
5	110	good	good	good
5	120	good	good	good
5	130	good	good	good
5	140	good	good	good
5	150	good	good	good
5	160	good	good	good
5	170	good	good	good
5	180	good	good	good
5	190	good	good	fair
5	200	good	good	fair
5	210	good	good	fair
5	220	fair	fair	fair
5	230	fair	fair	fair
5	240	fair	fair	fair
5	250	fair	fair	fair
5	260	fair	fair	fair
5	270	fair	fair	fair

Table 44
QoS Levels (Part 17 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
5	280	fair	fair	fair
5	290	fair	fair	fair
5	300	fair	fair	fair
5	310	fair	fair	fair
5	320	fair	fair	fair
5	330	fair	fair	fair
5	340	fair	fair	fair
5	350	fair	fair	fair
5	360	fair	fair	fair
5	370	fair	fair	poor
5	380	fair	fair	poor
5	390	fair	fair	poor
5	400	fair	fair	poor
6	50	good	good	fair
6	60	good	good	fair
6	70	good	good	fair
6	80	good	good	fair
6	90	good	good	fair
6	100	good	good	fair
6	110	good	good	fair

Table 44
QoS Levels (Part 18 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
6	120	good	good	fair
6	130	good	good	fair
6	140	good	good	fair
6	150	good	good	fair
6	160	good	good	fair
6	170	good	good	fair
6	180	good	good	fair
6	190	good	good	fair
6	200	good	good	fair
6	210	fair	fair	fair
6	220	fair	fair	fair
6	230	fair	fair	fair
6	240	fair	fair	fair
6	250	fair	fair	fair
6	260	fair	fair	fair
6	270	fair	fair	fair
6	280	fair	fair	fair
6	290	fair	fair	fair
6	300	fair	fair	fair
6	310	fair	fair	fair

Table 44
QoS Levels (Part 19 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
6	320	fair	fair	fair
6	330	fair	fair	fair
6	340	fair	fair	poor
6	350	fair	fair	poor
6	360	fair	fair	poor
6	370	fair	fair	poor
6	380	fair	fair	poor
7	50	good	good	fair
7	60	good	good	fair
7	70	good	good	fair
7	80	good	good	fair
7	90	good	good	fair
7	100	good	good	fair
7	110	good	good	fair
7	120	good	good	fair
7	130	good	good	fair
7	140	good	good	fair
7	150	fair	fair	fair
7	160	fair	fair	fair
7	170	fair	fair	fair

Table 44
QoS Levels (Part 20 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
7	180	fair	fair	fair
7	190	fair	fair	fair
7	200	fair	fair	fair
7	210	fair	fair	fair
7	220	fair	fair	fair
7	230	fair	fair	fair
7	240	fair	fair	fair
7	250	fair	fair	fair
7	260	fair	fair	fair
7	270	fair	fair	fair
7	280	fair	fair	fair
7	290	fair	fair	fair
7	300	fair	fair	fair
7	310	fair	fair	fair
7	320	fair	fair	poor
7	330	fair	fair	poor
7	340	fair	fair	poor
8	50	fair	fair	fair
8	60	fair	fair	fair
8	70	fair	fair	fair

Table 44
QoS Levels (Part 21 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
8	80	fair	fair	fair
8	90	fair	fair	fair
8	100	fair	fair	fair
8	110	fair	fair	fair
8	120	fair	fair	fair
8	130	fair	fair	fair
8	140	fair	fair	fair
8	150	fair	fair	fair
8	160	fair	fair	fair
8	170	fair	fair	fair
8	180	fair	fair	fair
8	190	fair	fair	fair
8	200	fair	fair	fair
8	210	fair	fair	fair
8	220	fair	fair	fair
8	230	fair	fair	fair
8	240	fair	fair	fair
8	250	fair	fair	fair
8	260	fair	fair	fair
8	270	fair	fair	fair

Table 44
QoS Levels (Part 22 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
8	280	fair	fair	fair
8	290	fair	fair	fair
8	300	fair	fair	poor
8	310	fair	fair	poor
8	320	fair	fair	poor
9	50	fair	fair	fair
9	60	fair	fair	fair
9	70	fair	fair	fair
9	80	fair	fair	fair
9	90	fair	fair	fair
9	100	fair	fair	fair
9	110	fair	fair	fair
9	120	fair	fair	fair
9	130	fair	fair	fair
9	140	fair	fair	fair
9	150	fair	fair	fair
9	160	fair	fair	fair
9	170	fair	fair	fair
9	180	fair	fair	fair
9	190	fair	fair	fair

Table 44
QoS Levels (Part 23 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
9	200	fair	fair	fair
9	210	fair	fair	fair
9	220	fair	fair	fair
9	230	fair	fair	fair
9	240	fair	fair	fair
9	250	fair	fair	fair
9	260	fair	fair	fair
9	270	fair	fair	fair
9	280	fair	fair	poor
9	290	fair	fair	poor
9	300	fair	fair	poor
10	50	fair	fair	fair
10	60	fair	fair	fair
10	70	fair	fair	fair
10	80	fair	fair	fair
10	90	fair	fair	fair
10	100	fair	fair	fair
10	110	fair	fair	fair
10	120	fair	fair	fair
10	130	fair	fair	fair

