Meridian 1

Meridian Internet Telephony Gateway (ITG) Line 1.0/IP Telecommuter

Description, Installation and Operation

Document Number: 553-3001-119
Document Release: Standard 2.00
Date: April 2000

Printed in Canada

Revision history

April 2000

Standard 2.00. This is a global document and is up-issued for X11 Release 25.0x. Document changes include removal of: redundant content; references to equipment types except Options 11C, 51C, 61C, and 81C; and references to previous software releases.

June 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 provides information on the Meridian Internet IP Telecommuter and IP Line card products.

This document contains the following sections:

Description describes the IP Telecommuter and IP Line card functional and physical characteristics.

IP Telecommuter Client describes the features and operation of the H.323 desktop terminal, or client, used by IP Telecommuter.

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

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

Administration describes the ITG Line card administration procedures and parameter configuration.

Maintenance describes maintenance and report generating.

Appendix A describes IP Line card cabling for CISPR Class A.

Appendix B describes IP Line card cabling for CISPR Class B.

Appendix C describes IP Line card product integrity.

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

Description

IP Telecommuter provides the communication between the circuit switched telephony network and the H.323 IP Telecommuter clients on a Corporate IP network in the Enterprise environment (see Figure 1 on page 17). The IP Line card Gateway(s) interact with the IP Line card Gatekeeper which controls Client access, registration, and monitoring. Through the IP Line card, calls between H.323 IP Telecommuter clients, and the telephone sets and trunks behind the Meridian 1 in the enterprise network are supported.

In addition, a subset of the Meridian 1 set features, such as Conference, Transfer, Hold and Message Waiting Notification are available to the H.323 IP clients, much like a regular digital set behind the Meridian 1.

Parts of the IP Telecommuter system

The following parts compose the IP Telecommuter system: Terminals (IP Telecommuter Clients), IP Line card Gateways, IP Line card Gatekeepers, the Meridian 1, and MAT.

Terminals

The IP Telecommuter Client is an H.323 application used with the IP Line card.

During the installation of the IP Telecommuter Client, user DN, and Gatekeeper IP address are entered. The DN is used to associate with a port on the IP Line card. An initial password will be assigned by the technician during the process of configuring the IP Line card in MAT. This password should be changed by the end user when using the system for the first time.

The IP Telecommuter Client consists of a PC running Windows 98 with an M9617 USB telephone connected as the primary user interface. The user may then either use the keys on the telephone or the Graphical User Interface (GUI) on the PC to initiate calls and use set features. On a PC running Windows 95/98/Windows NT 4.0 operating system, the IP Telecommuter application may also be used while travelling by plugging a headset into the sound card on the PC and using the GUI for call control.

See the *IP Telecommuter Client* section for a detailed description.

IP Line card Gateways

Gateways in the system contain two interfaces: one interface to the Meridian 1, and the other is an H.323 interface to the IP network. The Gateway provides the necessary conversion for both call signaling and voice stream/packets across the two interfaces. IP Line cards provide the Gateway functionality.

IP Line card Gatekeepers

The Gatekeeper provides endpoint management including registration/unregistration, authentication, address resolution (DN to IP and endpoint to Gateway), and maintaining a list of endpoints currently active on the network. The IP Telecommuter system provides the Gatekeeper functionality in the active leader and backup leader cards.

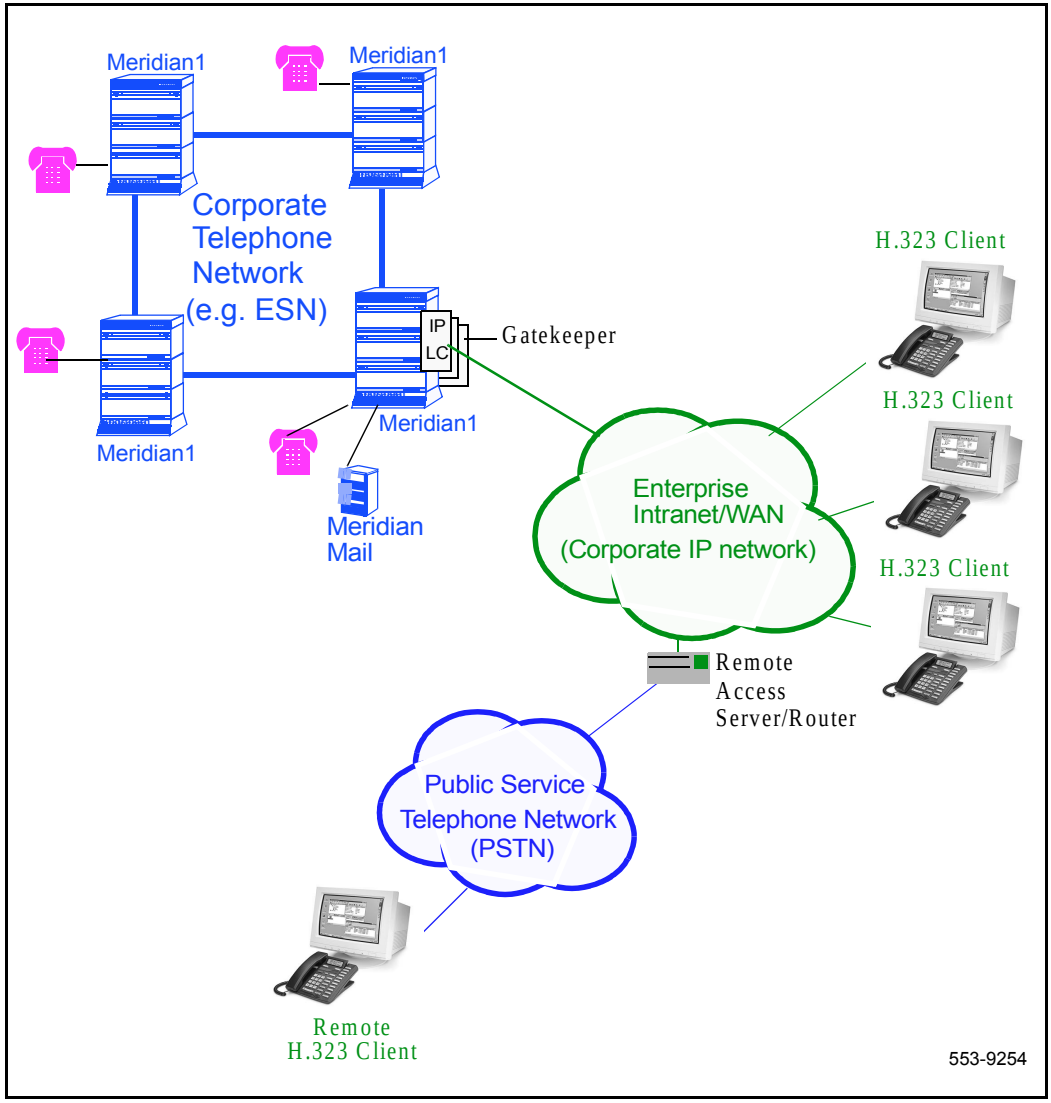
Meridian 1

The Meridian 1 provides the telephony features and call routing in the IP Telecommuter system.

MAT

Meridian Administration Tools (MAT) is used for the installation and configuration of the IP Line card(s).

Figure 1
IP Telecommuter system architecture



Figures 2 through 5 show four possible IP Telecommuter configurations..

Figure 2
Multi-zone, two subnets, and central management

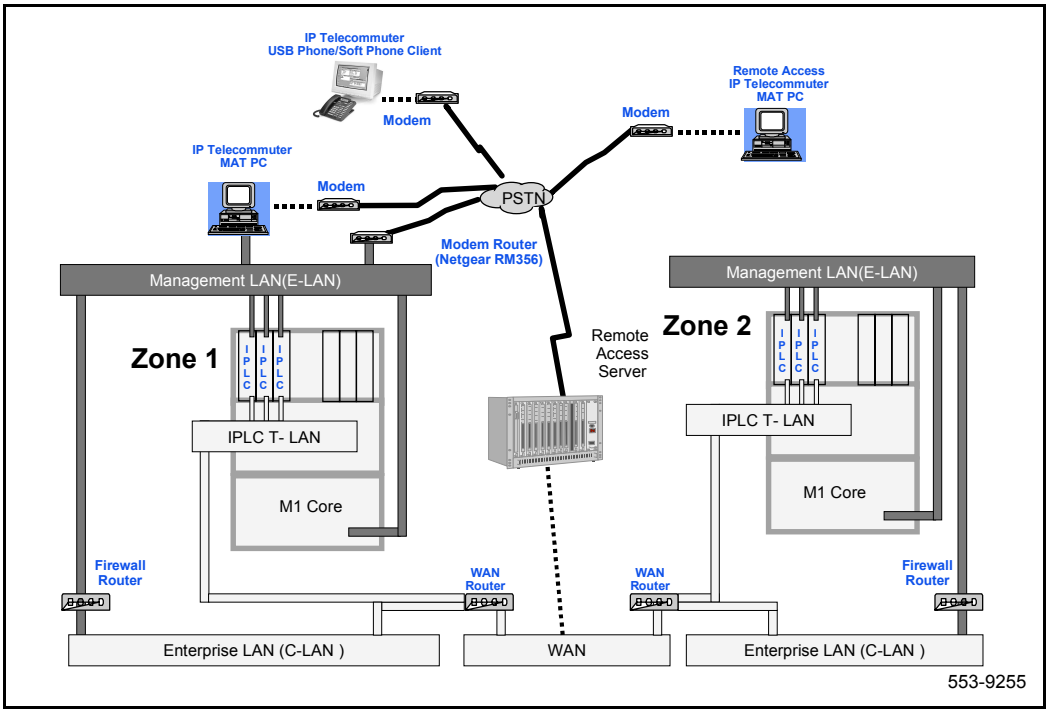


Figure 3
Multi-zone, two subnets, and local management

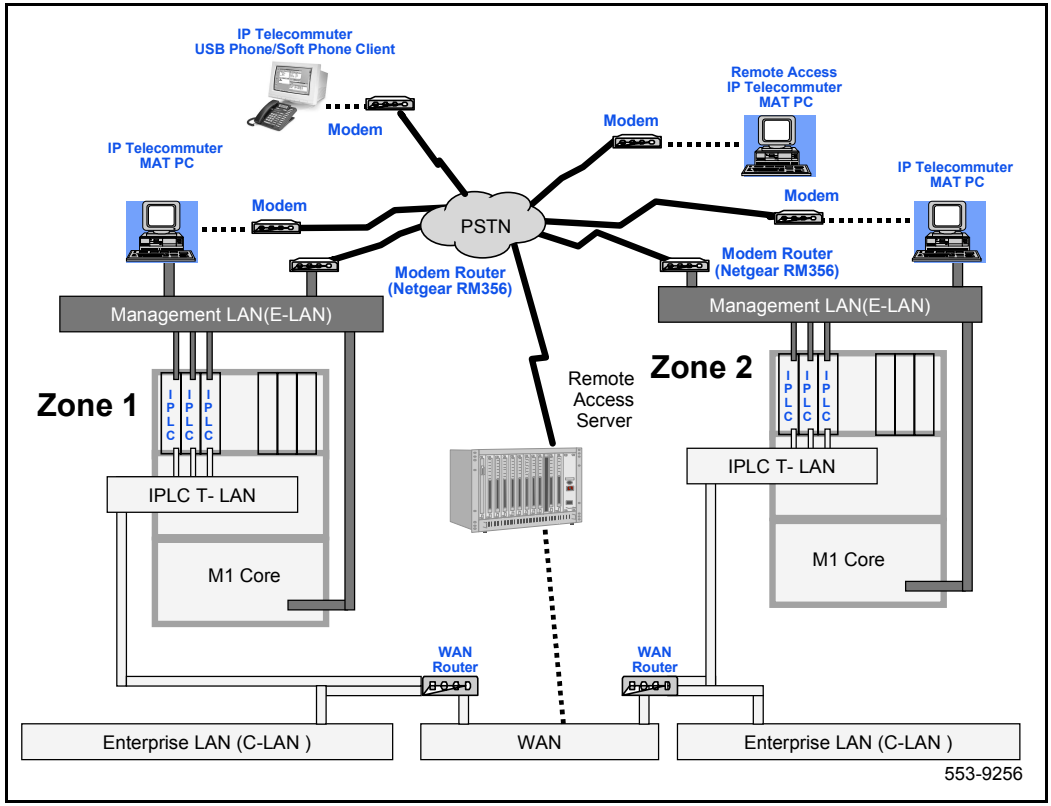


Figure 4
One zone, one subnets, and local management

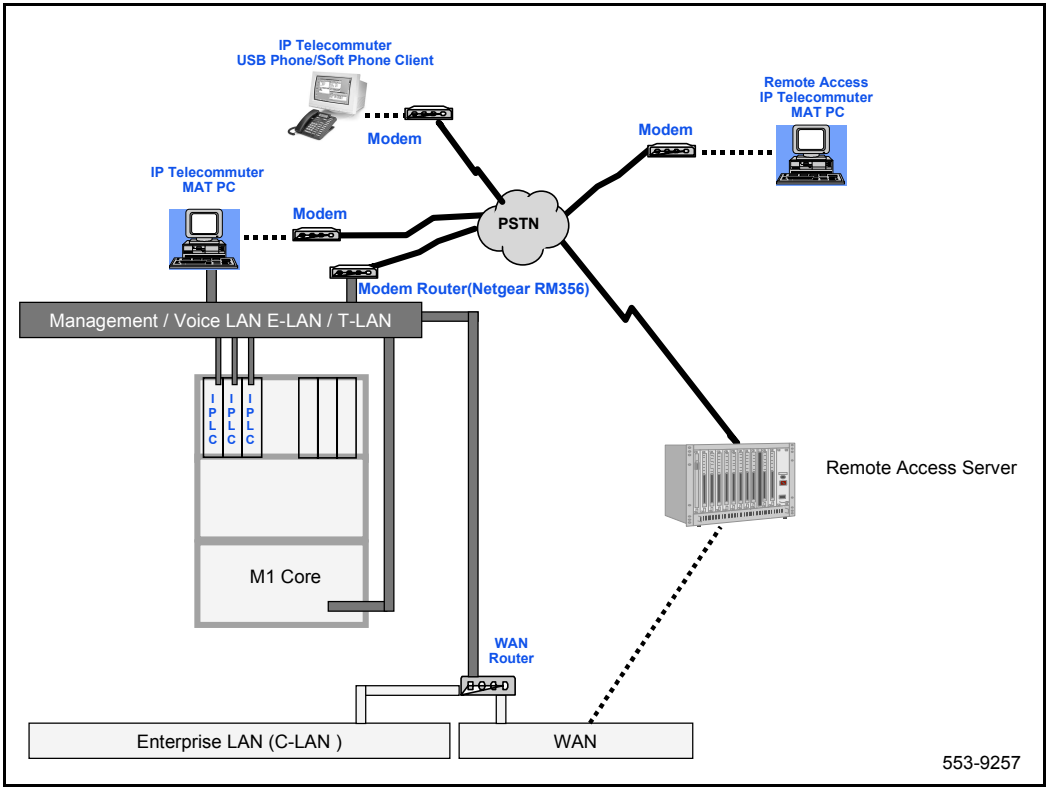
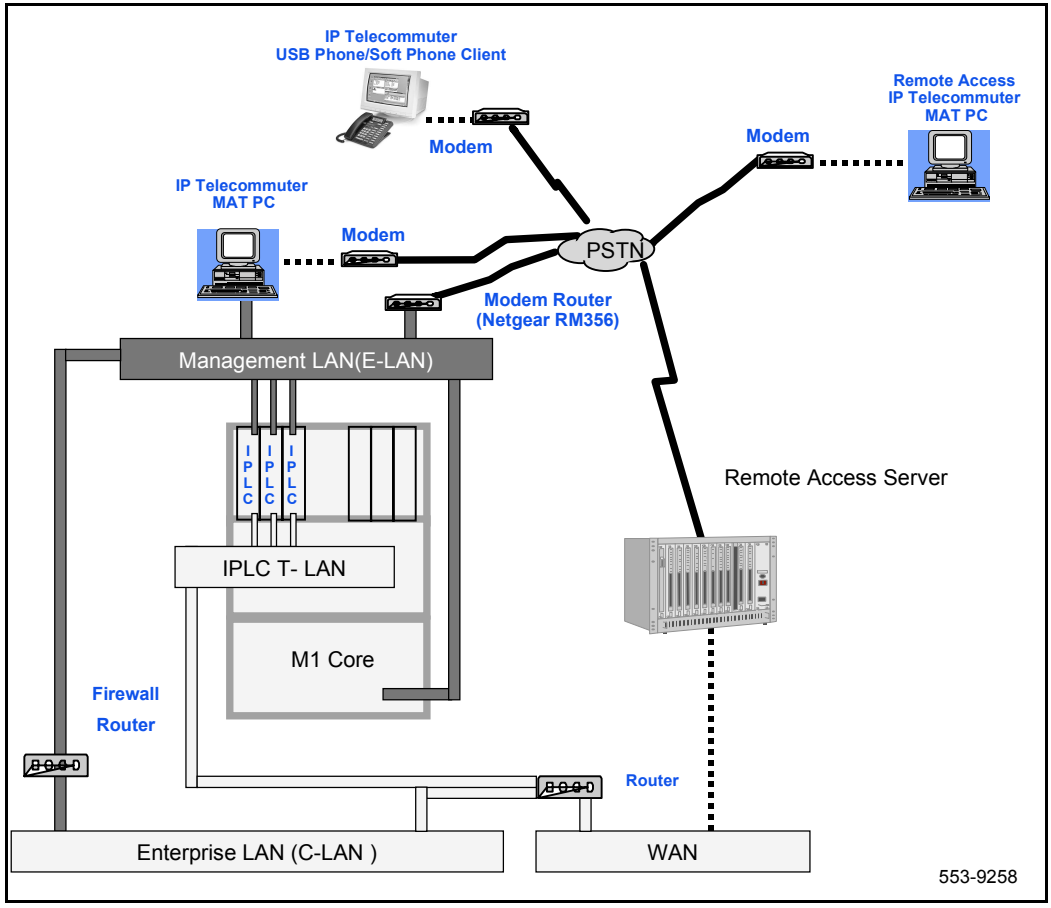


Figure 5
One zone, two subnets, and local management



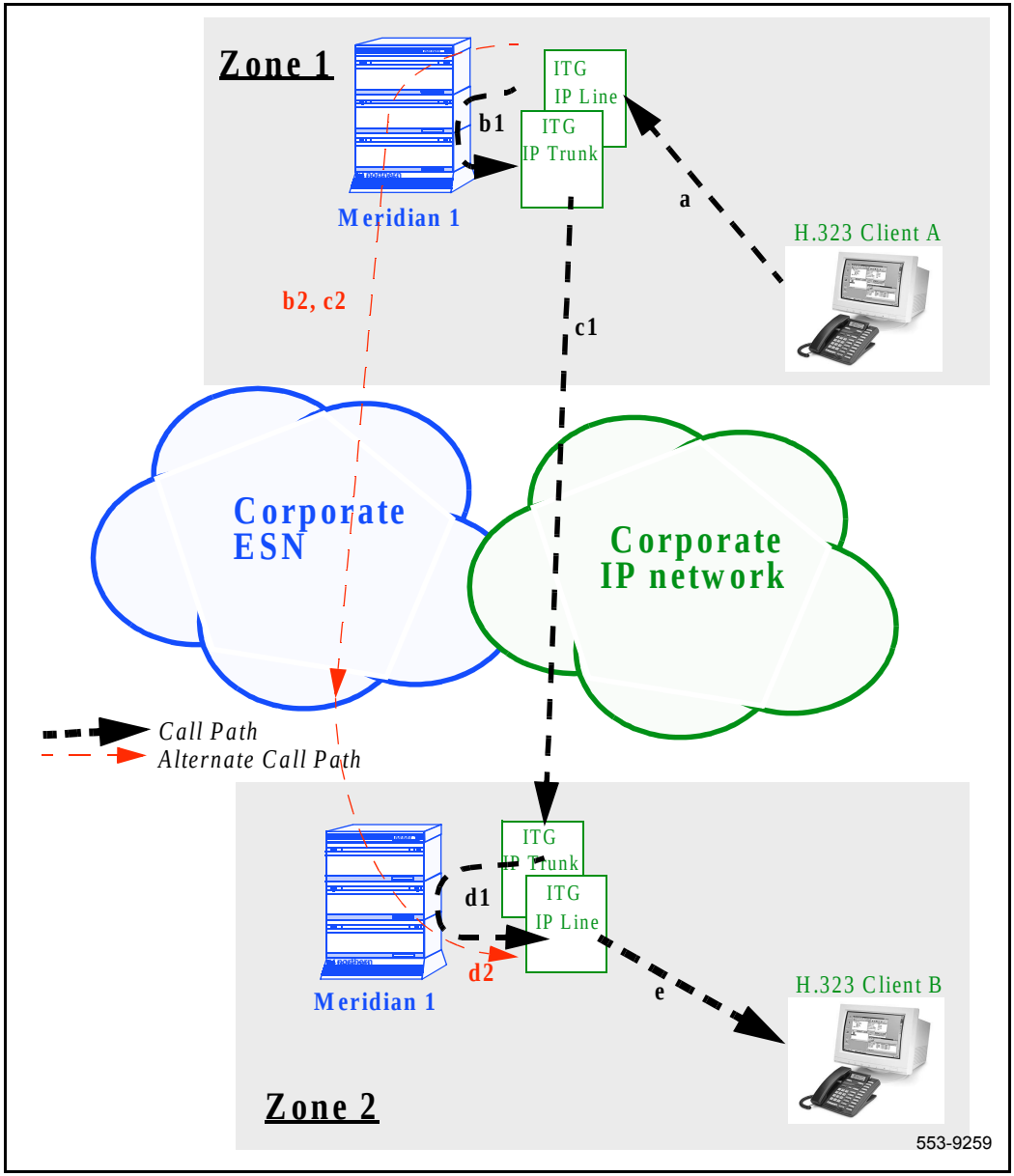
IP Telecommuter multi-zone architecture

In a H.323 network, each Gatekeeper controls one H.323 *zone*; each H.323 zone consists of many H.323 IP clients, and potentially many Gateway cards.

In the IP Telecommuter system, each Meridian 1 system may have multiple H.323 zones. Each customer within a Meridian 1 system can also be partitioned into different zones.

All calls are routed through the Meridian 1 system whether the call is within the same H.323 zone, or across different zones within the same Meridian 1, or across different zones in different Meridian 1 systems. The Meridian 1 system determines the route. As demonstrated in Figure 6, a two zone network, when H.323 client A in zone 1 calls H.323 client B in zone 2, the calls are routed through the Meridian 1 in zone 1 and the Meridian 1 in zone 2. Communication across the two zones have two alternative paths: one via IP trunk (path a -> b1 -> c1 -> d1 -> e), and the other via ESN network (path a -> b2 -> c2 -> d2 -> e).

Figure 6
IP Telecommuter multi-zone architecture



Applicable systems

The IP Telecommuter is available for Meridian 1 options 11C, 51C, 61C, 81 and 81C systems running X11 release 22 or later software.

System requirements

IP Telecommuter requires X11 release 22 or later software. X11 release 22 or later software is required for the Flexible Voice/Data TN feature to support all 24 ports.

IP Telecommuter requires MAT 6.5 or later and the MAT Common Services, Alarm Notification. Alarm Notification is part of the MAT Alarm Management. The IP Telephony Gateway applications is included with MAT Common Services.

Table 1 lists required IP Telecommuter packages:

Table 1
Required packages

Package	Package number
Digital Set Package (DSET)	88
Terminal Package	170
MAT to manage the Meridian 1	164, 242, 243, 296, 315

List of IP Telecommuter components

Tables 2 through 4 list IP Telecommuter components.

Note: MAT 6.5 or later, including the Common Services, Alarm Management, and IP Telephony Gateway applications, is a pre-requisite and must be ordered separately.

Table 2
List of IP Telecommuter components for CISPR Class A/North America orderable through the Meridian 1 Price Book

Component	Code
IP Telecommuter System Package (NT8R16BB IP Line card with Security Device and pre-installed software that supports 24 configured users, required cables, Liberation CTI Headset, IP Telecommuter Client package (24 quantity), NTP)	NTZC65AA A0806188
Spare Meridian Integrated IP Line card (no Security Device included), CISPR Class A	NT8R17AC A0801187
Spare Client CD	A0747149
IP Telecommuter PC card (optional)	NTZC19AA A0774189
Meridian Integrated IP Telephony Gateway IP Telecommuter NTP	P0905051
Meridian Integrated IP Telephony Gateway IP Telecommuter NTP CD	N8R70AA A0774197
Cables	
I/O Panel E-LAN, T-LAN and Serial Port Adaptor cable	NTMF94DA A0782283
Faceplate Maintenance Port cable	NTAG81CA A0655007
Maintenance Extender cable	NTAG81BA

Table 3
Other IP Telecommuter components orderable in North America

Component	Code
Liberation CTI headsets (ordered through Nortel Networks' Meridian Business Sets catalog).	NTA149BN A0757154
M9617 USB Telephone sets for use with IP Telecommuter (ordered through Nortel's Consumer/Business Telephone catalog).	NT2N49AAAA/A0774004 Chameleon Grey NT2N49AAAB/A0774005 Black

Table 4
List of IP Telecommuter components for CISPR Class B orderable through the European Meridian 1 Price Book

Component	Code
European IP Telecommuter Systems Package (NT8R16BB IP Line card with Security Device with pre-installed software that supports 24 configured users, required cables, Liberation CTI Headset, IP Telecommuter Client package (24 quantity), NTP)	NTZC65AA A0806188
Spare Meridian Integrated IP Line card (no Security Device included), CISPR Class B	NT8R17AC A0801187
Spare Client CD	A0747149
Liberation CTI headsets.	NTA149BN A0757154
M9617 USB Telephone sets for use with IP Telecommuter. In Europe, you can only order the black USB set. In Europe you cannot use the analog functionality of the USB set.	NT2N49AAAB/A0774005 Black
IP Telecommuter PC card (optional)	NTZC19AA A0774189

Table 4
List of IP Telecommuter components for CISPR Class B orderable through the European Meridian 1 Price Book

Component	Code
Meridian Integrated IP Telephony Gateway IP Telecommuter NTP	P0905051
Meridian Integrated IP Telephony Gateway IP Telecommuter NTP CD	NT8R70AA A0774197
IP Telecommuter User Guide?	P0887563
Cables	
E-LAN, T-LAN, and RS232 Serial Maintenance cable	NTMF94DA
Faceplate Maintenance Port cable	NTAG81CA A0655007
Maintenance Extender cable	NTAG81BA
Netgear RM356 Modem Router	Ordered through consumer electronics distribution channels.

IP Line card functional description

Card Roles

The three major card roles are:

- active leader: performs IP address assignment, interfaces with MAT, and performs Gatekeeper and Gateway functions.
- backup leader: acts as a Gateway that monitors the heartbeat of active leader, and will take over the active leader functions if the active leader fails.
- followers: function as Gateways only.

Active leaders and backup leaders provide IP addresses to the followers, run the Gatekeeper software, and function as Gateways.

Gatekeeper role

The Gatekeeper provides Client and Gateway management including registration/unregistration, authentication, address resolution (DN to IP and endpoint to gateway), and maintaining a list of Clients currently active on the network. The Gatekeeper functionality is provided by the active leader card and the backup leader card.

The Gatekeeper is the H.323 element which controls address translation, admissions control, call authorization, bandwidth control and management, call control signaling, call management, and zone management.

Currently the IP Line card Gatekeeper supports the following H.323 Gatekeeper functions:

- Registration/Unregistration
- address translation
- call authorization
- call management

The active leader IP Line card performs the Gatekeeper function for a given IP Telecommuter node. The backup leader will assume the Gatekeeper role if the active leader card goes out of service.

In a H.323 network, each Gatekeeper controls one H.323 zone; each H.323 zone consists of many H.323 IP clients, and many Gateway cards.

In the IP Telecommuter system, each Meridian 1 system may have multiple H.323 zones. Each customer within a Meridian 1 system can also be partitioned into different zones.

The IP Telecommuter Client is the H.323 desktop application that is used in the IP Telecommuter product. See the *IP Telecommuter Client* section for detailed information.

Discovery and registration

A Gatekeeper Discovery and Registration process occurs, where the IP Telecommuter Clients and the IP Line Gateway cards must register with the designated IP Line Gatekeeper card. Registration provides a means to map DNs to IP addresses between IP Telecommuter clients and Gateways dynamically (instead of statically via a configuration file).

Registration allows the Gatekeeper to authenticate Clients and Gateways to provide security (i.e., that those accessing the network are who they claim to be). An encrypted block provides the authentication used in registration and admission messages. Each client and the gatekeeper separately know the password used in the key encryption.

During the Client registration process, the Gatekeeper obtains the DN, password, and the associated IP address from the registering IP client, authenticates the client, and populates the client address translation database with entries of these active IP clients.

During IP Line Gateway card registration, the IP Line Gatekeeper card obtains the lists of DNs and the Gateway IP address from the registering IP Line Gateway card. Similarly, the Gatekeeper populates the active Gateway entries with its IP address and the list of DNs it serves in the Gateway address table.

These address translation databases are then used by the Gatekeeper to perform address translation whenever a call is made from the Meridian 1 to an IP client, from an IP client to the Meridian 1, or from an IP client to an IP client.

The value of *Time To Live* that is specified for the Gatekeeper provides the duration of the Registration.

Admission

Admission occurs when a client or Gateway attempts to make a call. The Gatekeeper authenticates the Clients and Gateways involved. Admission occurs between both the originating and terminating sides and the Gatekeeper per H.323. The Gatekeeper maps between the originating and terminating sides of the call (address translation). The mapping is a simple dynamic mapping between the Gateway and client.

The Gatekeeper tracks the active calls for logging and debugging purposes.

Unregistration and disengage

The Gatekeeper also allows the opposing actions to registration and admission, in the form of unregistration and disengage. These allow Clients and Gateways to inform the Gatekeeper when they are finished using services.

Registration renewal: Time To Live

As the Gatekeeper confirms the Client and Gateway registration in the initial registration request, the Gatekeeper specifies a *Time To Live* message for the Client and Gateway. This is a deadline by which the Clients and Gateways must re-register in order to maintain registration. The purpose of *Time To Live* is to allow Gatekeepers, Clients, and Gateways to know whether they are still alive.

This is needed because an endpoint can become disconnected from the H.323 network without first unregistering with the Gatekeeper, or in case the Gatekeeper goes out of service. The Gatekeeper unregisters an endpoint that misses two consecutive registration renewals. If a call is ongoing when the Gatekeeper unregisters an endpoint, the call may be dropped.

The Time To Live value ranges from 10 to 60 minutes (configurable through the MAT IP Line application). The Clients and Gateways are required to renew the registration with *keepAlive* indications within the specified time.

Gatekeeper Fallover

Both the active leader and backup leader run the Gatekeeper software. When the backup leader takes over for the active leader upon failure of the active leader heartbeat, the Gatekeeper on the backup leader takes over for the Gatekeeper on the active leader.

Clients must re-register with the new gatekeeper in the case of such fallover.

IP Address Distribution

Bootp protocol provides IP address provisioning. The leader card runs a bootp server, while followers run Bootp clients.

MAT transmits IP address information to the active leader card. The backup leader card receives its Bootp file from the active leader card.

The backup leader card can detect when the active leader fails. When this occurs, the backup leader becomes the active leader and takes over its functions.

Administration and Management

The Gatekeeper requires one file, the Gatekeeper Table file, for management. This is downloaded via the MAT "ITG M1 IP Lines" application to the card. The file resides in /C:/TABLE/GKTABLE.1 on the card’s file system.

Gatekeeper Table file format

Figure 7 shows the format of the Gatekeeper Table file:

Operational Measurements (OM)

The Gatekeeper collects and stores the following Operational Measurement (OM) parameters in a Gatekeeper OM file:

- GRQ (Discovery Request) attempted
- GCF (Discovery Confirm) attempted
- LRQ (Location Request) attempted
- BRQ (Bandwidth Request) attempted
- RRQ (Registration Request) attempted
- RCF (Registration Confirm) attempted

Figure 7
Gatekeeper Table file format

```
#this is the gatekeeper config file
gkonoff,1
clientttl,120
gatewayttl,120
pwd,tn,5000,password,1
pwd,tn,5001,password,1
[...]
pwd,tn,5017,password,1
```

- URQ (Unregister) timeout
- URQ (Unregistration Request) attempted
- ARQ (Admission Request) attempted
- ACF (Admission Confirm) completed
- DRQ (Disengage Request) attempted
- Authentication failures

These statistics are updated hourly and can be viewed within MAT, where they are exported to a Microsoft Excel spreadsheet.

Non-Standard Messaging

The IP Line card uses non-standard messaging for:

- password changes
- login/logoff of Gateways and Clients
- Message Waiting Indication

Password Changing and Authentication

The Gatekeeper allows Clients to change their password by sending an encrypted message which includes the new password, encrypted with the old password. The Gatekeeper is then able to authenticate the new password by decrypting the message with the old password.

Basic call setup

Once the IP Client and the Gateway cards have registered with the designated Gatekeeper on the network as described in “Discovery and registration” on page 29, the IP Client can start making and receiving calls through the corresponding Gateway.

IP Line card physical description

The IP Line cards plug into the IPE shelf. Each IP Line card supports 24 configurable TNs. Each IP Line card takes up 2 card slots. EMC limits the amount the number of IP Line cards that can be installed in the IPE module, or Option 11C system. See “ITG I/O cabling for EMC compliance” on page 43.

Interfaces

Each IP Line card has one 10BaseT ethernet interface connecting the IP Line card to the private LAN for management. One 10/100BaseT ethernet interface from the DSP daughterboard connects the IP Line card to the IP based network. The interface provides or voice transmission and communications with the IP client and Gatekeeper (See Figure 3).

Inter-IP Line card communications for OA&M related information route through the 10BaseT interface on the ITG host module. Communications for voice and H.323 related information route through the 100/10BaseT interface on the DSP daughterboard.

The IP Line card has a faceplate serial port connection on the faceplate and on the I/O backplane. You can only connect a serial device through one port at a time. A TTY can be connected via an NTAG81CA cable and the ITG shell command line interface can be accessed.

Physical assembly

Figure 8 shows the how the PCI interconnect board connects the ITG motherboard and DSP daughterboard. Figure 9 shows the IP Line card faceplate. The card consists of a motherboard and a DSP daughterboard connected via a PCI interconnect board. The DSP daughterboard consists of DSP sections. Each section connects to 128 Kwords of high speed SRAM.

The core ITG processor is an Intel x86 processor. The Intel 82420 PCI chipset provides the system interface. The IP Line card has 16MB of DRAM memory, 4MB of file storage flash memory, 4MB of application flash memory, and 512 Kbytes of BIOS flash memory. The BIOS loads the application memory.

The IP Line card has no switches or jumpers.

.

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 8
IP Line card assembly

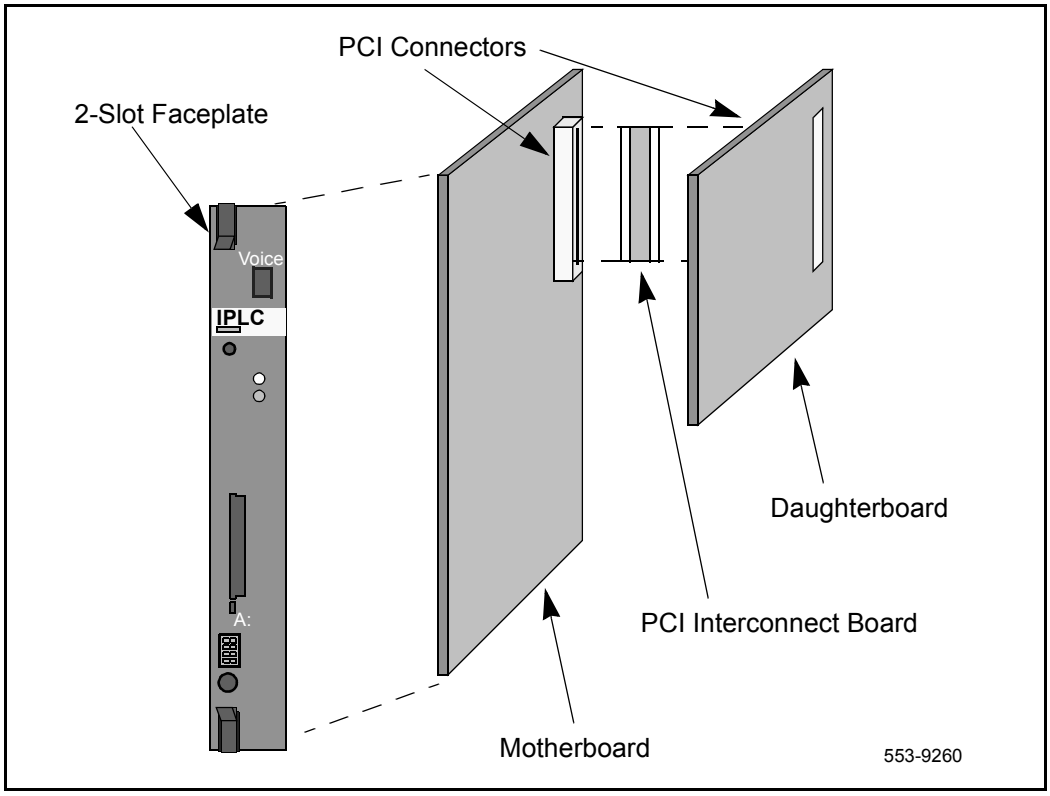
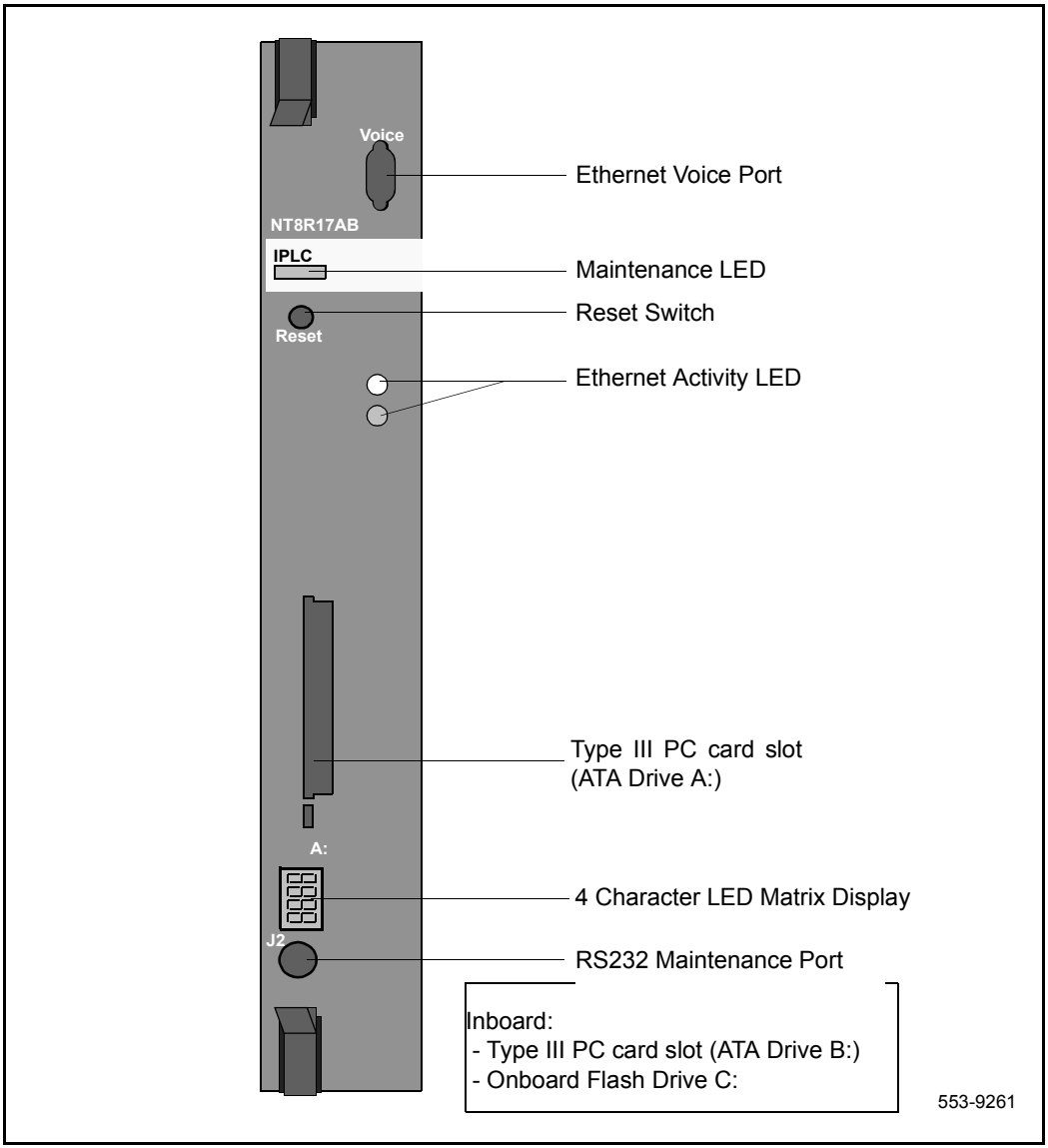


Figure 9 shows a faceplate view of the IP Line card:

Figure 9
IP Line card faceplate



PC cards

The IP Line card has two PC card slots. One PC card slot is on the faceplate (drive A:). One card slot is on the board (drive B:). The drives support PC based hard disks (ATA interface) or high-capacity PC flash memory cards for mass storage.

Security Device

A Security Device will come pre-installed on the IP Line card motherboard for new system orders (refer to "List of IP Telecommuter components" on page 25). If ordered as a spare part, the IP Line card (NT8R17AB) does not include a Security Device. If ordered as part of a package, the Security Device is included. 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.

When the Security Device is installed, the Nortel logo faces outward.

Figure 10 shows the Security Device. Figure 11 shows the location of the Security Device on the IP Line card motherboard:

Figure 10
IP Line card Security Device

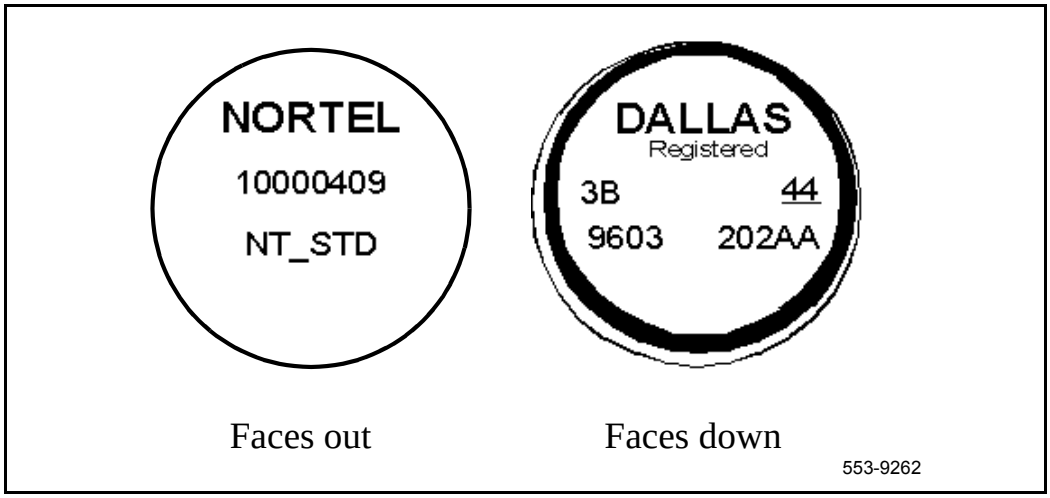
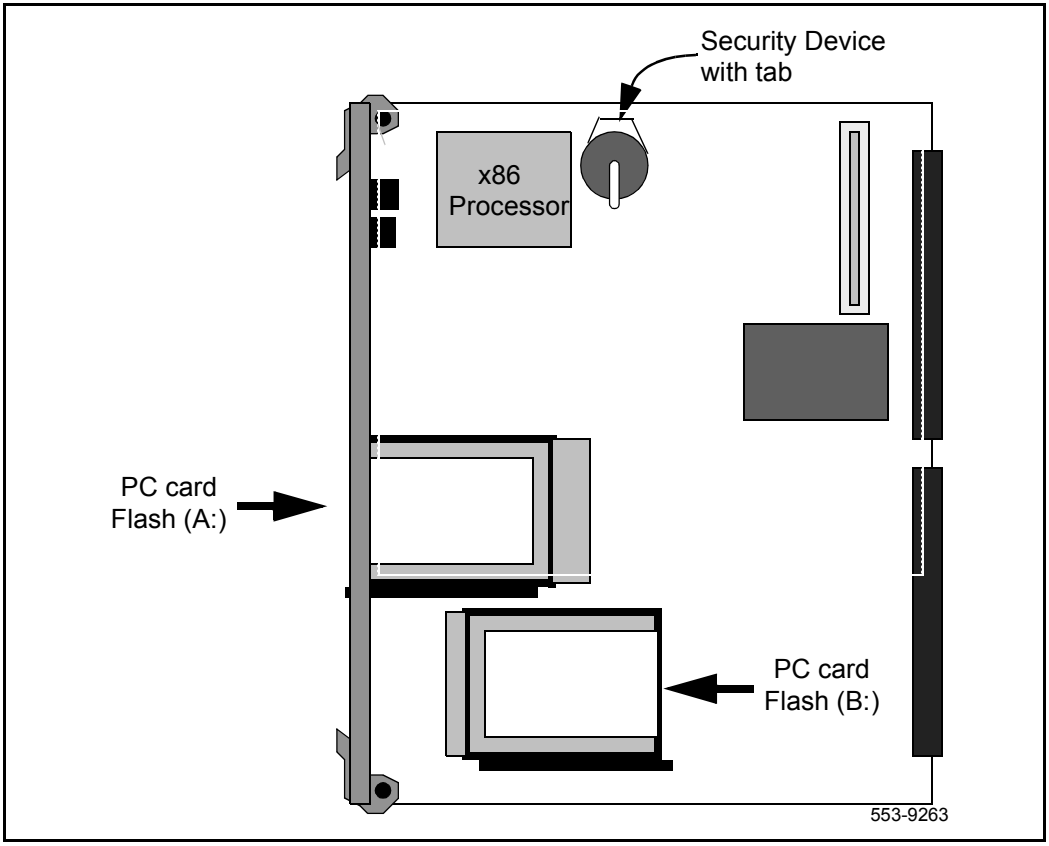


Figure 11
IP Line card Security Device location - beneath the daughterboard



OA&M

The IP Telecommuter OA&M access is provided through three different means: the MAT "ITG M1 IP Lines" application, the ITG shell command-line interface, and existing Meridian 1 system management interfaces.

MAT "ITG M1 IP Lines" application

A MAT PC with the MAT "ITG M1 IP Lines" application is used to perform IP Line card maintenance and administration functions.