Table 44
QoS Levels (Part 24 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
10	140	fair	fair	fair
10	150	fair	fair	fair
10	160	fair	fair	fair
10	170	fair	fair	fair
10	180	fair	fair	fair
10	190	fair	fair	fair
10	200	fair	fair	fair
10	210	fair	fair	fair
10	220	fair	fair	fair
10	230	fair	fair	fair
10	240	fair	fair	fair
10	250	fair	fair	fair
10	260	fair	fair	fair
10	270	fair	fair	poor
10	280	fair	fair	poor
11	50	fair	fair	fair
11	60	fair	fair	fair
11	70	fair	fair	fair
11	80	fair	fair	fair
10	190	fair	fair	fair

Table 44
QoS Levels (Part 25 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
10	200	fair	fair	fair
10	210	fair	fair	fair
11	90	fair	fair	fair
11	100	fair	fair	fair
11	110	fair	fair	fair
11	120	fair	fair	fair
11	130	fair	fair	fair
11	140	fair	fair	fair
11	150	fair	fair	fair
11	160	fair	fair	fair
11	170	fair	fair	fair
11	180	fair	fair	fair
11	190	fair	fair	fair
11	200	fair	fair	fair
11	210	fair	fair	fair
11	220	fair	fair	fair
11	230	fair	fair	fair
11	240	fair	fair	fair
11	250	fair	fair	fair
11	260	fair	fair	poor

Table 44
QoS Levels (Part 26 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
11	270	fair	fair	poor
12	50	fair	fair	fair
12	60	fair	fair	fair
12	70	fair	fair	fair
12	80	fair	fair	fair
12	90	fair	fair	fair
12	100	fair	fair	fair
12	110	fair	fair	fair
12	120	fair	fair	fair
12	130	fair	fair	fair
12	140	fair	fair	fair
12	150	fair	fair	fair
12	160	fair	fair	fair
12	170	fair	fair	fair
12	180	fair	fair	fair
12	190	fair	fair	fair
12	200	fair	fair	fair
12	210	fair	fair	fair
12	220	fair	fair	fair
12	230	fair	fair	fair

Table 44
QoS Levels (Part 27 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
12	240	fair	fair	poor
12	250	fair	fair	poor
12	260	fair	fair	poor
13	50	fair	fair	fair
13	60	fair	fair	fair
13	70	fair	fair	fair
13	80	fair	fair	fair
13	90	fair	fair	fair
13	100	fair	fair	fair
13	110	fair	fair	fair
13	120	fair	fair	fair
13	130	fair	fair	fair
13	140	fair	fair	fair
13	150	fair	fair	fair
13	160	fair	fair	fair
13	170	fair	fair	fair
13	180	fair	fair	fair
13	190	fair	fair	fair
13	200	fair	fair	fair
13	210	fair	fair	fair

Table 44
QoS Levels (Part 28 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
13	220	fair	fair	fair
13	230	fair	fair	fair
13	240	fair	fair	poor
13	250	fair	fair	poor
14	50	fair	fair	fair
14	60	fair	fair	fair
14	70	fair	fair	fair
14	80	fair	fair	fair
14	90	fair	fair	fair
14	100	fair	fair	fair
14	110	fair	fair	fair
14	120	fair	fair	fair
14	130	fair	fair	fair
14	140	fair	fair	fair
14	150	fair	fair	fair
14	160	fair	fair	fair
14	170	fair	fair	fair
14	180	fair	fair	fair
14	190	fair	fair	fair
14	200	fair	fair	fair

Table 44
QoS Levels (Part 29 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
14	210	fair	fair	fair
14	220	fair	fair	poor
14	230	fair	fair	poor
15	50	fair	fair	fair
15	60	fair	fair	fair
15	70	fair	fair	fair
15	80	fair	fair	fair
15	90	fair	fair	fair
15	100	fair	fair	fair
15	110	fair	fair	fair
15	120	fair	fair	fair
15	130	fair	fair	fair
15	140	fair	fair	fair
15	150	fair	fair	fair
15	160	fair	fair	fair
15	170	fair	fair	fair
15	180	fair	fair	fair
15	190	fair	fair	fair
15	200	fair	fair	poor
15	210	fair	fair	poor

Table 44
QoS Levels (Part 30 of 30)

Packet loss (%)	One-way delay (ms)	QoS level		
		G.729A	G.711A G.711U	G.723
15	220	fair	fair	poor
15	230	fair	fair	poor
16	50	fair	fair	fair
16	60	fair	fair	fair
16	70	fair	fair	fair
16	80	fair	fair	fair
16	90	fair	fair	fair
16	100	fair	fair	fair
16	110	fair	fair	fair
16	120	fair	fair	fair
16	130	fair	fair	fair
16	140	fair	fair	fair
16	150	fair	fair	fair
16	160	fair	fair	fair
16	170	fair	fair	poor
16	180	fair	fair	poor

Index

Meridian 1

Meridian Internet Telephony Gateway (ITG) Trunk 1.0/ Basic Per-Trunk Signaling

Publication number: 553-3001-116
Document release: Standard 2.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.