Information that is configured on the MAT PC and downloaded to the Gatekeeper function on the active leader and backup leader cards consists of:

- Enable Gatekeeper Function on the Leader and Backup Leader card by assigning an internal Gatekeeper (only an internal Gatekeeper, not external, is supported).
- Endpoint Registration Time To Live for IP client.
- Endpoint Registration Time To Live for Gateway.
- Endpoint password table, including entries for each endpoint alias and its corresponding password. (For Gateway, the card TN is used as the endpoint alias, and for IP client, the DN is used as the endpoint alias).

Information that is downloaded to each IP Line card (i.e. the Gateway), including both leader and backup leader if its ports are intended to be used for handling calls consists of:

- Gatekeeper IP address. (In the integrated Gatekeeper, the Gatekeeper IP address for both the primary and backup gatekeepers is default to be the Node IP that is shared between the leader and backup cards).
- List of DNs associated with each of the 24 ports (or less) on the IP Line card (This must correspond to the overlay 11 configuration. This can be datafilled by the craftperson or preferably obtained from overlay 11 configuration based on the IP Line card port TN).

The technician performs the following functions through the MAT PC related to the Gatekeeper and its data:

- Upload Gatekeeper properties including password table
- Open Gatekeeper Call Information (uploads the list of current active calls, and calls in progress on the Gatekeeper.)

- Open gatekeeper Endpoint Information (uploads the list of all registered endpoint and its associated information.)
- Open Gatekeeper Log File
- Open Gatekeeper Trace File
- Open Gatekeeper OM (Operational Measurement) File

Although the Gatekeeper function resides on the active leader and backup leader cards, the Gatekeeper Log, Trace and OM files are maintained separately from those of the gateway's.

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 IP Line 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.

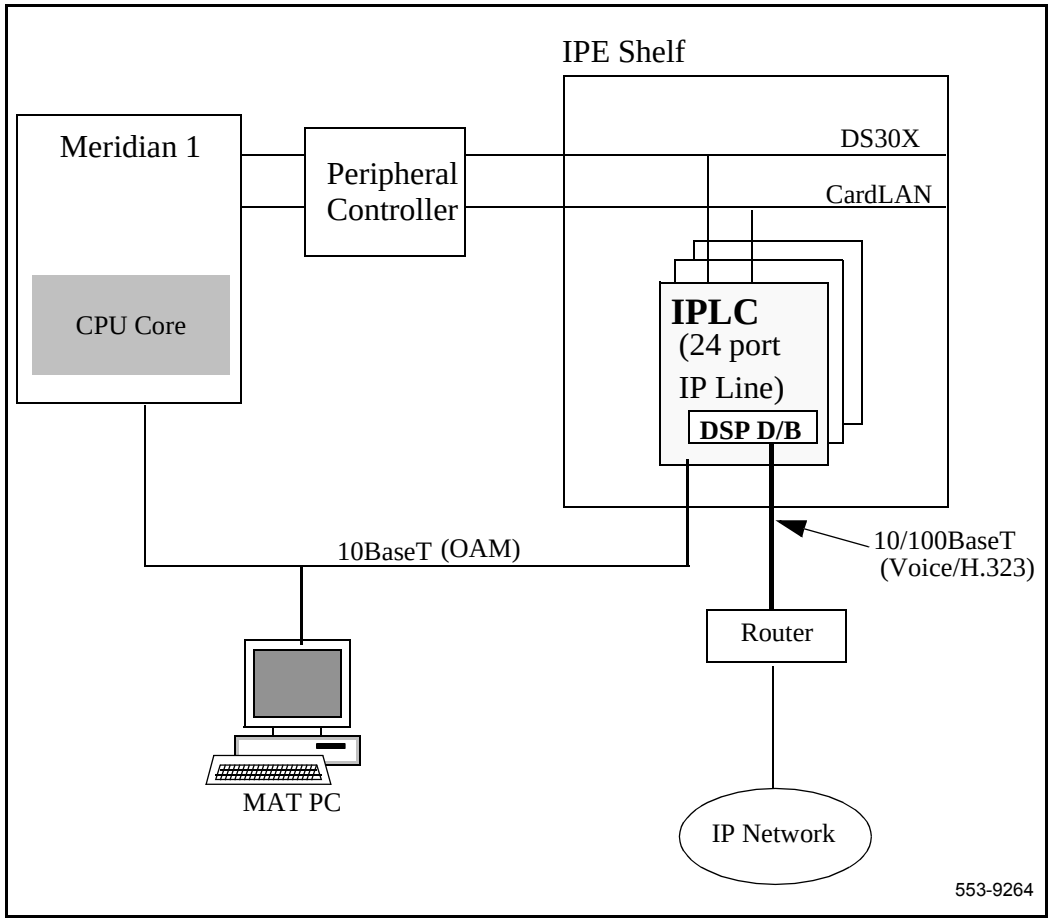
Once connected via Telnet or RS-232 cable, the ITG shell command-line interface is available. The ITG shell is used initially to program the IP address of the Leader 0 IP Line card during ITG node installation. Also, certain ITG administration, maintenance, and file transfer commands are available.

A list of ITG shell commands and Meridian 1 system commands is described in "Maintenance" on page 207.

Meridian 1 system management commands.

The IP Line card uses a subset of the existing Meridian 1 system management commands and diagnostic messages used for the Digital Line card (XDLC). You must configure the IP Line using the appropriate Meridian 1 service change overlay, as described in the *Installation and configuration* section. The IP Line card will appear to the Meridian 1 as an XDLC line card, and use the same card LAN ID as an XDLC card (see Figure 12).

Figure 12
IP Line card connectivity



IP Telecommuter Engineering Guidelines

EMC compliance

EMC compliance requirements depend on the regulations in effect for the country where the Meridian 1 system is located.

ITG Line card and Trunk card provisioning rules for EMC compliance

The ITG provisioning rules for EMC compliance cover all combinations of trunk card, line card, and Class A/Class B types of cards.

Meridian 1 Large Systems

There are no EMC provisioning restrictions in Meridian 1 Large Systems on ITG Line cards and Trunk cards for either CISPR Class A or CISPR Class B.

Meridian 1 Option 11C

For CISPR Class A compliance, you can provision a combined maximum of four IP Line cards or Trunk cards of any version per Option 11C system regardless of the number of cabinets.

For CISPR Class B compliance, you can provision a combined maximum of two NT8R17AB IP Line cards or NTCW80CA Trunk cards per Option 11C system regardless of the number of cabinets.

Check product bulletins for the latest EMC provisioning rules.

ITG I/O cabling for EMC compliance

The ITG card requires two 10BaseT Ethernet cables to connect to the E-LAN and T-LAN. In addition, a serial cable is required to connect to the faceplate for maintenance purposes.

NT8R17AB IP Line card cable description

The NT8R17AC card uses the NTMF94DA cable to break out the signals from the I/O connector on large systems and Option 11 to the ethernet management port (E-Lan connection) ethernet voice port (T-Lan connection) and one maintenance RS232 port brought out on a 9-way D-type connection. The required cable is:

- one NTMF94DA shielded backplane to RJ45 and D-subminiature communications port cable.
- one NTAG81CA Maintenance cable from the RS-232 port on the ITG card faceplate to a TTY.

It is very important to use the mounting screw provided on the top of the 25-pair amphenol connector to secure the NTMF94DA cable to the Meridian 1.

The NTMF94DA cable provides a shielded RJ45 to RJ45 coupler at the end of both its E-LAN and T-LAN interfaces. Both of the RJ45 ends of the cables are clearly labelled as to which is the T-LAN and which is the E_LAN. These provide the connection point to the customer's E-LAN and T-LAN equipment. You must use Shielded Cat. 5 cable for connection from this point to the customer's hub or router.

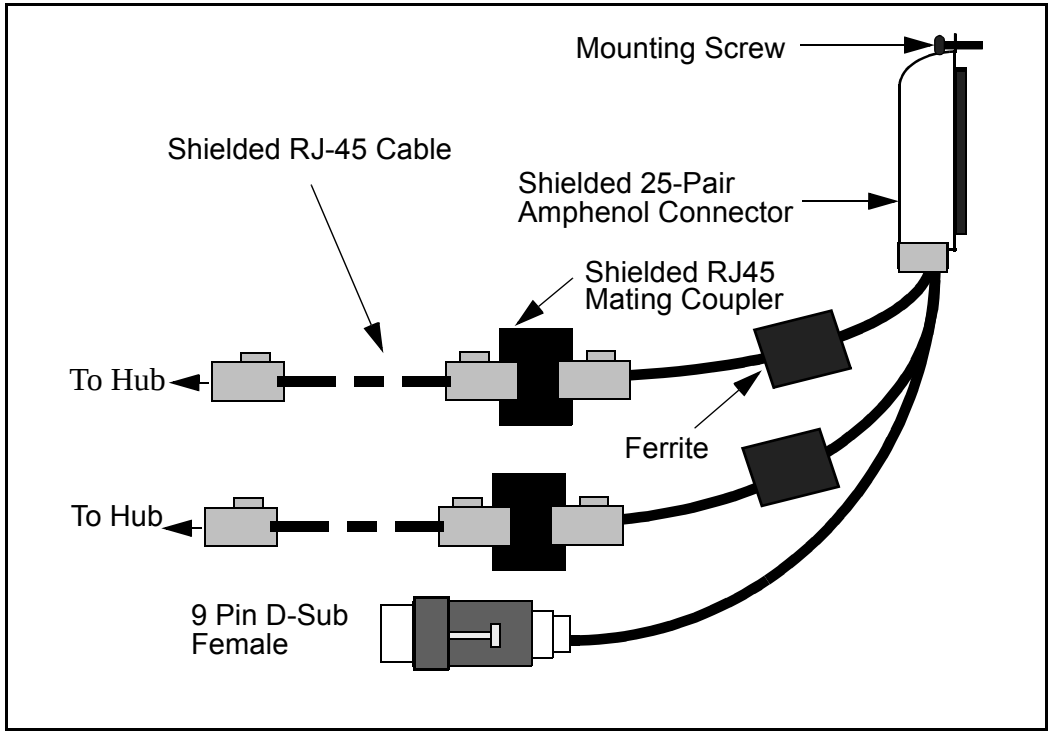
Note: Use standard cable ties to bundle all LAN cables together as they route out of the system.

CAUTION

The serial ports presented at the faceplate and at the backplane are identical. Do not connect to both access points simultaneously. This will result in incorrect and un-predictable operation of the ITG Assembly.

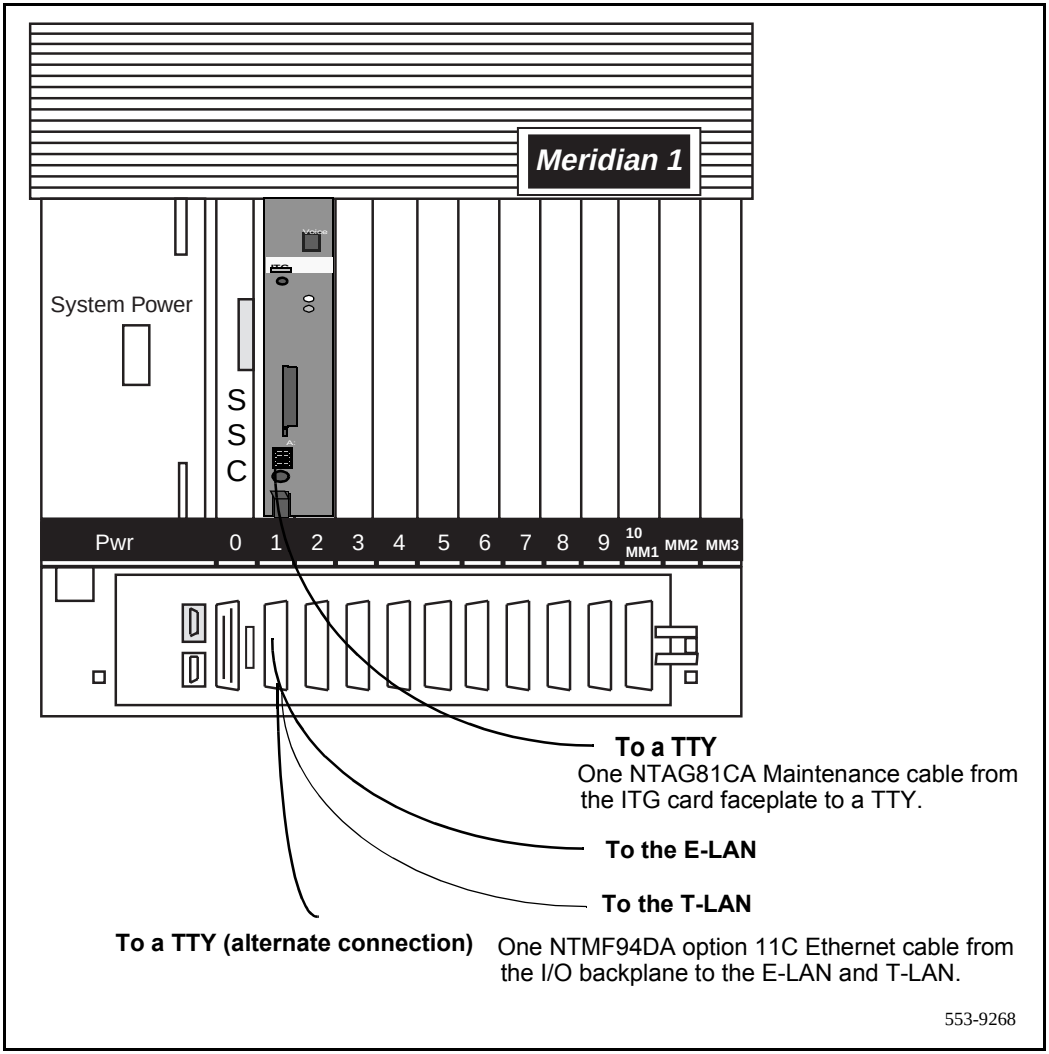
Note: Refer to *Appendix A and B* for more details on cables.

Figure 13
NTMF94DA management port, voice port and serial I/O cable (large system



Note: Refer to "I/O, maintenance and extender cable description" on page 247 for more details on cables.

Figure 14
I/O cabling for NT8R17AB IP Line card - in Meridian 1 Option 11C



Shielded Category 5 cable for external IP Line card LAN connections

You must use Shielded Cat 5 cable only to connect from the Meridian 1 I/O backplane (Option 11C) or I/O panel (Large Systems) to the customer's hub or router. Ground the cable shields at one end only - either at the Meridian 1 I/O panel connector or at the hub, but not at both ends.

Use the appropriate grounded or non-grounded RJ-45 coupler provided with the I/O cable assembly to ground the shield or isolate the shield at the Meridian 1 I/O panel.

Refer to "Prevent ground loops on connection to external customer LAN equipment" on page 250 for information on how to conduct a test for ground loops.

NTMF94DA cable pin description

Table 1 describes the NTMF94DA cable pins.

Table 1
NTMF94DA cable connections

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-21	BSOUTB-	P2-2	RED
P1-22	BDTRB-	P2-4	GREEN
	SGRND	P2-5	BROWN
P1-45	BSINB-	P2-3	BLUE
P1-46	BDCDB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RXDB+	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

Network engineering overview

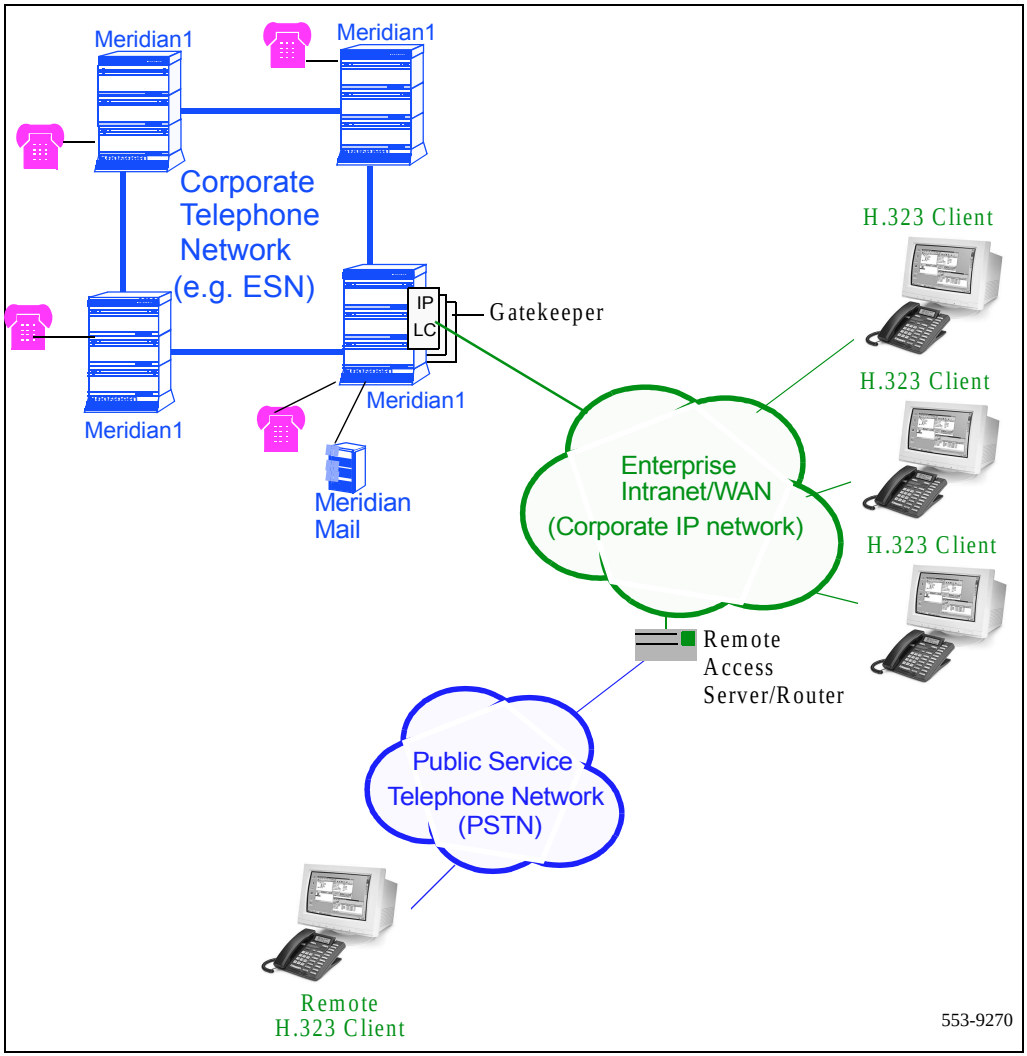
Traditionally Meridian 1 networks rely on voice services such as LEC and IXC private lines. With ITG technology, the Meridian 1 can now choose a new kind of delivery mechanism, one that uses packet-switching over a data network, specifically a corporate intranet. The role of the IP Line Card in this regard is essentially to convert steady data stream digital voice into fixed-length IP packets, and vice versa.

When a corporate data network is used to deliver voice traffic, it introduces impairments, primarily delay and packet loss, at levels that are higher than those delivered by voice networks. Delay between a speaker and listener changes the dynamics and reduces the efficiency of conversations, whereas delay variation and packet loss introduce glitches in the conversation. Simply connecting IP Line card nodes to the corporate intranet without preliminary capacity and performance assessment may result in unacceptable degradation in the voice service; thus proper design procedures and principles must be considered.

A simplified network block diagram showing the potential ITG Telecommuter network is presented in the following Figure 15.

Note that when H.323 Clients are connected to the intranet, they will most likely reach a subnet first, which will be the destination reference point for any packet delay or loss measurement.

Figure 15
M1 IP Telecommuter Network

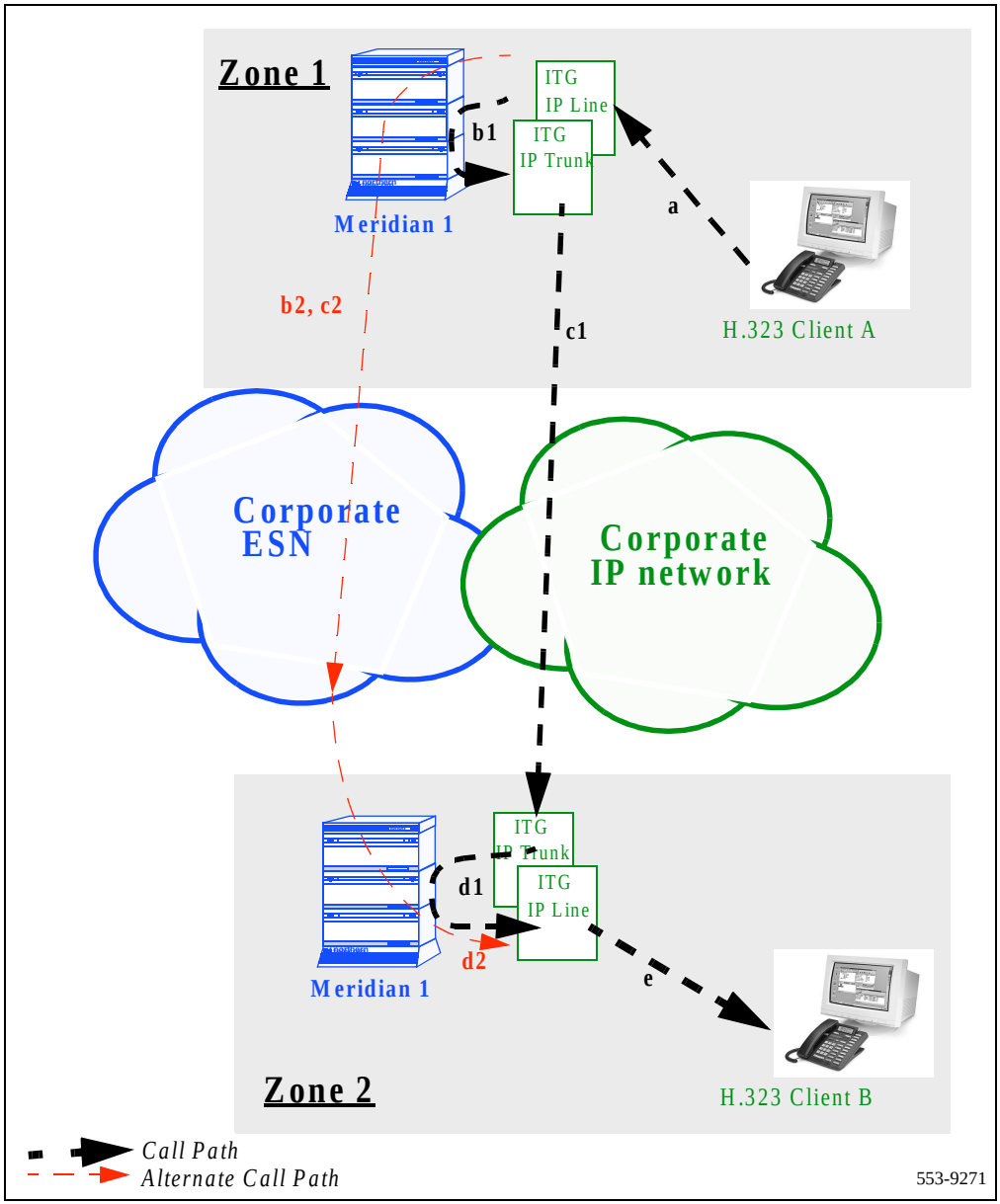


A good design of the IP telephony network must begin with an understanding of traffic, and the underlying network that will carry the traffic. There are three preliminary steps that the technician must undertake.

- Forecast IP Telecommuter traffic. The technician must estimate the amount of traffic that the Meridian 1 system will process via the IP telephony network. This will place a traffic load on the LAN to which the Meridian 1 and its IP Line Cards are connected.
- Assess WAN link resources. If calls from H.323 Clients traverse through the corporate intranet, sufficient WAN resources must be engineered to assure that adequate support is provided to voice services. If calls are from a PSTN without going through the corporate intranet, they will have capacity impact on the T-LAN only.
- Measuring existing intranet's QoS. The technician must estimate the quality of voice service the corporate intranet can deliver. Description on how to measure prevailing delay and error characteristics of an intranet will be presented.

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

Figure 16
M1 IP Telecommuter Gateway Multi-zone Architecture



Setting up a system with separate subnets for voice and management

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

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

- to optimize Voice over IP performance on the Telephony LAN (T-LAN) segment by segregating it from Embedded LAN (E-LAN) traffic and connecting the T-LAN as close as possible to the WAN router,
- to make the amount of traffic on the T-LAN more predictable for QoS engineering,
- to optimize E-LAN performance, e.g., for Symposium Call Center Server (SCCS) and Call Pilot functional signaling, by segregating the E-LAN from ITG T-LAN VoIP traffic,
- to enhance network access security by allowing the modem router to be placed on the E-LAN, which can be isolated from the customer's enterprise network (C-LAN) or have access to/from the C-LAN only through a fire-wall router.

Note: When using separate subnets as recommended the Network Activity LEDs provide valuable maintenance information for the Ethernet voice interface. The single subnet configuration eliminates the use of the Ethernet voice interface with its associated Network Activity LEDs.

Single subnet option for voice and management

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

LAN traffic engineering with RAS on T-LAN

When a remote H.323 Client generates a voice call through a PSTN, its entry point to an IP network is most likely at a Remote Access Server/Router or the router directly connected to the T-LAN of Meridian 1 ITG. The impact of the call will be calculated for the T-LAN only. We will assume that it does not use the intranet of an enterprise (if it has one).

LAN and WAN traffic engineering with distributed RAS and clients

This is a configuration that remote H.323 Clients concentrate their traffic to a subnet in an intranet that will traverse through the corporate WAN to reach the router connected to the T-LAN of Meridian ITG.

In this scenario, traffic from H.323 Clients will impact both corporate WAN and T-LAN of the IP Line card node. Only this type of network will have QoS and WAN requirement calculations associated with it.

Resource impacts

Ethernet and WAN bandwidth calculation

Table 2 lists the Ethernet and WAN bandwidth usage of IP Line ports with the 729AB codec only. Traffic generated by an H.323 client is typically similar to that of a digital set. The default value is assumed to be 6 CCS per set. However, to estimate IP Telecommuter’s impact on T-LAN and WAN, all traffic from clients are to be aggregated and divided by 36 to get the number of fully utilized ports to use the bandwidth usage table.

To calculate the bandwidth requirements of a route, the total route traffic after having been divided by 36, should be multiplied by the bandwidth usage per port to obtain the data rate requirement of that route. All traffic data should be based on busy hour requirements.

Note that to calculate resource requirements (IP Line card ports and T-LAN/WAN bandwidth), traffic parcels are summarized in different ways: (1) All sources of traffic destined for the IP telephony network using the same LAN should be added together to calculate the total T-LAN requirement. (2) For data rate requirement at the intranet route, calculation is based on duplex channels. Therefore, the engineering procedures for T-LAN and WAN are slightly different. Data rate for a T-LAN is the total bit rate, for a WAN is the duplex data rate. For example, 120 Kbps on the LAN is equal to a 64 Kbps duplex channel on the WAN.

Table 2
T-LAN Ethernet and WAN IP bandwidth usage per IP Line card port (silence suppression always enabled)

Codec type	Frame duration in ms (payload)	Voice payload in bytes	IP packet in bytes	Ethernet frame bytes	Bandwidth usage on T-LAN: kbps	Bandwidth usage on WAN: kbps
G.729 Annex AB (8kbps)	**30**	**30**	**70**	**96**	**25.6**	**9.3**

Note 1: T-LAN data rate is the effective Ethernet bandwidth consumption.

Note 2: T-LAN kbps = Ethernet frame bytes*8*1000/Frame duration in ms

Note 3: WAN kbps = IP packet bytes*8*1000/frame duration in ms/2.

Note 4: 50% voice traffic reduction due to silence suppression.

Note 5: Overhead of IP packet over voice packet is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.

Note 6: 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.

Note 7: Overhead of (RTP+UDP+IP) packets over the voice payload multiframe is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.

Note 8: The interframe gap of 12 bytes is not included in the above bandwidth calculation, because of the low probability of occurring in this type of application.

Input/Output of 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 engineering 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. Traffic engineering will require input as follows:

- CCS/H.323 client
- Number of H.323 clients
- Number of subnets/servers accessed by H.323 clients

The result of calculation will provide estimated values for the following:

- Total T-LAN bandwidth requirement
- WAN bandwidth requirement per subnet or server/router

A subnet is defined as a remote network serving a collection of H.323 clients, which is represented by a Server or Router communicating with the ITG processor for VoIP service (See Figure 19).

The Quality of Service (QoS) provided to clients can be estimated by specifying the objective one-way packet delay and percentage packet loss as set by the user. Whether the objectives have been met will only be verified when the ITG system is in service, and its performance data can be collected through Ping and TraceRoute or other measurement packages. The QoS issue will be further discussed after measuring tools have been described.

ITG Engineering Processes

Loading on an ITG Card

There are 24 ports on an ITG Line Card, each card takes up two card slots on an IPE shelf of 16 slots. Therefore, a maximum of 8 ITG Line Cards per shelf are allowed.

The ITG Line Card will appear to the Meridian 1 as an XDLC Line Card. Each port is associated with one H.323 Client, hence an ITG Line Card can support 24 registered H.323 Clients.

Due to the capacity limitation of an ITG Line Card processor, a card can process 15 simultaneous calls with minimum packet delay or loss. To protect QoS of calls in progress, when the 16th call comes in, it will be blocked and not allowed into the system under the flow control rule implemented in the ITG software. Assuming 4 calls per hour per client, and a holding time of 300 seconds, the probability of blocking to occur is less than 0.001. This critical load amounts to 12 CCS per client with a 20% peaking allowance.

With the loading of 6 CCS or less per set in a typical office model, the blocking probability is negligible. However, users should take care not to engineer an application beyond the stated capacity.

T-LAN Engineering Procedure

- Obtain total subnet traffic: Number of clients*CCS/client
- Convert to erlangs: total CCS/36
- Find T-LAN kbps number from bandwidth table
- Bandwidth per subnet: total erlangs*T-LAN kbps
- Repeat the procedure for each subnet
- Sum us total T-LAN bandwidth
- ITG cards = total H.323 clients/24

T-LAN Engineering Example

Subnet A: 36 clients, average 6 CCS/client.

Total erlangs =36*6/36 =6

Subnet B: 72 clients, average 5 CCS/client.

Total erlangs =72*5/36 =10

Subnet C: 12 clients, average 6 CCS/client.

Total erlangs =12*6/36 =2

T-LAN Bandwidth = 25.6*(6+10+2)= 460.8 kbps

Number of ITG cards=(36+72+12)/24=5

WAN Engineering Procedure

- Obtain total subnet traffic: Number of clients*CCS/client
- Convert to erlangs: total CCS/36
- Find WAN kbps number from bandwidth table
- Bandwidth per subnet: total erlangs*WAN kbps
- Adjust for traffic peaking by *1.3
- Repeat the procedure for each subnet

Adjust WAN bandwidth to account for WAN overhead depending on WAN technology used:

- ATM (AAL1): subnet bandwidth*1.20 (9 bytes overhead/44 bytes payload)
- ATM (AAL5): subnet bandwidth*1.13 (6 bytes overhead/47 bytes payload)
- Frame Relay: subnet bandwidth*1.20 (6 bytes overhead/30 bytes payload -variable payload up to 4096 bytes)

WAN Engineering Example

Subnet A: 36 clients, average 6 CCS/client.

Total erlangs =36*6/36 =6

Subnet B: 72 clients, average 5 CCS/client.

Total erlangs =72*5/36 =10

Subnet C: 12 clients, average 6 CCS/client.

Total erlangs =12*6/36 =2

WAN Bandwidth to subnet A = 9.3*6=55.8 kbps

WAN Bandwidth to subnet B = 9.3*10 = 93 kbps

WAN Bandwidth to subnet C = 9.3*2 =18.6 kbps

Bandwidth to subnet A with 30% peaking =55.8*1.3 = 72.54 kbps

Bandwidth to subnet B with 30% peaking = 93*1.3 = 120.9 kbps

Bandwidth to subnet C with 30% peaking =18.6*1.3 = 24.18 kbps

If the WAN is known to be an ATM network (AAL1), the estimated bandwidth requirements are:

Bandwidth to subnet A with ATM overhead =72.54*1.2 = 87.0 kbps

Bandwidth to subnet B with ATM overhead = 120.9*1.2 = 145.1 kbps

Bandwidth to subnet C with ATM overhead = 24.18*1.2 = 29.0 kbps

> ***Note:*** Each WAN link should be engineered to be no more than 80% of its total bandwidth if the bandwidth is 1536 kbps or higher (T1 rate); if the rate is lower, up to 50% loading on the WAN is recommended.

Performance Evaluation and Enhancement

Assessing WAN link resources

For most applications, H.323 Client calls will come from PSTN. In that case, only LAN traffic engineering is required. However, if calls are routed through intranet, WAN links are frequently 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 IP telephony network.

Link utilization

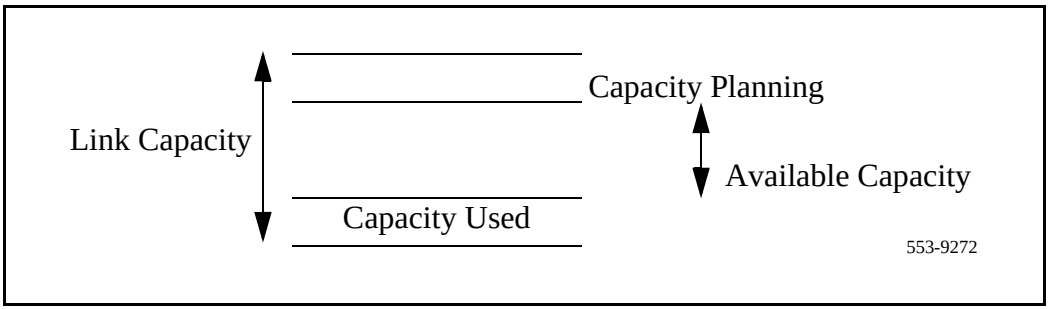
The starting point of this assessment is to obtain a current topology map and link utilization report of the intranet. A visual inspection of the topology map should reveal which WAN links are likely to be used to deliver IP Telecommuter traffic. Alternately use the `traceroute` tool.

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 link. Also, because WAN links are full-duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.

The third step is to assess how much spare capacity is available. Enterprise entrants 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 80%. The carrying capacity of the 56 kbps link would be 28 kbps, and for the T1 1.2288 Maps. 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.

The difference between the current capacity and its allowable limit is the available capacity. This can be better illustrated in Figure 17. For example, a T1 link utilized at 48% during the peak hour, with a planning limit of 80% would have an available capacity of about 492 kbps.

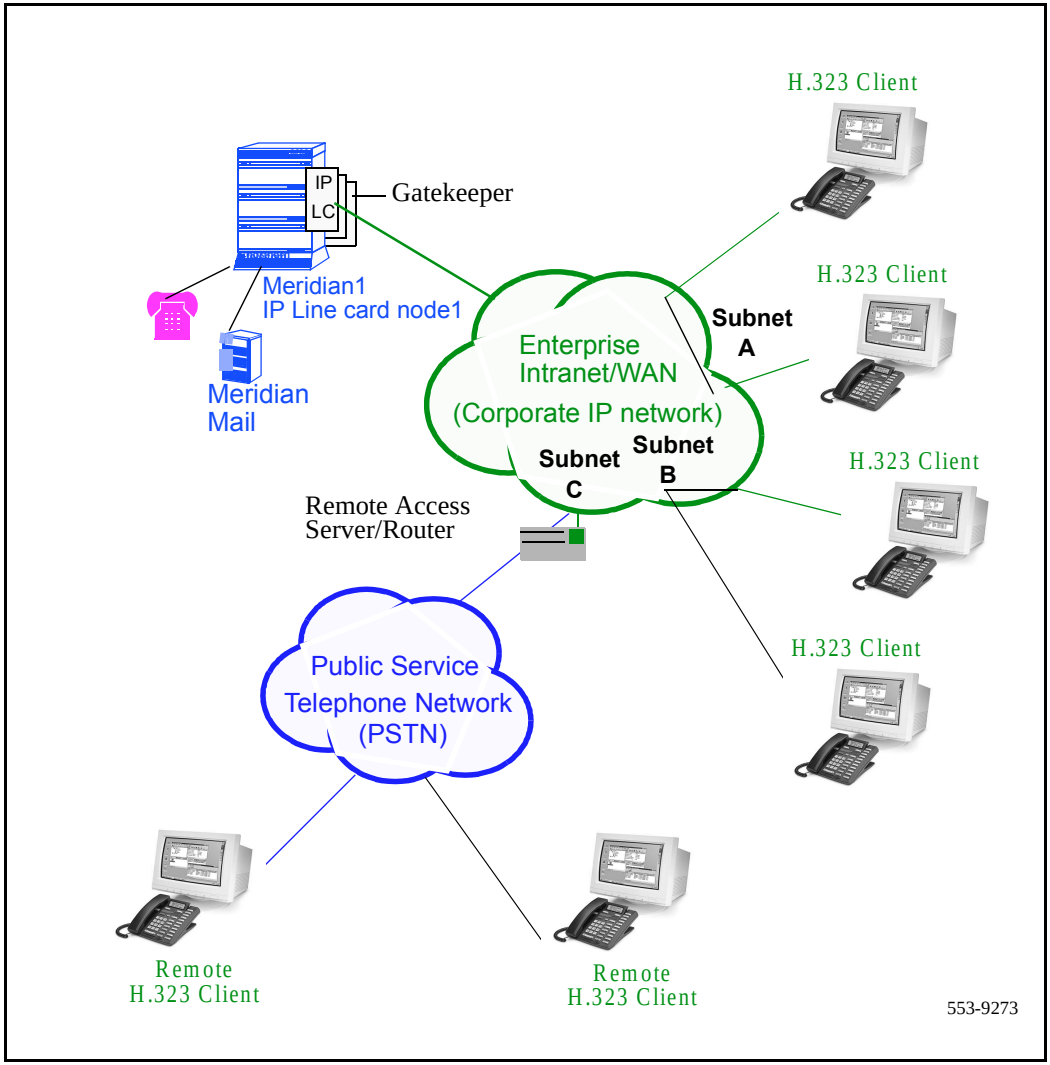
Figure 17
Link Capacity



Estimating network loading due to IP Telecommuter traffic

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

Figure 18
An Example of an Intranet with Subnetworks



Suppose the intranet has a topology as shown in Figure 18, and the technician wants to predict the amount of traffic between the IP Telecommuter node and corporate intranet. From the IP Telecommuter Traffic Engineering section and `traceroute` measurements, traffic between IP Telecommuter node and subnet A, IP Telecommuter node and subnet B, and IP Telecommuter node and Router/Server C are collected.

To complete this exercise, the traffic flow from the IP Telecommuter node to all routes needs to be summed to determine the load to the link (T-LAN).

Remote Access Server

The location of a RAS, where dial up voice traffic enter the network, should be located as closely as possible to the T-LAN of the IP Line card node as closely as possible, so that the calls from outside will not need to traverse a long distance on the packet network.

Decision: Sufficient capacity?

A link is defined as the channel between the IP Line card node and a subnet. Table 3 organizes the computations so that for each link, the available link capacity can be compared against the additional IP Line card load. For example, on the link from the IP Line card Node to Subnet C, there is plenty of available capacity (568 kbps) to accommodate the additional 24 kbps of IP Line card traffic.

Table 3
Link Utilization Summary Example

Link		Utilization (%)		Available capacity (kbps)	Incremental ITG load Traffic (kbps)	Sufficient capacity?
End-points	Capacity (kbps)	Threshold	Used			
ITG_Node1 - SubnetA	1536	80	75	76.8	72.5	Yes
ITG_Node1 - SubnetB	1536	80	50	460.8	120.9	Yes
ITG_Node1 - SubnetC	1536	80	48	492	24.2	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, the following option should be considered:

- Upgrade the link's bandwidth.

Quality of Service (QoS) Determination

Bottlenecks caused by non-WAN resources are less frequent. For a more thorough assessment the technician should also consider the impact of incremental IP Telcommuter traffic on routers and LAN resources in the intranet. Perhaps the IP Telecommuter traffic will traverse LAN segments that are saturated, or routers whose CPU utilization is high. A customer should consider re-routing scenarios in the case where a link breaks.

It should be noted that the service provided by the intranet is “best-effort delivery of IP packets”, not “guaranteed QoS for real-time voice transport.”

QoS Measurements

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.

To use measuring tools requires that a starting point and an end point be defined. The starting point can be a `ping` host on a LAN segment attached to the router intended to support the IP Line card node. The destination node can be a remote access server or a remote subnet depending on the network topology. The requirement is briefly described as follows.

Criteria

- **End-to-end packet delay:** Packet delay is the point to point one-way delay between the time a packet is sent to the time it is received at the remote end. It comprises of delays at the ITG node and WAN route. To minimize delays, the ITG node should be positioned as close as possible to the network backbone, or WAN, with a minimum number of hops.

  To assure a good voice quality, the end-to-end delay is recommended to be <= 200 ms.

- **End-to-end packet loss:** Packet loss is the percentage of packets sent that do not arrive at their destination. Transmission equipment problems, packet delay, and network congestion cause packet loss. It voice conversation, packet loss appears as gaps in the conversation. Sporadic loss of small packets can be more tolerable than infrequent loss of large packets.

  For high quality voice transmission, a packet loss of <= 2% is recommended.

Measuring tools

- Ping
- Traceroute

Both Ping and Traceroute are basic measuring tools for IP network. They come with Window 95, Window NT and other packages. Pint is used to measure round trip delay of a packet and the percentage of packet loss; while Traceroute breaks down delay segments of a source-destination pair and any hops in-between.

There are many vendor packages doing data collection as Ping and Traceroute do. In addition, these programs also analyze data and plot performance charts. To directly use Pint/Traceroute to collect data for manual analysis is tedious. However, the information provided by these basic tools is just as useful as any sophisticated package.

Consequently, all sequel analysis will use Ping/Traceroute data for discussion, even though in practice, some third party packages will most likely be used.

Destination Types

To a Remote Access Server

This configuration is applicable when a remote H.323 Client originates the call from a PSTN. Its entry point to the intranet is through a Remote Access Server/Router. The ping host should target this Server/Router for delay measurement. A fixed delay between the Server/Router to the remote Client should be added to the measured value to account for the last leg of delay the Client would experience. Refer to Figure 19 for a chart that shows the effect of delay on Quality of Service.

To a Remote Subnet

This configuration involves an intranet subnet that is attached to a number of H.323 Clients, which serves as a hub for delivering voice packets between the Client and IP network. The delay measurement should be collected between the `ping` host and the subnet server.

Measuring 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:

```
ITG_Node1 % ping -s subnetA 60

PING subnetA (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

^?

--- ITG_Node1 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_node1 would experience, the `ping` host should be on a healthy LAN segment attached to the router intended to support the IP Line card 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 can be any numbers, the default is 60 bytes.

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 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 a specific route.

Delay characteristics vary depending on the site pair and the time-of-day. A “site pair” is defined as the measurement between the host ITG and the remote subnet served by a remote access server or router (for example, ITG to subnet A in Figure 18). 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).

Recording routes

Routing information for all source-destination pairs needs to be recorded as part of the network assessment. This is done using the `traceroute` tool; an example of the output is shown below.

```
itg_node1 % traceroute subnetA

traceroute to subnetA 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     subnetA (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, as illustrated in the following command syntax:

```
itg_node1 % traceroute -g  subnetA itg_node1
```

Adjusting 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 should 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 IP Line card 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 directions of flow. This can be true even if the flow is on a symmetric route due to 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.

A "site pair" is defined as the measurement between the host ITG and the remote subnet served by a server (for example, ITG to subnet A in Figure 18).

Table 4 shows the way to record one way delay, packet loss, and expected QoS level for each site pair.

Table 4
QoS Measurements Summary

Site pair	Measured One way delay (ms)		Measured Packet loss (%)		Expected QoS level (see Table 6)	
	Mean	Mean+σ	Mean	Mean+σ	Mean	Mean+σ
ITG_Node1/SubnetA	171	179	2	2.3	Excellent	Good
ITG_Node1/SubnetB	120	132	1.3	1.6	Excellent	Excellent
ITG_Node1/SubnetC	190	210	2.1	2.3	Good	Good
ITG_Node1/Router1	220	235	2.4	2.7	Good	Good
ITG_Node1/Router2	305	345	2.2	2.6	Good	Fair
ITG_Node1/Router3	260	286	2.4	2.8	Good	Fair

As an example, the site pair ITG_Node1 and SubnetA has the mean delay and average packet loss meeting "excellent" criteria while with standard deviation, they satisfy only "good" QoS level.

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 service. Looking at the "Expected QoS level" column in the above table, the technician can gauge the QoS level for each site pair.

In order to offer good voice quality, the technician should keep the network Mean+σ operating region within a “Good” or “Excellent” QoS level.

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 Table 6 data, the technician can estimate the amount of one-way delay or percentage packet loss that needs to be reduced to raise the QoS level.

If the decision is to keep costs down, and accept a “Fair” QoS level for a particular route, the technician will need to closely monitor the QoS level, reset expectations with the end users, and be receptive to user feedback to make changes.

Network Fine-tuning

There are a number adjustments can be made to fine-tune the network and to improve its QoS. Here are some practical approaches.

Reducing delays

In this and the next few sections, the guidelines explore different ways of cutting down *one-way delay* and *packet loss* in the IP telephony 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. 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 with.
- Implementing a priority queueing discipline.

To determine which links should be considered for upgrading, first list all the intranet links used to support the IP Telecommuter 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:

```
ITG_Node1 % traceroute SubnetA

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

      router1 (10.8.0.1) 1 ms  1 ms  1 ms

      router2 (10.18.0.2) 42 ms  44 ms  38 ms

      router3 (10.28.0.3) 78 ms  70 ms  81 ms
```

```
router4 (10.3.0.1) 92 ms  90 ms  101 ms

SubnetA (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.

Reducing hop count

The IP Line card 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 no more than 8 cards share the same 10BaseT LAN collision domain, provided that the preferred codec throughout the IP telephony network is set to G.729 AB with 30 ms default payload size. (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.)

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 IP Line card node can still provide voice services even if one of the hubs fails.

The IP Line card node and the T-LAN router should be placed as close to the WAN backbone as possible, again to minimize the number of router hops, segregate constant bit-rate Voice over IP traffic from bursty LAN traffic, and simplify the end-to-end Quality of Service engineering for packet delay, jitter, and packet loss. If an access router separates the IP Line card 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.

Reducing 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.

Adjusting 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.

The jitter buffer size is adjustable through the MAT input. It is not applicable to a client (optimized built-in value cannot be changed).

The following parameters control the size of the jitter buffer in the destination IP Line card node.

- Voice playout nominal delay. This can range from twice the payload size to 10 times. The MAT default value is 60.
- Voice playout maximum delay is 120.

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. 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.

Implementing 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 which now need to deliver IP Telecommuter traffic, it is likely that the QoS objectives pertaining to delay will impose an additional design constraints.

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 a relatively recent technology, infrequently implemented on intranets, and it is difficult to predict the consequences.

This section outlines the QoS mechanisms that can work in conjunction with the IP Line card node, and the intranet-wide consequences if implemented.

Traffic mix

Traffic mix is the mix of IP Telecommuter traffic and data traffic on the intranet.

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 IP Telecommuter traffic, and all traffic flows are equal priority, then there is no need to consider QoS mechanisms. This network would have only one class of traffic.

In most corporate environments, the intranet primarily supports 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 IP Telecommuter traffic should take advantage of established mechanisms if possible.
- What is the traffic mix? If the IP Telecommuter traffic is small compared to data traffic on the intranet, then IP QoS mechanisms might do well. On the other hand if IP Telecommuter traffic is significant, data services might be impacted when those mechanisms are biased toward IP Telecommuter 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
- IP Telecommuter traffic streams are unfairly affected

Post-installation network measurements

The design process is continual, even after implementation of the IP telephony network and commissioning of voice services over the network. Network changes – in actual IP Telecommuter 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.

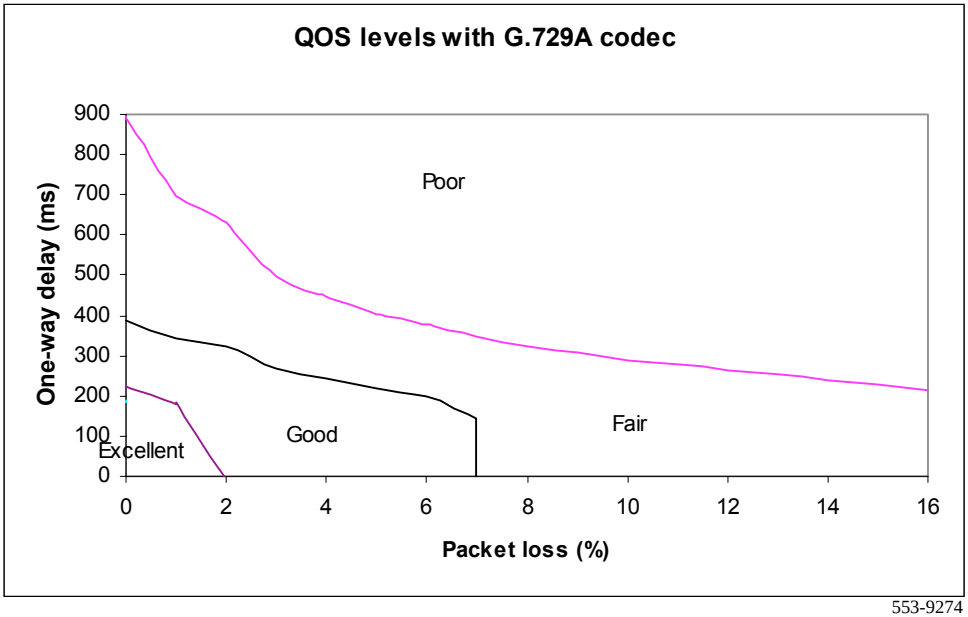
It is assumed that the customer's organization already has processes to monitor, analyze, and re-design both the Meridian 1 network and the corporate intranet so that both networks continue to conform to internal quality of service standards. When operating voice-over-IP services, the customer's organization needs to incorporate additional monitoring and planing processes. They are:

- Collect, analyze, and trend IP Telecommuter 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 IP telephony network can be managed to ensure that desired QoS objectives are always met.

Measured data of one-way delay (ms) and packet loss (%) for a given route (link) should be checked against Figure 19 QoS regions to determine the QoS of this route. Refer to Table 6 for more specific reading of QoS based on numerical pairs of one-way delay and packet loss.

Figure 19
QoS levels with G.729AB codec



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 the IP Telecommuter site. The delay monitoring tool will be running continuously, injecting probe packets to each remote subnet or router/server 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.

A target QoS objective for each route from the IP node to a remote subnet (or router) is set by the customer.

At the end of the month, the technician can analyze each remote subnet QoS based of information summarized in Table 5. Fill Table 5 with measurements between the remote access server or PCs and the IP Line card, or between the PCs and the card.

Table 5
QoS monitoring

Site pair	One-way delay Mean+σ (ms)		Packet loss Mean+σ (%)		QoS		
	Last period	Current period	Last period	Current period	Last period	Current period	Objective
ITG_Node1 /SubnetA	135	166	1	2	Excellent	Good	Excellent
ITG_Node1 /SubnetB	210	155	3	1	Good	Excellent	Excellent
Etc.							

Declines in QoS can be observed through the comparison of QoS between last period and current period. A consistent inferior measurement of QoS for a route compared with the objective should trigger an alarm to the customer that the customer must take steps to strengthen the performance of the route.

Estimating QoS level

Use Table 6 to estimate the IP telephony QoS level based on QoS measurements of the intranet. To limit the size of this table, the *packet loss* and *one-way delay* values are tabulated in increments of 1% and 10ms respectively. Nortel Networks has applied for a patent on the techniques used to determine and apply the information in this table.

Table 6
QoS based on intranet measurements

Packet loss (%)	One-way delay (ms)	Qos level G.729 AB
0	50-200	excellent
0	210-220	excellent
0	230-330	good
0	340-360	good
0	370-380	good
0	390-620	fair
0	630-780	fair
0	790	fair
1	50-180	excellent
1	190-200	good
1	210-320	good
1	330-340	good
1	350-360	fair
1	370-630	fair
1	640-690	fair
1	700-780	poor
2	50-270	good

Table 6
QoS based on intranet measurements

Packet loss (%)	One-way delay (ms)	Qos level G.729 AB
2	280-300	good
2	310-320	good
2	330-510	fair
2	520-580	fair
3	50-250	good
3	260	good
3	270-460	fair
3	470-490	fair
4	50-200	good
4	210-240	good
4	250-390	fair
4	400-440	fair
5	50-180	good
5	190-210	good
5	220-360	fair
5	370-400	fair
6	50-200	good
6	210-330	fair
6	340-380	fair
7	50-140	good
7	150-310	fair
7	320-340	fair

Table 6
QoS based on intranet measurements

Packet loss (%)	One-way delay (ms)	Qos level G.729 AB
8	50-290	fair
8	300-320	fair
9	50-270	fair
9	280-300	fair
10	50-260	fair
10	270-280	fair
11	50-250	fair
11	260-270	fair
12	50-230	fair
12	240-260	fair
13	50-230	fair
13	240-250	fair
14	50-210	fair
14	220-230	fair
15	50-190	fair
15	200-230	fair
16	50-160	fair
16	170-210	fair

Internet protocols and ports

The following IP applications and protocols are used, and must be transmitted across the customers intranet by all IP routers and other network equipment.

ITG Management Protocols

IP Telecommuter uses the "well-known" UDP and TCP port numbers for SNMP, Telnet, and FTP, i.e. the default port numbers for these common IP applications.

ITG H.323 Voice Gateway Protocols

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

Realtime Transport Protocol (RTP) uses UDP port 2300-2315.

IP Telecommuter Client

The IP Telecommuter Client is the H.323 desktop application or client, used in the IP Telecommuter product. It provides users with the functionality of a desktop telephone with which they can access the voice network from any point of presence on their enterprise intranet.

Network organization

Terminals are managed by organizing them into zones. Each zone is managed by an IP Line card Gatekeeper (Leader 0 or Leader 1) and serviced by one or more Gateways. The IP Line card Gatekeeper controls which endpoints are allowed to log onto a zone, as well as providing DN to IP address translation. Each IP Line card provides 24 ports.

System requirements

IP Telecommuter Client with USB set

- M9617 USB set
- Pentium 150 MHz or higher multimedia PC
- Windows 98 operating system
- USB port
- 32 MB RAM
- 10 MB free disk space
- Dialup or Ethernet connection
- 28.8 kbps modem or better (for dialup RAS access)

IP Telecommuter without USB set

- Headset
- Pentium 150 MHz or higher multimedia PC
- Windows 95/98 or Windows NT operating system
- Full duplex soundcard
- 32 MB RAM
- 10 MB free disk space
- 28.8 kbps modem or better
- Dialup or Ethernet connection

Use of sound cards and headsets

We recommend the USB phone as the speech device for Casual Telecommuters. While Headsets and sound cards work with the same PC software, a number of problems have been seen that relate to the users PC and the usage of sound cards for voice. These events are independent of the IP Telecommuter application.

The following problems have been noted on various PC's using sound cards and headsets. The symptoms can appear on similar makes, models and vintages.

Problems by specific PC:

- electrical noise generated by PC and unfiltered by sound card
- full duplex driver enabled sound card (simplex = push to talk)
- headset microphone adapters may be required to convert to 'stereo' from 'mono' for certain headsets
- gain (sound level) can be very low, depending upon your sound card

Problems on a per-call use

- poor quality headsets can impact the quality of conversation
- microphone position is very sensitive (much more so than telephone headsets)
- multi-media sound settings are very coarse and can over/under drive sound

Use of WinModem and SoftModems

It should also be noted that modems that use the PC to process their activity (Winmodem and/or Softmodems) can cause very long network response times. This delay can cause severe impact to both USB and Softclient configurations.

Feature summary

Voice calling

Calls can be placed both from the IP Telecommuter client to the Meridian 1 and from the Meridian 1 to the IP Telecommuter client.

Set features

The IP Telecommuter Client has access to the following Meridian 1 telephone features: Conference, Transfer, and Hold.

Voice mail

The IP Telecommuter Client shares a voice mailbox with the user's desktop set. This includes message indication, the MWI indicator on the user's IP telephone reflects the status of the MWI indicator of their desktop set.

Called/Calling Party Name Display

IP Telecommuter Client users can see both the names of other parties and have their name seen by other parties.

Voice compression

The IP voice packets are compressed using G.729AB speech compression only. Compression is provided by a software codec running on the PC.

Authentication

When the IP Telecommuter Client starts up the user will be asked to enter their authentication password. The client must be authenticated by the ITG Line card Gatekeeper before being allowed to log onto the voice network. When a call is made or answered, an authentication check is also performed.

Address translation

The ITG Line card Gatekeeper (Leader 0 or Leader 1) in each node provides DN to IP address translation, allowing endpoint accessing by DN.

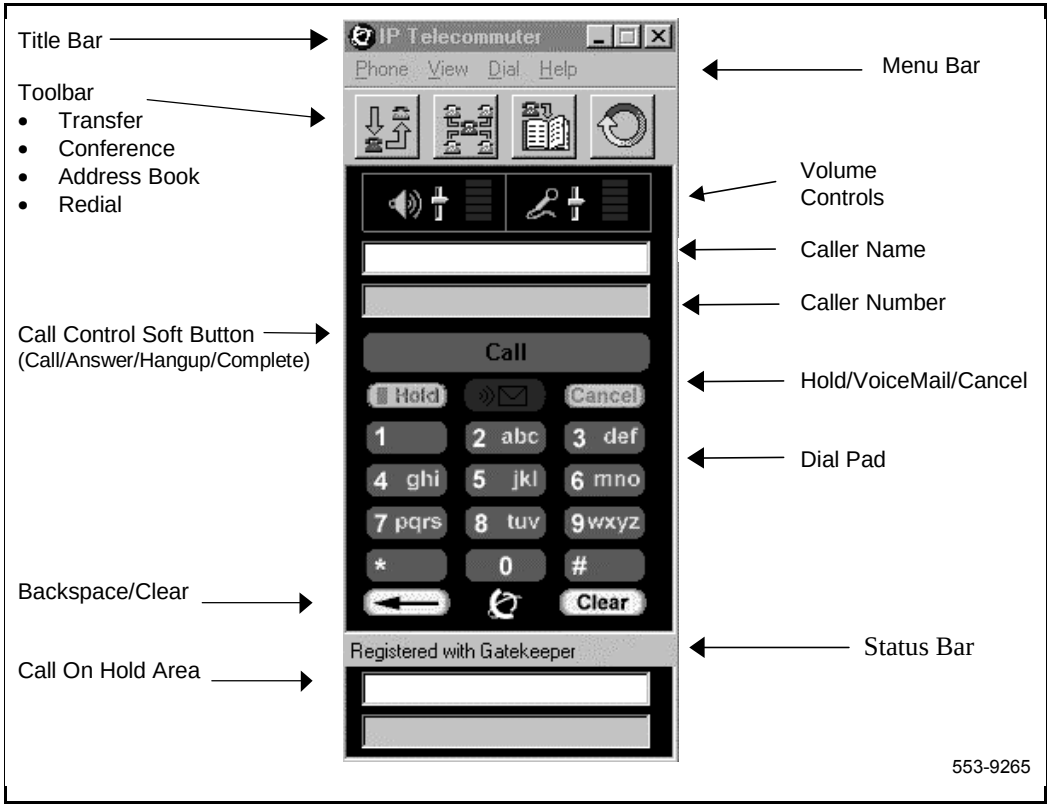
Client documentation

A complete and comprehensive set of Client documentation is included on the IP Telecommuter Client CD.

User Interface description

Figure 20 shows the IP Telecommuter Client main window. User controls are labelled as described below.

Figure 20
IP Telecommuter Client main window



Installation and configuration

This chapter describes the installation and configuration of an ITG node on MAT and the Meridian 1. This installation assumes that MAT, including Alarm Management and the MAT ITG IP Telecommuter application has already been installed, that no IP Line 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 IP Telephony network.

The DN to TN configuration in MAT must be coordinated with the Meridian 1 overlay 11 configuration.

Installation summary

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

Create the IP Line card Installation Summary Sheet

It is recommended that an IP Line card Installation Summary Sheet (Table 7) 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 (Table 7) will greatly facilitate entry of configuration data on MAT and Meridian 1.

The MAC address is the Motherboard Ethernet address shown on the IP Line card faceplate. The E-LAN Management IP address is the address of the management interface used to perform management via MAT. The T-LAN Voice IP address is the IP address of the voice interface.

Table 7
IP Line card Installation Summary Sheet (Part 1 of 3)

Site_____**M1 system**_____**M1 customer**_____
T-LAN Node IP address_____**SNMP Manager List IP 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
				leader	0
				leader	1
				follower	2
				follower	3
				follower	4
				follower	5
				follower	6
				follower	7
				follower	8
				follower	9

Table 7
IP Line card Installation Summary Sheet (Part 2 of 3)

Site_____**M1 system**_____**M1 customer**_____
T-LAN Node IP address_____**SNMP Manager List IP 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

Table 7
IP Line card Installation Summary Sheet (Part 3 of 3)

Site_____**M1 system**_____**M1 customer**_____
T-LAN Node IP address_____**SNMP Manager List IP 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

Add an ITG node on MAT manually

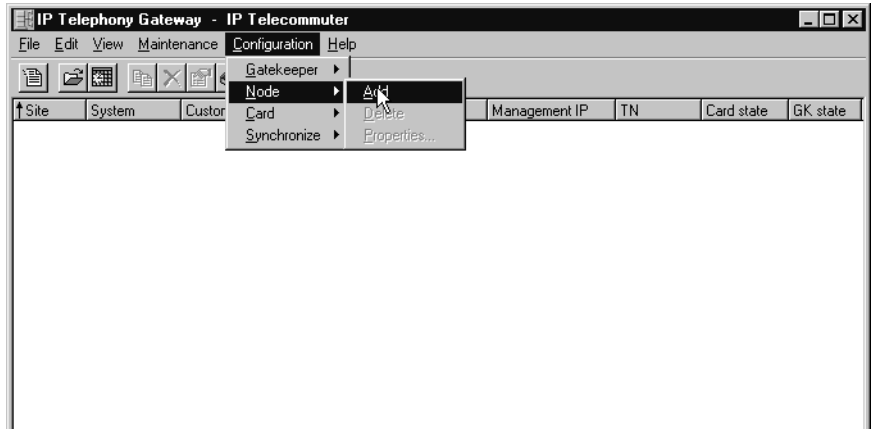
This section uses the ITG IP Telecommuter application to manually add and configure an ITG node, and add IP Line cards to the node. Every ITG node must be first be added manually on the MAT IP Line PC, and the MAT IP Line configuration data must be transmitted to the ITG node during installation. Thereafter,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

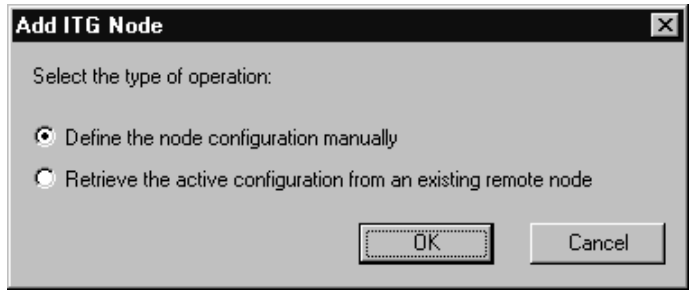
The site name, Meridian 1 system name, and Meridian 1 customer number must exist in the MAT Navigator before you can add a new ITG node. Only one ITG node can be added in the ITG IP Telecommuter application per Meridian 1 customer on a MAT Meridian 1 system.

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.

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

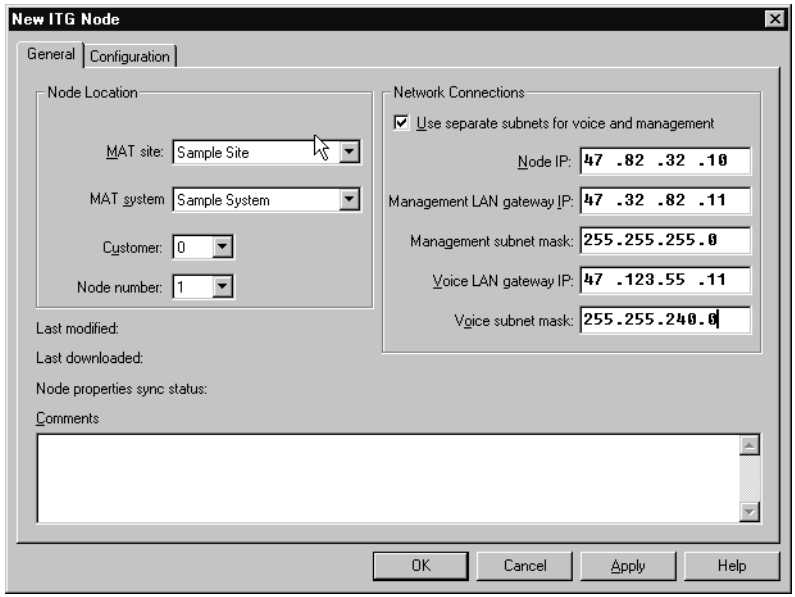
1. Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.
2. Select Click **Configuration | Node | Add.**
3. When the "Add ITG Node" dialog box appears, click **OK** to accept the default choice of manually defining an ITG node.


IP Telephony Gateway - IP Telecommuter
File Edit View Maintenance Configuration Help
Gatekeeper
Node
Card
Synchronize
Add
Delete
Properties...
Site
System
Custor
Management IP
TN
Card state
GK state


Add ITG Node
Select the type of operation:
Define the node configuration manually
Retrieve the active configuration from an existing remote node
OK
Cancel

Configure the node

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



2 Select the MAT site: MAT system, customer and Node Number 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 Configure Network as described below:

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, remove the check from the "Use separate subnet for voice and management" box and 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, leave the default “Use separate subnet for voice and management” box checked, 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 IP Line card Installation Summary Sheet.

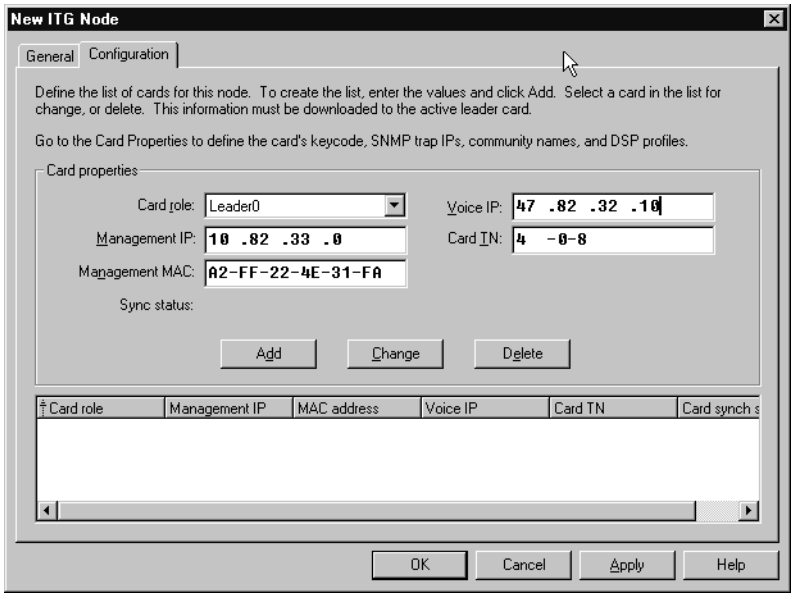
Add IP Line cards to the node

The “Configuration” tab is used to add IP Line 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.”

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. MAT displays "enable:active" for Leader 0 and "enable:standby" for Leader 1 on the card state field.
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.

1 Click the **Configuration** tab.



2 To add a card:

a 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 IP Line card.

b Select “Leader 0”, “Leader 1”, or “Follower” from the “Card role” pull-down menu.

c Click **Apply** then **OK**.

3 Repeat the previous steps for each card to be added within that ITG Node.

4 When all IP Line cards have been configured, click **OK**. The "IP Telephony Gateway - IP Telecommuter" window displays all configured IP Line cards.

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

What to do next?

Once you have completed the configuration of the node properties, there are two ways to proceed:

1 If the IP Line cards are on site, you should proceed with "Install the IP Line cards in the Meridian 1" on page 101, and then proceed to transmit the ITG node properties from MAT to the newly installed IP Line 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 IP Line cards.

2 If the IP Line cards are not on site, you can proceed now to "Configure the properties of each IP Line card" on page 113. After the IP Line cards arrive on site, and have been physically installed in the Meridian 1 system, you can then proceed to transmit the ITG node properties, Gatekeeper properties, and card properties.

Install the IP Line cards in the Meridian 1

Physical placement of the cards

The IP Line cards that have been added in MAT should now be installed in the Meridian 1. IP Line 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.

EMC requirements limit the number of IP Line cards you can install in an IPE shelf or Meridian 1 Option 11C systems. See "ITG I/O cabling for EMC compliance" on page 43.

The IP Line card can be configured as an XDLC card in slots 0 to 6 and 8 to 15 in an IPE shelf. The IP Line card cannot be configured as an XDLC 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 11C

systems, the IP Line card can be provisioned in the main or expansion cabinets. In an Option 11 main cabinet the IP Line card cannot be configured as an XDLC 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 IP Line cards per module, each card should preferably be installed such that the left slot is an even-numbered slot and the IP Line card is configured as an XDLC card in the even-numbered slot.

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

Note: In NT8D37AA IPE shelves only 16 tip and ring pairs are supported for most card slots. Since the IP Line card requires 24 tip and ring pairs in the left-hand card slot, the IP Line card can only be configured as an XDLC card in slots 0, 4, 8, and 12 in the NT8D37AA IPE shelf. The NT8D81AA IPE Expansion Kit is 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 IP Line 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 telephony capability in case of the failure of a single IPE shelf.

CAUTION

Do not install an IP Line 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 IP Line card, may damage the card.

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

Note: Refer to and update the IP Line card TNs on the IP Line card 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 IP Line card faceplate.

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

Note 1: When IP Line 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 IP Line card 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 "Faceplate maintenance display codes for card reset" on page 208 for a listing of display codes.

Install IP Line card NTMF94DA cable

The NTMF94DA cable provides the E-LAN, T-LAN and serial interface for the NT8R17 IP Line card. Refer to *Appendix A* for pinouts and technical specifications on the NTMF94DA cable.You must plug all IP Line card T-LAN interfaces belonging to the same ITG node into the same T-LAN hub. Plug all IP Line 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 250 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 IP Line card slot (see Figure 21).
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 22) into the faceplate Main port or in the serial port of the NTMF94DA interface cable. If required, use the NTAG81BA maintenance extender cable (see .

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 21
NTMF94DA E-LAN, T-LAN and serial cable

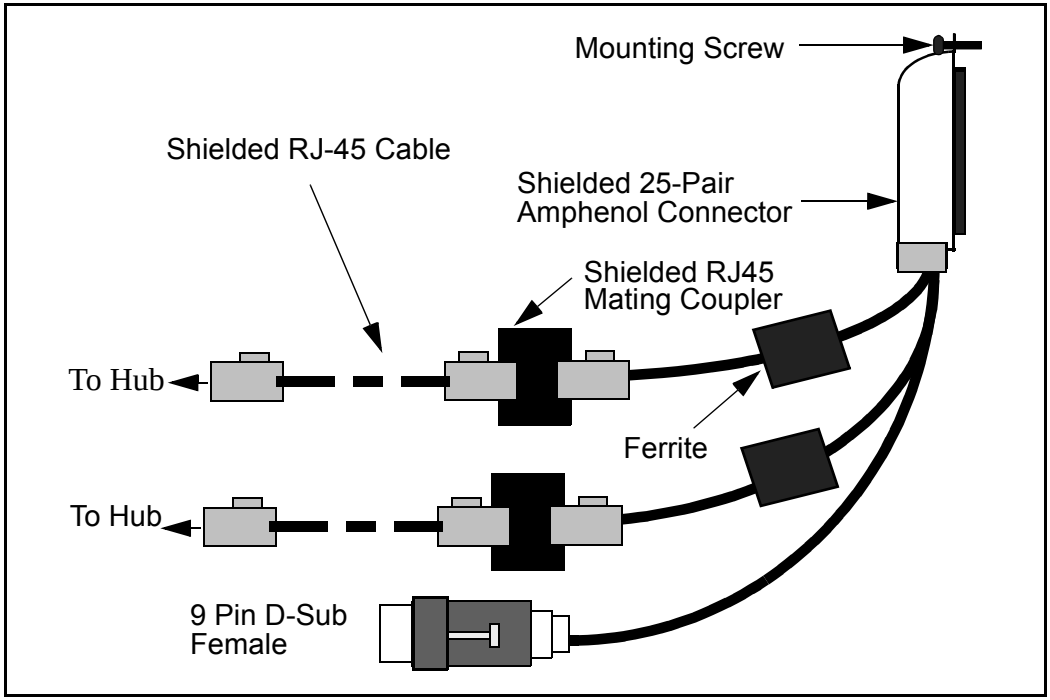


Figure 22
NTAG81CA Maintenance cable

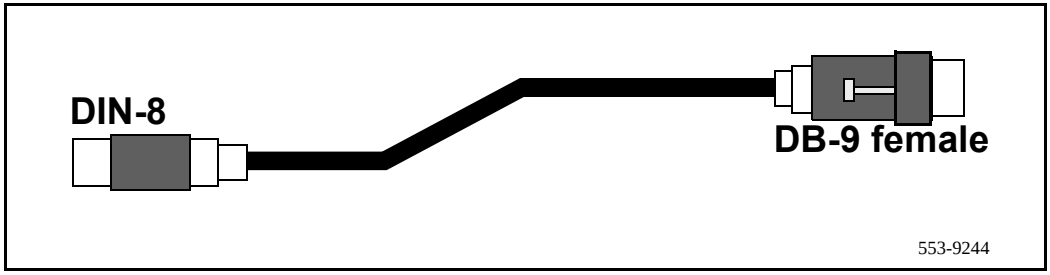


Figure 23
NTAG81BA Extender cable

Add IP Line card configuration data in Meridian 1

IP Line card configuration guidelines

Each port on an IP Line card is configured as an M2616 unit. To distinguish the IP Line card for administrative purposes, set the DES (designator) code in LD11 to "ITG". Each IP Line card supports up to 24 configured TNs. Each TN corresponds to an IP Client. You configure each TN as a M2616 set through overlay 11. Set the Flexible Voice/Data class of service to "Allowed" to use the TNs with unit number 16 and above. All 24 TNs on the same IP Line card must have the same Customer Number, and same configuration.

All Leader, Backup Leader, and Follower IP Line cards in the same group must also have the same Customer Number. You can configure multiple independent groups of Leader, Backup Leader, and Follower cards under the same Customer Number. Coordinate the DN configuration on each TN with the configuration of DNs to IP Line card ports in MAT (see Table 8).

Table 8
LD11 Configure IP Line cards (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	2616	Type of telephone set.
TN	l s c u	Terminal Number (corresponding to ports on the IP Line card, u = 0-23 for the 24 configured TNs on each IP Line card).
DES	ITG	To identify the IP Line card.

Table 8
LD11 Configure IP Line cards (Part 2 of 2)

CDEN	4D	Card density.
...	...	...
CUST	0-99	Customer Number (All sets corresponding to the same IP Line card must have the same customer number).
AOM	0	Number of Add-On Modules.
FDN	xxxxxxx	Flexible CFNA DN (Configure with Voice Mail DN).
...	...	...
CLS	ADD	Automatic Digit Display.
	CNDA	Call party Name Display Allowed
	FLXA	Flexible voice/data Allowed.
	FNA	Forward No Answer Allowed.
	MWA	Message Waiting Allowed.
	VCE	Voice Terminal. (for unit 16 and up).
...	...	...
KEY	00 MCR xxxxxxx	Multiple call ringing DN key. (Must be configured on key 0. xxxxxxx is the IP Client's DN).
- CPND	NEW	
- NAME	aaaa, bbbb	CPND name (First name, Last name).
- XPLN	xx	Expected name length.
-DISPLAY _FMT	Last, FIRST/(FIRST, LAST)	Display format for CPND Name.
KEY	01 TRN	Transfer key.
KEY	02 AO6	6 party Conference key.
KEY	03 MWK xxxxxxx	Message Waiting key. xxxxxxx is the Voice Mail DN.

Transmit ITG configuration information from MAT

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

Set the Leader 0 IP address

1. Connect the MAT PC com port or another terminal device to the serial port on the IP Line card on the faceplate or I/0 serial maintenance port of the NTMF94DA cable. 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 IP Line 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 IP Line card displays "T:20" on the 4-character display, the IP Line card will begin sending bootp requests on the E-LAN. A series of dots appears on the TTY.

3 Type **+++** and then press **Enter**. Enter the default "user ID" and "password" of itgadmin to access the ITG shell command line prompt:

...+++

user ID: itgadmin
password: itgadmin

ITG>

4 When the ITG shell prompt appears on the TTY, enter the IP address for the Leader card:

Wait until the display shows "T:21," then enter:
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.

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*.

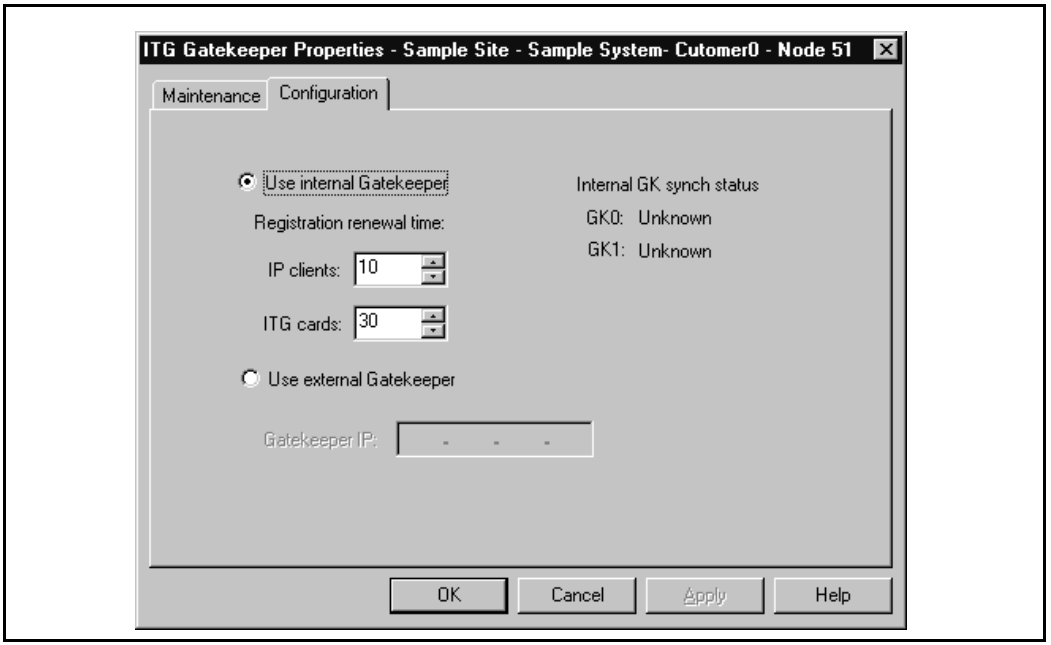
Leader 1 card will automatically be set as a leader after node properties are successfully transmitted.

5 Reboot the Leader 0 IP Line 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”.

Configure the Gatekeeper Properties

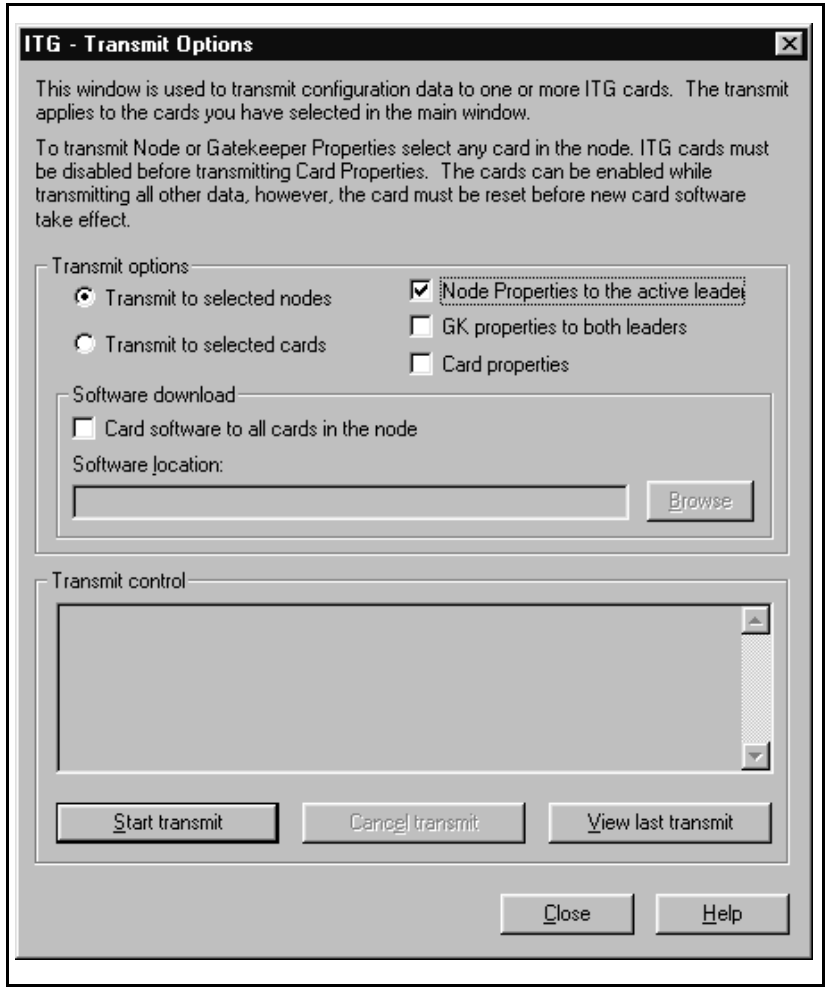
1. Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.
2. Click **Configuration** | **Gatekeeper** | **Properties.**
3. In the "ITG Gatekeeper Properties" window, click the **Configuration** tab.
4. Select the "Use internal Gatekeeper" option.
5. Configure the Registration renewal time for the "IP Clients" and "IP Line cards."
6. Click **OK**.



Transmit node properties

1 In the “IP Telephony Gateway - IP Telecommuter” 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 default setting of “Transmit to selected nodes”. Check the “Node Properties to the active leader” check box.

Note: Card Properties and Gatekeeper Properties will be transmitted in “Transmit card properties and Gatekeeper properties” on page 122.

Note: IP Line 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 IP Line 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.

4 Click the **Start Transmit** button.

Monitor progress in the “Transmit Control” window. Confirm that the node properties are transmitted successfully.

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

6 Reboot the Leader 0 IP Line 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.

Note: If you are installing ITG from a remote MAT ITG PC and if you cannot communicate with the node after transmitting the node properties and rebooting the Leader 0 card, this means that the ITG cards are unable to communicate back to the remote MAT ITG PC through the voice gateway. To reestablish communication with the ITG node, you may connect to the ITG maintenance port and use the ITG shell ’routeAdd’ command on each ITG card to add a new IP route that points to the remote MAT ITG PC subnet. This step must be repeated every time a card is reset until the card properties (containing the SNMP Manager IP addresses) have been successfully transmitted to the card.

7 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.

8 Verify that the TN, management interface MAC addresses, and IP addresses are configured correctly for each IP Line 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 IP Line card Installation Summary Sheet.

What to do next?

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

- If you have previously configured the card properties of each IP Line card in the node, you should proceed to “Transmit card properties and Gatekeeper properties” on page 122.
- If you chose to configure the card properties of each IP Line card in the system after you physically installed the IP Line cards in the Meridian 1 system, you may now proceed to “Configure the properties of each IP Line card” on page 113.

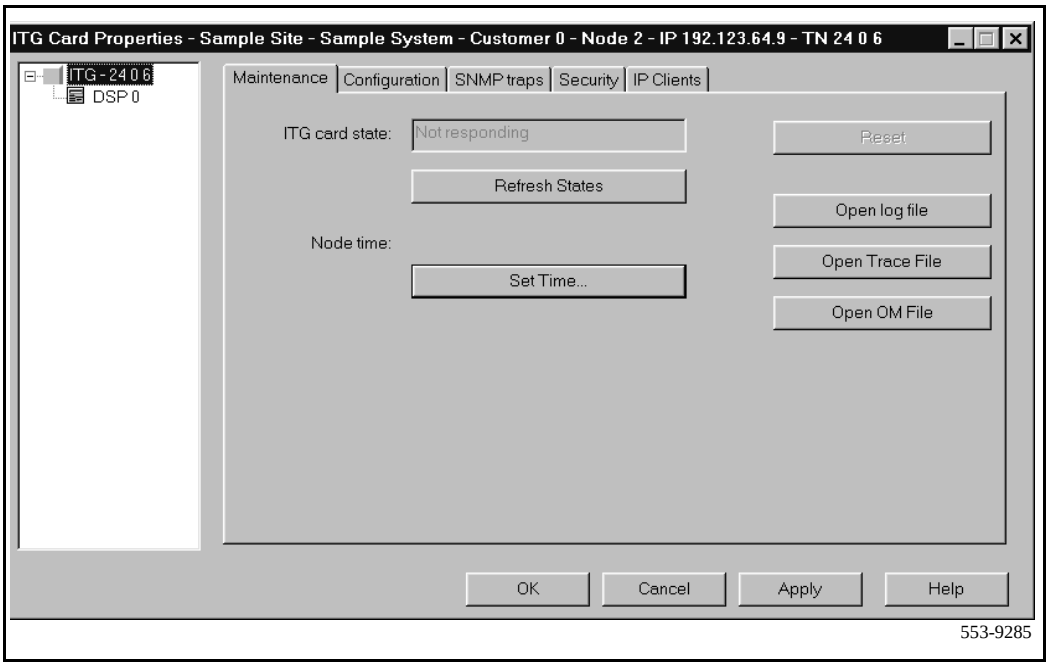
Configure the properties of each IP Line card

This procedure may be used before or after you physically install the IP Line 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:

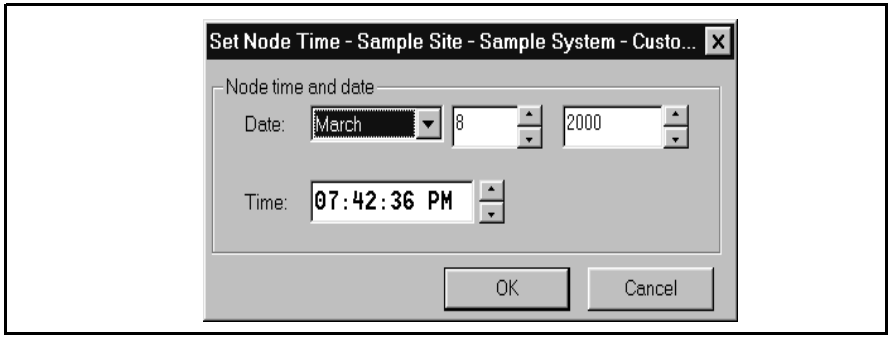
- If the cards are present and responding, all DSPs will appear in the left side of the window. On the “Maintenance” tab, “IP Line card state” will show “Unequipped.” On the Configuration tab, the “S/W release” will show the value actually read from the card.
- If the cards have not yet been physically installed, only DSP 0 will appear in the left side of the window. On the “Maintenance” tab, “IP Line card state” will show “Not responding.” On the Configuration tab, the “S/W release” will show nothing.

To configure the IP Line cards, do the following:

9 In the “IP Telephony Gateway” window, double-click on an IP Line card to display the “IP Line card Properties” window. Leave the IP Line card icon selected in the left side of the window.



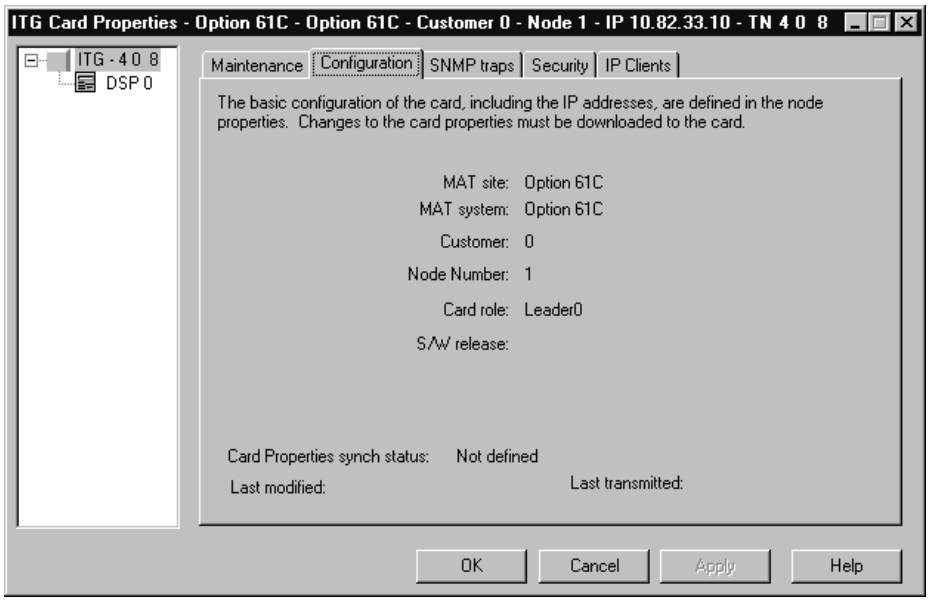
10 If the Leader 0 IP Line card is present and responding, set the time on the "Maintenance" tab of the card properties for Leader 0. If not, you must remember to come back and set the time on the Leader 0 card after the card is physically installed. Select the date and time from the list and click OK.



11 Click the **Configuration** tab.

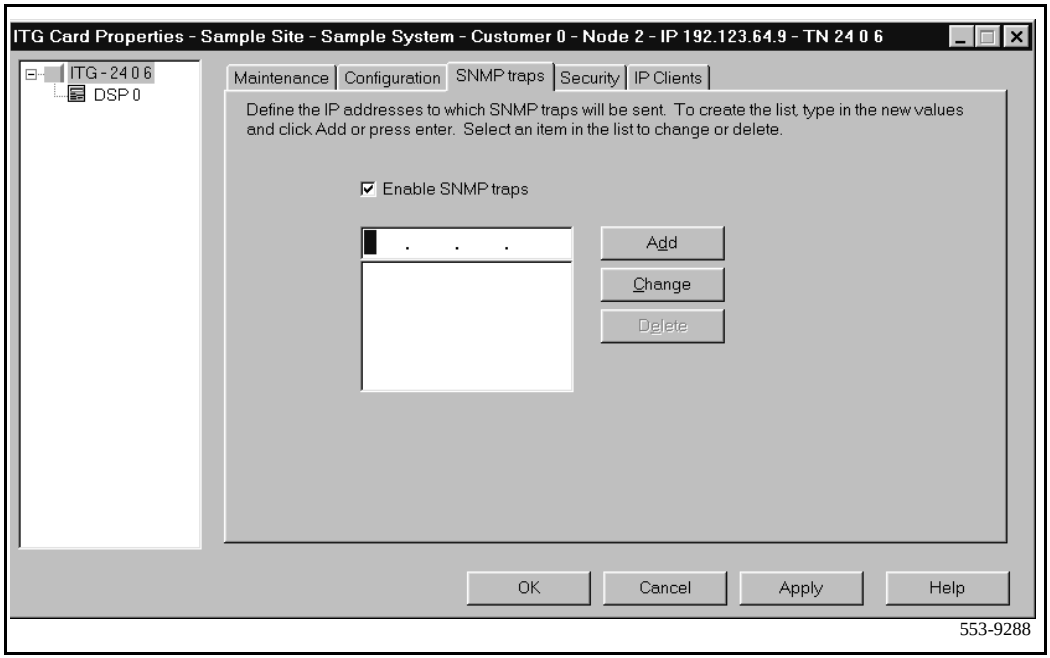
12 Verify that all cards in the same ITG node are running the same software version, and that the "S/W release" shows the latest recommended software version.

- If the software needs to be updated, refer to "Upgrading IP Line card software (if required)" on page 127.
- If the cards are not present and responding, you must remember to come back and verify the software version.


ITG Card Properties - Option 61C - Option 61C - Customer 0 - Node 1 - IP 10.82.33.10 - TN 4 0 8
ITG - 4 0 8
DSP 0
Maintenance
Configuration
SNMP traps
Security
IP Clients
The basic configuration of the card, including the IP addresses, are defined in the node properties. Changes to the card properties must be downloaded to the card.
MAT site: Option 61C
MAT system: Option 61C
Customer: 0
Node Number: 1
Card role: Leader0
S/W release:
Card Properties synch status: Not defined
Last modified:
Last transmitted:
OK
Cancel
Apply
Help

13 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.

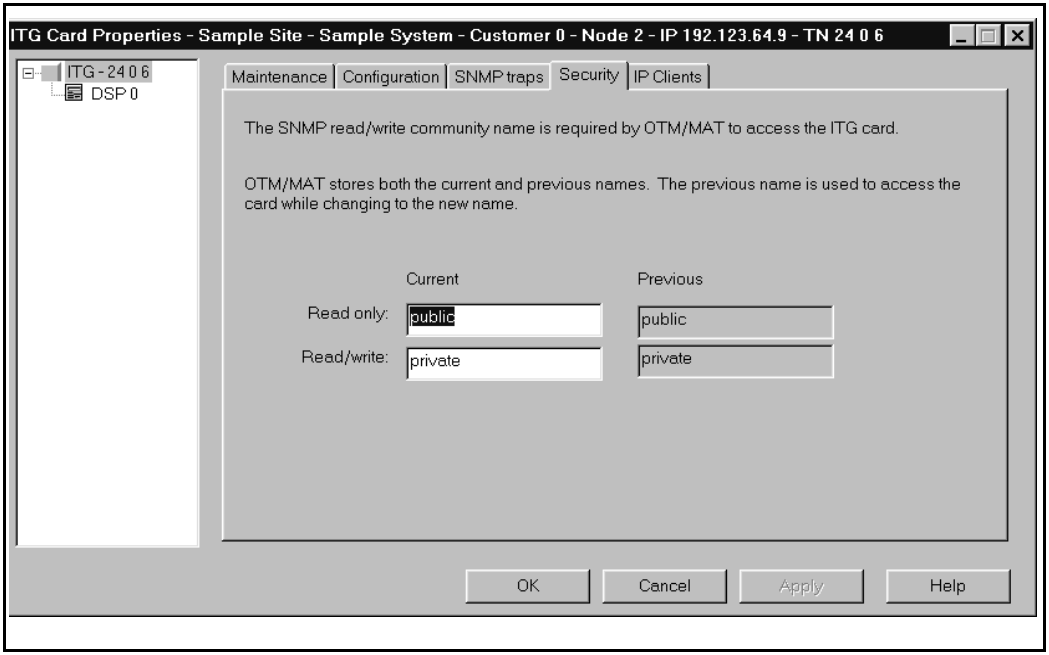


14 To add an SNMP Manager IP address, type the address in the entry field, and click **Add**. You should add SNMP Manager IP addresses for:

- 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. You must change the community names from the defaults in order to provide better security for the ITG node. MAT ITG uses this SNMP community name to refresh the node status, and to control the transmitting and retrieving of files.

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



16 Click the **IP Clients** tab.

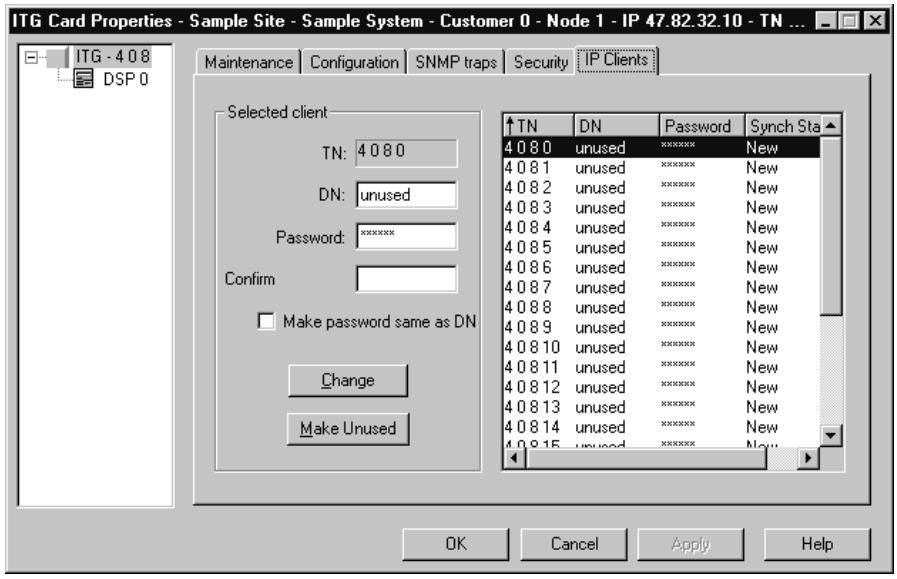
The "IP Clients" tab is used to define the DN and password for each of the 24 configured TNs on the IP Line card. The list of TNs is built by MAT when the card is added via the Node Properties. This MAT configuration must be coordinated with the overlay 11 Meridian 1 configuration.

17 Select the first TN in the list.

18 Enter the "DN" and "Password" fields. Check the "Make password same as DN" field if the default password is to be the DN.

19 Click the **Change** button then **Apply**.
The "Synch status" becomes "Changed."

20 Repeat the DN and password configuration for each TN in the list.



21 From the ITG shell use the command **shellPasswordSet** to change the default user ID and password for Telnet to ITG shell and FTP to the IP Line card file system. The default user ID is **itgadmin** and the default password is **itgadmin**.

Configure IP Line card DSP properties

Note: The properties of all DSPs on an IP Line card are modified by configuring the properties for "DSP 0" on an IP Line card.

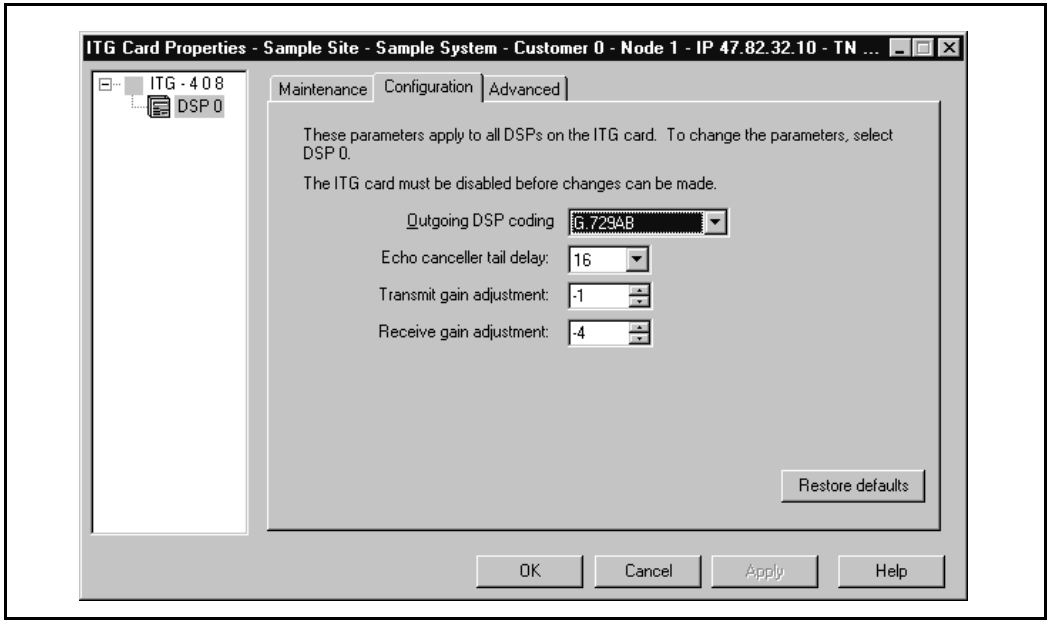
CAUTION

The default DSP parameters for the 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.

22 Click to select the **DSP 0** icon underneath the IP Line card.

23 Click the **Configuration** tab.

24 Select the “G.729 Annex AB" codec from the “DSP coding algorithm” pull-down menu.



25 Click **Apply** then **OK**.

26 Repeat the previous steps to configure the card and DSP properties for each IP Line card.

What to do next?

Once you have completed the configuration of the card properties, you will proceed to “Transmit card properties and Gatekeeper properties” on page 122.

Transmit card properties and Gatekeeper properties

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

When you configure or change passwords in the IP Clients tab but do not change other Card Properties, you must transmit the Gatekeeper Properties file only.

When you make a change to Card Properties but not to the passwords in the IP Clients tab, you must transmit the Card Properties file only.

When you configure or change passwords in the IP Clients tab and make other changes to Card Properties, you must transmit both the Gatekeeper Properties file and Card Properties files.

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 IP Line 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.”

Note: If you are attempting to transmit the Card Properties for a new ITG node from a remote MAT ITG PC and if the card is unable to communicate back to the remote MAT ITG PC through the voice gateway, you may be able to establish a connection through the management gateway by connecting to the ITG maintenance port and use the ITG shell 'routeAdd' command and add a new route that points to the MAT ITG PC. This step must be repeated every time a card is reset until the card properties (containing the SNMP Manager IP addresses) have been successfully transmitted to the card.

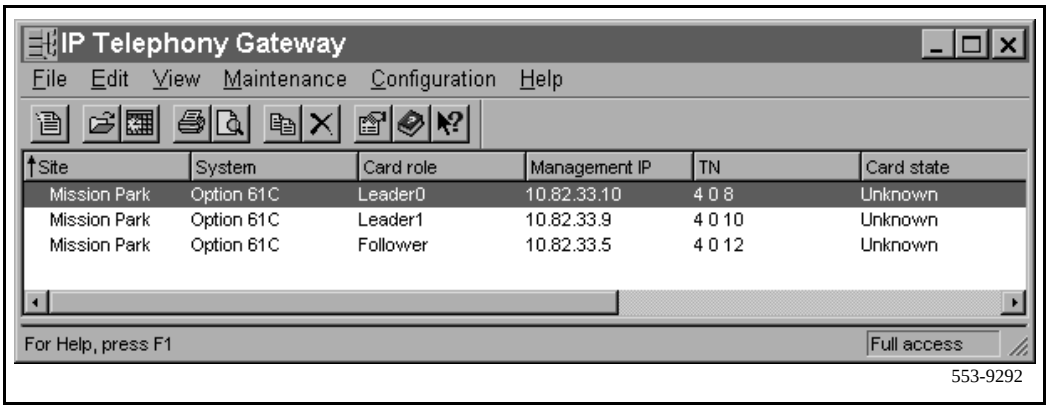
For Telnet to the ITG shell and FTP to the ITG card file system, the default user name is **itgadmin** and the default password is **itgadmin**.

The syntax for the routeAdd command is:

routeAdd "xxx.xxx.xxx.xxx","yyy.yyy.yyy.yyy"

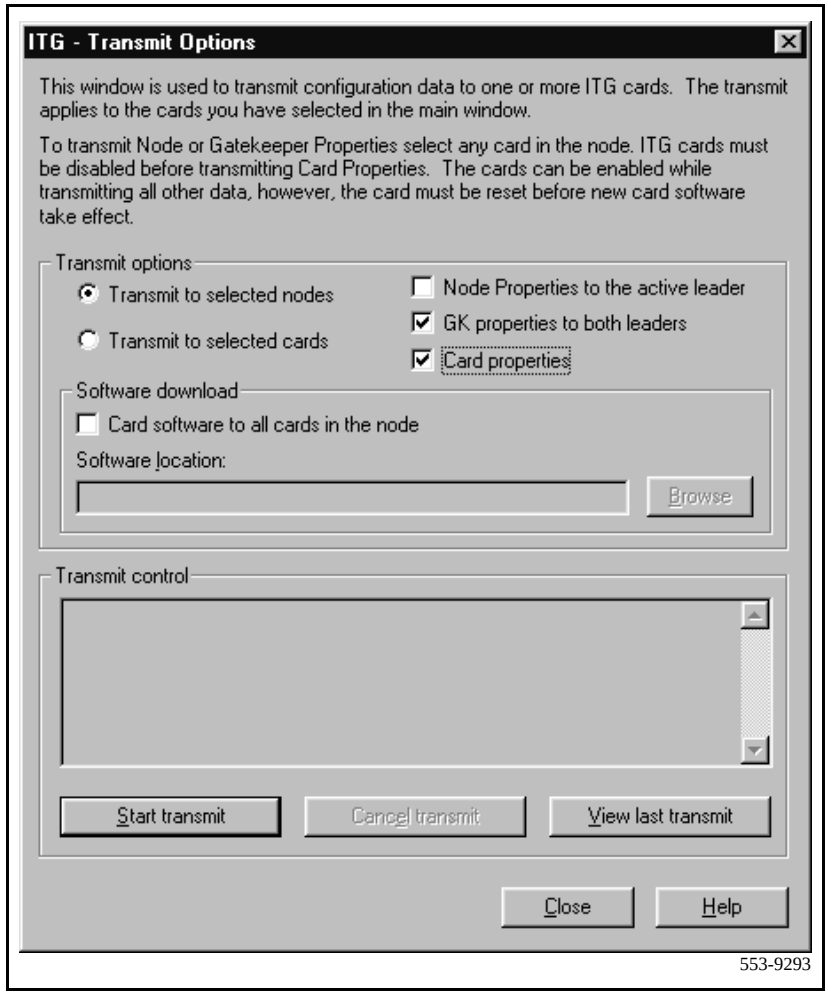
Where: xxx.xxx.xxx.xxx is the host address of the remote MAT ITG PC, and yyy.yyy.yyy.yyy is the IP address of the local E-LAN management gateway. The xxx.xxx.xxx.xxx and yyy.yyy.yyy.yyy parameters must be enclosed by double quotes and separated by a comma.

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



28 Click **Configuration** | **Synchronize** | **Transmit.**

The “ITG - Transmit Options” window appears.



29 Leave the radio button defaulted to “Transmit to selected nodes”. Check the "GK properties to both leaders", and “Card properties” boxes.

30 Click the **Start Transmit** button.

The transmission status is displayed in the “Transmit control” box. Confirm that card properties are transmitted successfully.

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

32 Use the overlay 32 ENLC command to re-enable the IP Line cards.

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

34 Verify the TN, management interface MAC address, and IP addresses for each IP Line card. Compare the displayed values with those on the IP Line card Installation Summary Sheet.

Once the Card Properties have been successfully transmitted, the new Card Properties are automatically applied to each card. The ITG node is now ready to make test calls as soon as the Meridian 1 configuration is performed.

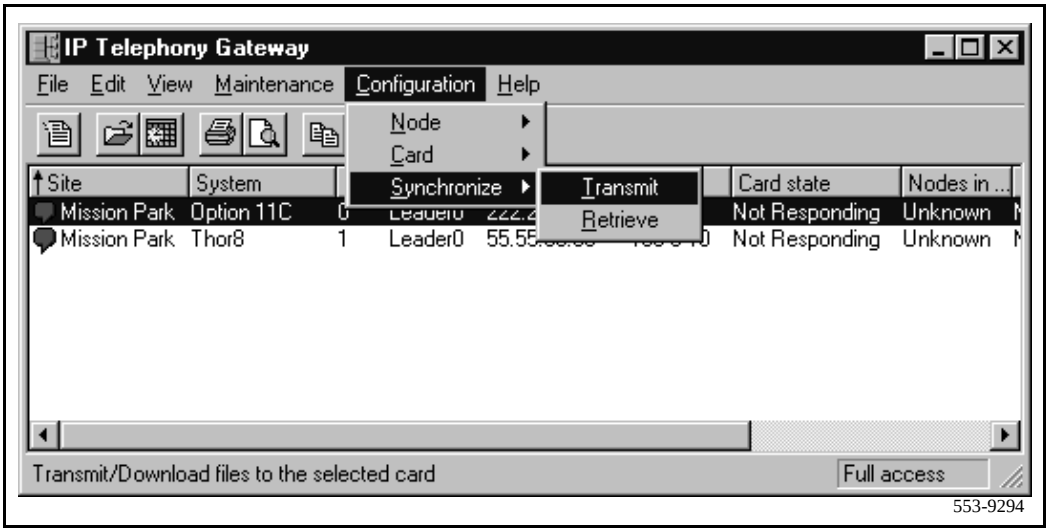
Verifying card software

In the IP Telephony Gateway window, starting with the Leader 0 IP Line card, double-click each IP Line card to open the IP Line card Properties window. Leave the default selection of the IP Line 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 IP Line card is the latest recommended software release for the card. The website URL to check the latest recommended IP Line card software release is "https://www.nortelnetworks.com/entprods/cts/option11c/". If any of the cards require a software upgrade, refer to the next procedure, *Upgrading IP Line card software*.

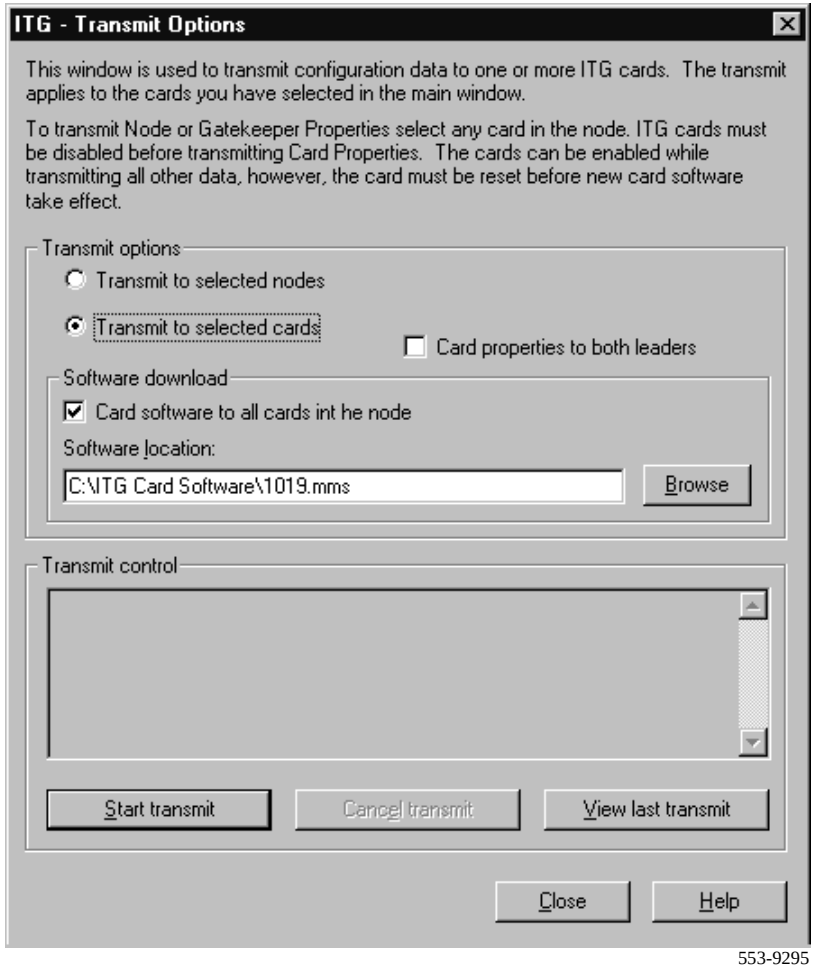
Upgrading IP Line card software (if required)

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:
   https://www.nortelnetworks.com/entprods/cts/option11c/
   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 "IP Telephony Gateway" application, if not already opened.
3. Verify the current software version of the IP Line 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 IP Line 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 IP Line 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**.



8 An “ITG - Transmit Options” dialog box is displayed.



553-9295

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

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

11 Click on the **Browse** button to locate the IP Line 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 IP Line card software appears in the edit box next to the "Browse" button.

12 Click on the **Start Transmit** button to begin the IP Line card software upgrade process.

The software is transmitted to each card in turn, and burned into the flash ROM on the IP Line 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 IP Line card. The cards continue to run the old software until they are rebooted.

13 Reboot each IP Line 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 IP Line cards have been reset and have successfully rebooted and are responding again to the MAT ITG status refresh (disabled: active; disabled: backup; disabled).

Note: These cards must remain in the "Disabled" state after the upgrade, so that the technician can issue a "Reset" command from the Maintenance menu or the "Maintenance" tab in the "IP Line 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.

14 Double-click each upgraded card and verify the software version on the "Configuration" tab of the Card Properties.

15 Use the overlay 32 ENLC command to re-enable the IP Line cards.

The software upgrade procedure is complete.

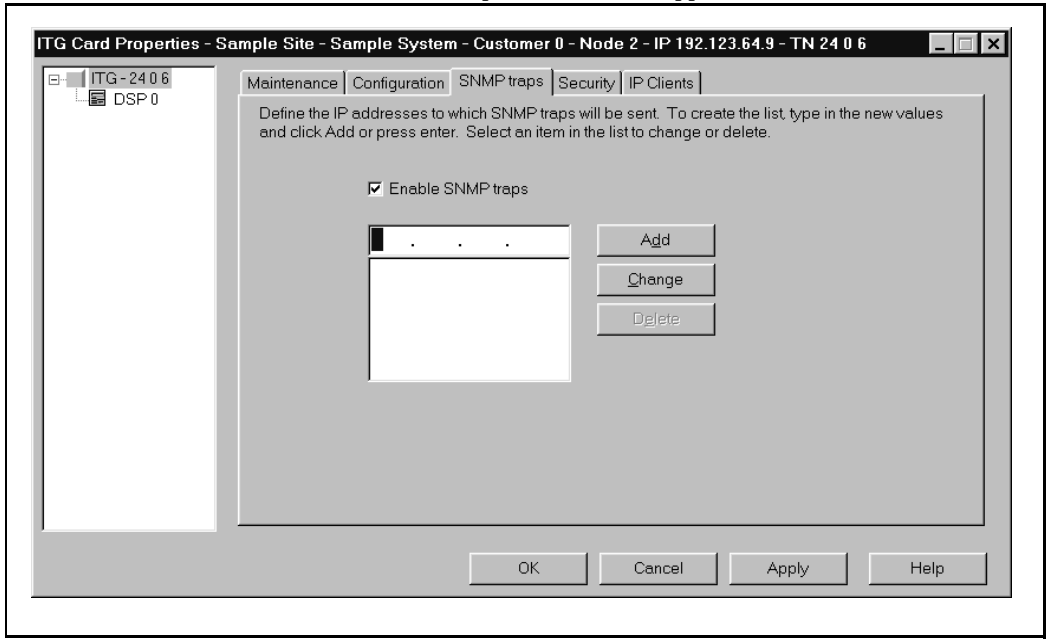
Activate SNMP traps for IP Line cards

Define and activate SNMP traps with the following procedure:

1 Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.

2 Double-click an IP Line card to define the SNMP traps for that card.

3 The "ITG Card Properties" window appears. Click the **SNMP traps** tab.



4 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:

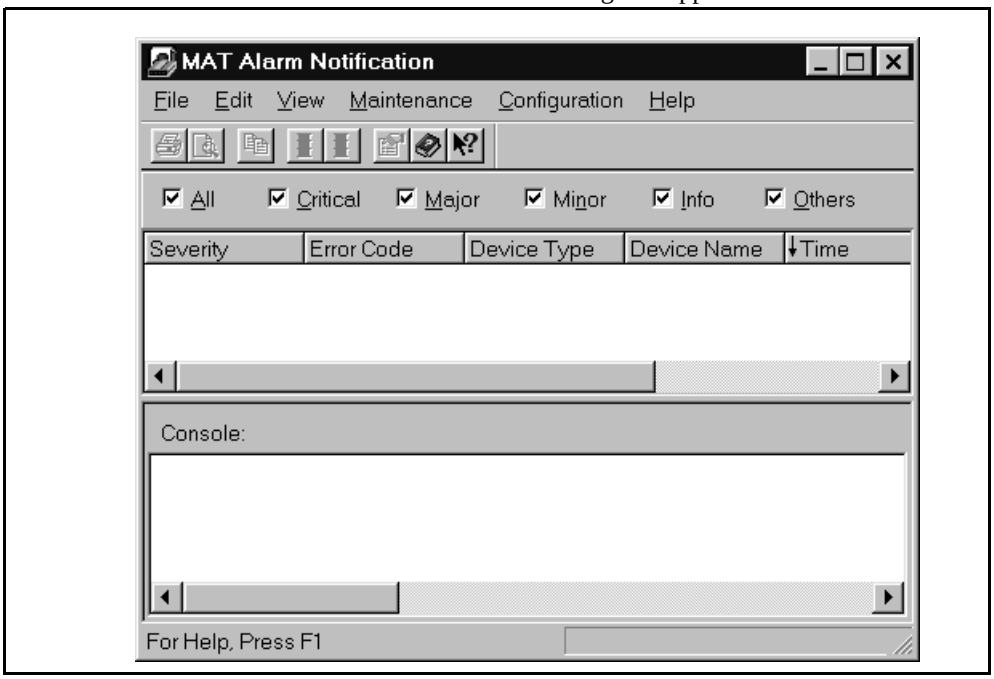
- the local MAT PC
- PPP IP address configured in the Netgear RM356 Modem Router, or equivalent, on the E-LAN for the remote support MAT PC
- the SNMP manager for remote alarm monitoring via SEB2 and IRIS nGEN (if present).
- Any remote MAT PCs on the customer's IP network

5 Repeat the definition of SNMP traps for each IP Line card.

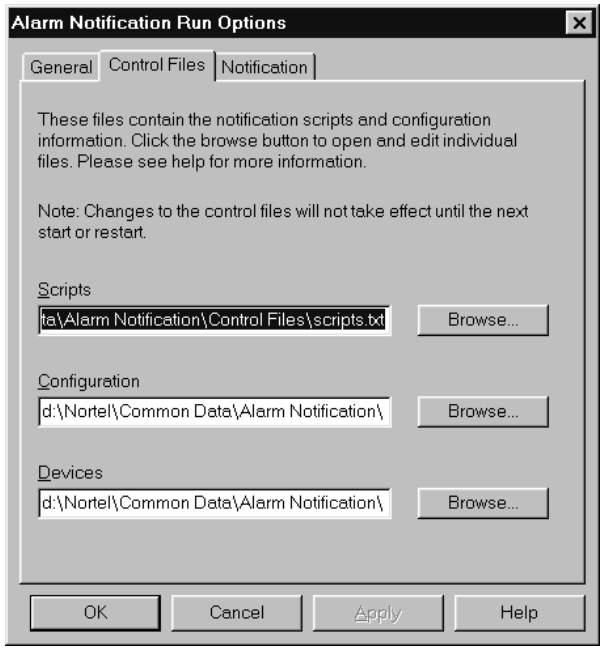
6 Return to the "MAT Navigator" window.

7 In the MAT Navigator window select **Utilities | Alarm Notification**.

The "MAT Alarm Notification" dialog box appears.

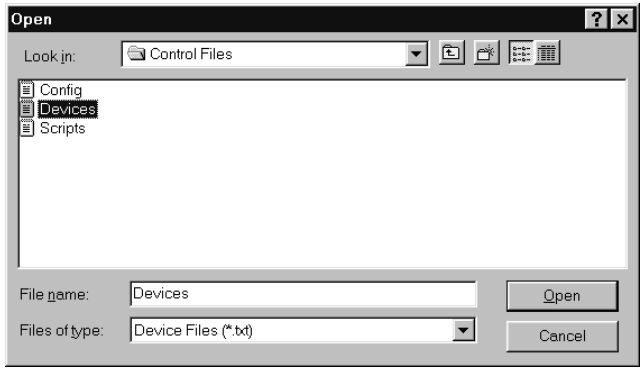


8 Select **Configuration | Run Options**. The "Alarm Notification Run Options" dialog box appears. Click the **Control Files** tab.

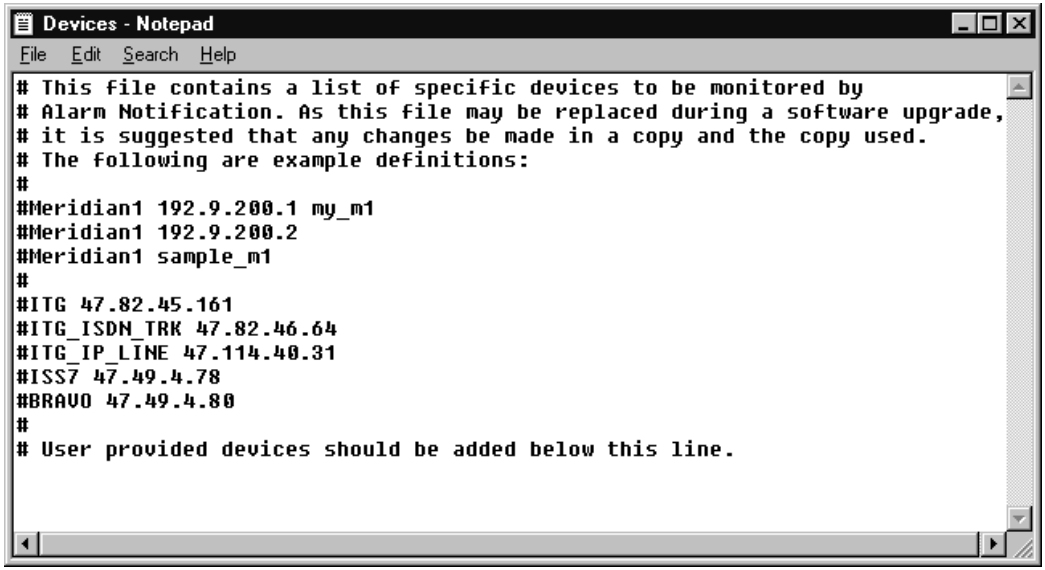


9 Click **Devices | Browse**. The "Open" dialog box appears.

10 Select the "Devices.txt" file from the "Control Files" folder and click **Open**.



The "Devices.txt" file opens as follows:



11 For each IP Line card in each monitored IP Line card node, add a line consisting of three fields separated by spaces, as shown in Table 9. Enter the first line under the last line that begins with a "#".,

Table 9
Format of Devices.txt file

Device Type	IP Address	Device Name
ITG_IP_LINE	xxx.xxx.xxx.xxx	Site_Leader_0
ITG_IP_LINE	xxx.xxx.xxx.xxx	Site_Leader_1
ITG_IP_LINE	xxx.xxx.xxx.xxx	Site_Follower_2

12 Click **File | Save**.

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

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

14 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.

15 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.

16 Enter the **torpedoing** command from the ITG shell. A series of SNMP traps is emitted by the IP Line card and appears in the MAT Alarm Notification browser window. Verify the device name identifies the correct IP Line card.

The procedure is complete.

Enable the IP Line cards via overlay 32 on Meridian 1

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

2 Repeat the above step for each IP Line card.

Make test calls to and from IP Telecommuter clients

Make test calls to ensure that the IP Telecommuter system can process calls to and from clients, and that quality of service is acceptable. Check the IP Telecommuter operational report, as described in the *Administration* chapter.

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.

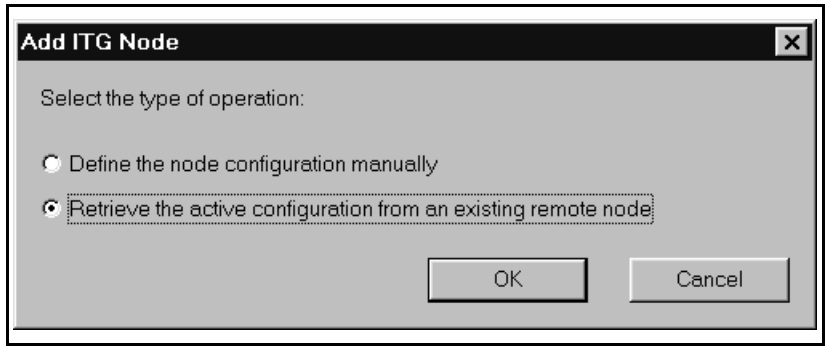
> ***Note:*** If multiple MAT ITG PCs are used to manage the same ITG network, care must be taken to synchronize the different copies of the ITG database. The MAT ITG **Configuration|Synchronize|Retrieve** function can be used to synchronize the MAT ITG database with the database on the ITG node.

Configuring the node and Leader 0

1 Launch the Meridian Administration Tools application on the MAT PC and double-click the ITG IP Telecommuter icon.

2 In the “IP Telephony Gateway - IP Telecommuter ” window, click the **Configuration** | **Node** | **Add**.

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



4 In the “Retrieve ITG Node” window, select the MAT Site, MAT System, Customer and Node. .

Note: The site name, Meridian 1 system name, and Meridian 1 customer number must exist in MAT 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.

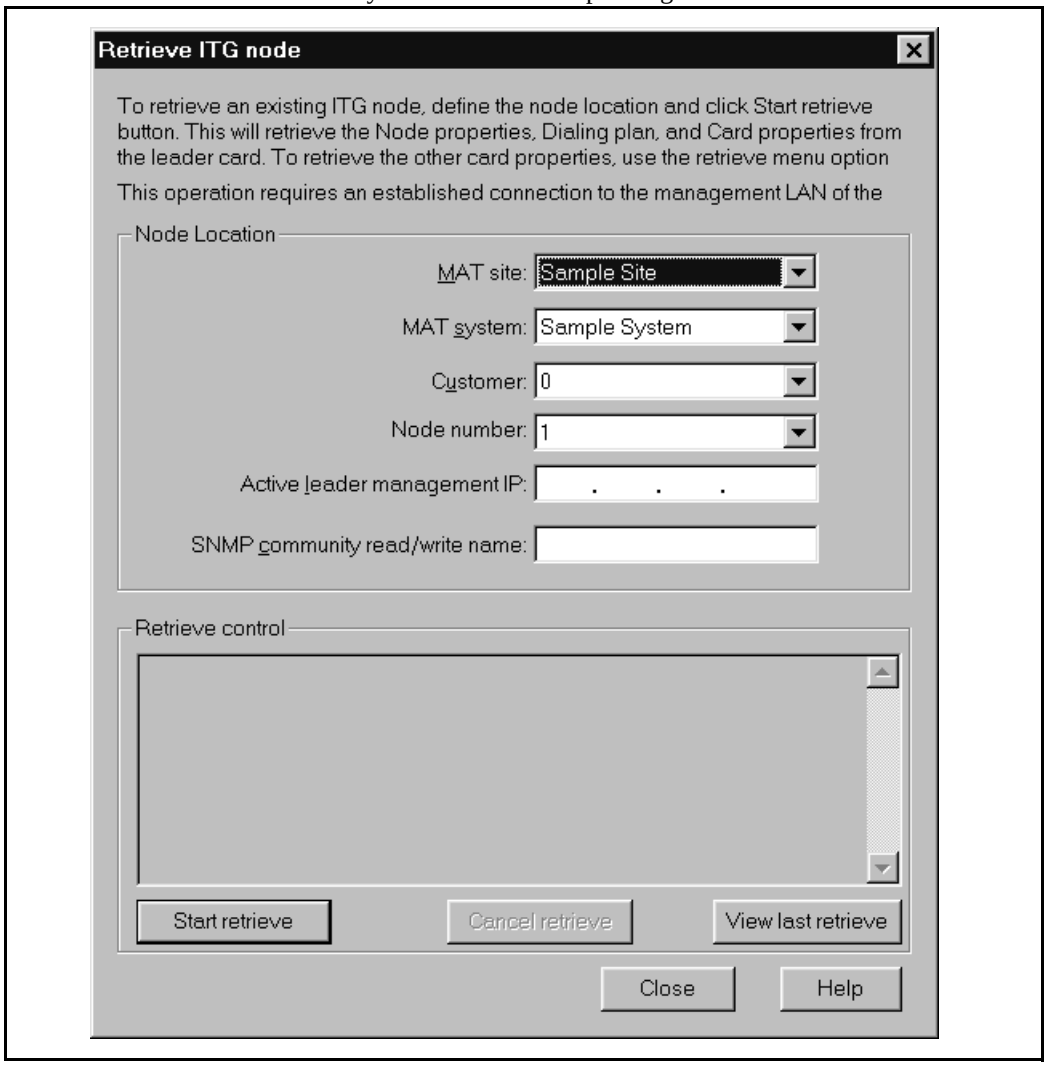
6 Enter the SNMP read/write community name. The default is “private”.

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 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 IP Line cards to the node

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

11 Use the **Configuration|Synchronize|Retrieve** command to retrieve the card properties for all IP Line cards in the selected node.

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

Add a “dummy” node to retrieve and view ITG node configuration

Use this procedure 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 technician 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 IP Line 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 and double-click on ITG IP Telecommuter icon. The "IP Telephony Gateway - IP Telecommuter" window opens.
2. In the "IP Telephony Gateway - IP Telecommuter" window, select Leader 0 or any card from the node.
3. In the "IP Telephony Gateway - IP Telecommuter" window, click the **Configuration** | **Synchronize** | **Retrieve.**

The “ITG - Retrieve Options” 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 IP Line 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,” "GK Properties" and “Card Properties,” if the MAT ITG data is out of date and you intend to synchronize all MAT ITG node data with the data from the IP Line 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,” "GK Properties" and “Card Properties,” will over-write the existing MAT ITG configuration data for the respective node or card.

The “Retrieving the ITG configuration information from the ITG node” procedure is complete.

Configure a modem router on the E-LAN for remote access to the ITG node

Management and support of the ITG network depend on IP networking protocols including SNMP, FTP, and Telnet. A modem router should be installed on the Meridian 1 site LAN (called the embedded LAN or E-LAN as opposed to the customer's enterprise network or C-LAN) in order to provide remote support access for ITG and other IP-enabled Nortel Networks products. The Bay Networks Netgear RM356 modem router integrates the functions of a V.90 modem, a PPP remote access server, an IP router, and a 4-port 10BaseT Ethernet hub, and provides a range of security features that may be configured so as to comply with the customer's data network security policy.

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

Security features of the RM356 modem router:

- Password Authentication Protocol (PAP) for dial-in PPP connection.
- RM356 manager password.
- CLID for dial-in user authentication (requires C.O. line with Calling Line ID).
- Callback for dial-in user authentication.
- Dial-in user profiles
- Static IP routing
- IP Packet Filtering
- Idle timeout disconnect for dial-in PPP connection.

Physical installation of the RM356 modem router

1. Place the modem router at a conveniently visible and physically secure location near an AC power outlet, an analog telephone line, and 10BaseT Ethernet cables. Up to four hosts or hubs can be connected to the integrated 10BaseT hub in the rear of the RM356 modem router. Use shielded Cat5 10BaseT Ethernet cables to connect the modem router to the Management interface of up to four ITG cards. Other IP-enabled Nortel Networks products on the E-LAN may be connected to the RM356 modem router, including the Meridian 1, a local MAT PC, Symposium Call Center Server, and Call Pilot.

   Note: The up-link connection to an additional E-LAN hub or optional C-LAN gateway requires either a cross-over 10BaseT Ethernet cable, or a special up-link port on the 10BaseT hub to which the RM356 is connected.

2. When the modem router is connected to the AC power source, the power LED is lit. After several seconds, the test LED flashes slowly four times, then stays off. For each of the four 10BaseT ports on the integrated hub there is a link/data LED that is lit steadily to indicate a good received link if there is a cable connection to a host or hub that is powered up, or flashing to indicate data received on the LAN.

3. Connect the RJ45 plug end of the local manager cable to the RS232 Manager port RJ45 jack on the rear of the modem router. Connect the other end of the cable to an RS232 terminal or PC COM port configured for the following communication parameters: 9600 bps, 8, none, and 1. The local maintenance cable connects directly to data terminal equipment (DTE).

4. The analog telephone line should be a Central Office (CO) line or an extension with a Direct Inward Dialing (DID) number if that is in compliance with the customer's network security policy.

Configure the RM356 modem router by the manager menu

Configuring the RM356 modem router by the manager menu can be completed from a terminal or PC connected to the local RS232 manager port on the rear of the modem router. Alternatively the manager menu can be accessed by Telnet after the IP addressing and routing have been set up initially from the local manager port.

Note: The arrow keys navigate in the RM356 manager menu. The spacebar key toggles pre-defined configuration values for a field. The Enter key saves data changes to ROM and exits the current menu. The Esc key exits the current menu without saving changes. Enter menu selection number when prompted to display a sub-menu, configuration form, or command prompts.

1 Press the **Enter** key.

The 'Enter Password:' prompt is displayed for 10 seconds.

2 Enter the default RM356 manager password: 1234

The "RM356 Main Menu" is displayed.

3 Enter menu selection number 1 to access "General Setup" under the "Getting Started" section of the "RM356 Main Menu."

"Menu 1 General Setup" is displayed.

4 Type in the system name(19 characters, no spaces), location, and contact person's name for the Meridian 1 site. Use the up and down arrow keys to move the cursor to the prompt "Press ENTER to Confirm or ESC to Cancel:"at the bottom of the menu . Press Enter to confirm and save data to ROM.

5 Enter menu selection number 2 under the "Getting Started" section.

"Menu 2: Modem" is displayed.

6 Type in modem name. Set "Active=Yes". Use arrow keys to navigate and space bar to toggle values. Set "Direction=Incoming". Type in the modem router's telephone number for reference. Press Enter to confirm and save data to ROM.

7 Enter menu selection number 3, "Ethernet Setup", under the "Getting started" section.

"Menu 3: Ethernet Setup" sub-menu is displayed.

8 Enter menu selection 2, "TCP/IP and DHCP Setup".

"Menu 3.2 - TCP/IP and DHCP Ethernet Setup" is displayed.

9 Use the space bar to toggle "DHCP=None".

10 Under "TCP/IP Setup", type in the IP address and the IP subnet mask for the modem router's Ethernet interface on the E-LAN.

11 Toggle "RIP Direction=None". Press Enter to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

12 Enter menu selection number 12, "Static Routing Setup", under the "Advanced Applications" section.

"Menu 12 - Static Route Setup" sub-menu is displayed.

Note: If firewall security is properly configured in the customer's Management GW router, and if the modem router is permitted access over the C-LAN to other ITG nodes on remote E-LANs, define a default network route pointing to the Management GW IP address on the local E-LAN. Alternatively, define up to four different static network routes or host routes in the modem router to limit routing access from the modem router to the C-LAN.

Note: To prevent access from the modem router to the C-LAN via the Management GW router on the E-LAN , disable RIP by setting "RIP Direction=None", and remove all static routes or disable a particular static route by setting "Active=No".

13 Enter menu selection number 1 to edit the first static route.

"Menu 12.1 - Edit IP Static Route" is displayed.

14 Type in a descriptive route name e.g. "DefaultGW" (no spaces). Toggle "Active=Yes/No" for security purposes. The gateway IP address is the Management GW IP address on the E-LAN where the modem router is connected. " Press Enter to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

15 Enter menu selection number 13, "Default Dial-in Setup", under the "Advanced Applications" section.

"Menu 13 - Default Dial-in Setup " is displayed.

16 Under "Telco Options" toggle "CLIDAuthen=None/Preferred/Required".

CLID requires a C.O. line subscribed for CLID service where available. "Preferred" means some dial-in user profiles may require CLID, but others may not. "Required" means no dial-in call is connected unless CLID is provided and user profiles require CLID for authentication.

Under "PPP Options" toggle "Recv Authen=PAP". Windows 9x Dialup Networking (DUN) is not compatible with CHAP/PAP or CHAP on the modem router: calls are disconnected after a few minutes.

Toggle "Compression=No". Windows 9x DUN is not compatible with software compression on the modem router: calls are randomly disconnected.

Toggle "Mutual Authen=No".

Under "IP Address Supplied By:" Toggle "Dial-in User=No", "IP Pool=Yes". For "IP Start Addr=" type in the E-LAN IP address that will be assigned to the Dialup Networking (DUN) PPP client on the remote MAT PC.

Note: The remote MAT PC will receive this E-LAN IP address whenever DUN makes a dial-in PPP connection to the modem router. As long as DUN remains connected to the modem router, IP applications on the remote MAT PC function as if the PC were located on the customer's E-LAN.

Under "Session Options" configure input and output filter sets according to the customer's IP network security policy and practices. The default setting is no filter sets. Set "Idle Timeout=1200" seconds to provide 20 minutes idle timeout disconnect for remote support purposes.

Press Enter to confirm and save data to ROM.

17 Enter menu selection number 14, "Dial-in User Setup", under the "Advanced Applications" section.

"Menu 14 - Dial-in User Setup " is displayed.

Note: Up to eight dial-in user profiles may be defined according to the customer's network security policy.

18 Enter menu selection 1 to edit the first dial-in user profile.

"Menu 14.1 - Edit Dial-in User" is displayed.

19 Type in the user name. Toggle "Active=Yes/No" for security purposes. Type in a password for PAP. The DUN client on the remote MAT PC must provide the user name and password defined here when dialing up the modem router.

Set "Callback=Yes/No" according to the customer's network security policy and practices. Nortel Networks Customer Technical Services (CTS), does not currently accept callback security calls from the modem router.

Set "Rem CLID=" to the PSTN Calling Number that is displayed when the remote MAT PC dials up the modem router, if CLID authentication is required for the user profile. CLID depends on providing a C.O. line subscribed for CLID service for the modem router's telephone line connection.

Set "Idle Timeout=1200" seconds to provide 20 minutes idle timeout disconnect for Nortel Networks remote support purposes.

Press Enter to confirm and save data to ROM, then press Esc to return from the sub-menu to the main menu.

20 Enter menu selection number 23 to access "System Password" under the "Advanced Management" section of the "RM356 Main Menu."

"Menu 23 - System Password" is displayed.

21 Type in the old password and new password, then retype the new password to confirm. Never leave the RM356 system manager password defaulted to 1234 after the modem router has been installed and configured on the E-LAN. The modem router's security features are worthless if the manager password is not changed regularly according to good network security practices.

RM356 modem router manager menu (application notes on Meridian 1 E-LAN installation)

This section displays the various menus of the RM356 modem router:

```
                        RM356 Main Menu

Getting Started                     Advanced Management
  1. General Setup                21. Filter Set Configuration
  2. MODEM Setup
  3. Ethernet Setup                 23. System Password
  4. Internet Access Setup          24. System Maintenance

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  13. Default Dial-in Setup
  14. Dial-in User Setup                99. Exit

                    Enter Menu Selection Number:

                       Menu 1 - General Setup

                  System Name= Room_304_RCH_Training_Center
                  Location= Sherman Ave., Richardson, TX
                Contact Person's Name= John Smith, 972 555-1212

                  Press ENTER to Confirm or ESC to Cancel:

                       Menu 2 - MODEM Setup

                  Modem Name= MODEM
                  Active= Yes
                  Direction= Incoming
                  Phone Number=
                  Advanced Setup= No
```

```
                    Press ENTER to Confirm or ESC to Cancel:

                              Menu 3 - Ethernet Setup

                    1. General Setup
                    2. TCP/IP and DHCP Setup

                          Enter Menu Selection Number:

                        Menu 3.1 - General Ethernet Setup

                    Input Filter Sets= 2
                    Output Filter Sets=

                    Press ENTER to Confirm or ESC to Cancel:

                    Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                    DHCP Setup:
                      DHCP= None
                      Client IP Pool Starting Address= N/A
                      Size of Client IP Pool= N/A
                      Primary DNS Server= N/A
                      Secondary DNS Server= N/A

                    TCP/IP Setup:
                      IP Address= 47.177.16.254
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= None
                        Version= RIP-2B

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
                    Menu 12 - Static Route Setup

                  1. DefaultGW
                  2. _________
                  3. _________
                  4. _________

                      Enter Menu Selection Number:

                   Menu 12.1 - Edit IP Static Route

                  Route #: 1
                  Route Name= DefaultGW
                  Active= Yes
                  Destination IP Address= 0.0.0.0
                  IP Subnet Mask= 0.0.0.0
                  Gateway IP Address= 47.177.16.1
                  Metric= 2
                  Private= No

                  Press ENTER to Confirm or ESC to Cancel:

                    Menu 13 - Default Dial-in Setup

 Telco Options:                    IP Address Supplied By:
   CLID Authen= None                  Dial-in User= No
                                      IP Pool= Yes
PPP Options:                       IP Start Addr= 47.177.16.253
   Recv Authen= PAP
   Compression= No                       Session Options:
   Mutual Authen= No                       Input Filter Sets=
     PAP Login= N/A                        Output Filter Sets=
     PAP Password= N/A                     Idle Timeout= 1200

 Callback Budget Management:
   Allocated Budget(min)=
```

```
       Period(hr)=

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                          Menu 14 - Dial-in User Setup

                    1. itgadmin
                    2. _________
                    3. _________
                    4. _________
                    5. _________
                    6. _________
                    7. _________
                    8. _________

                          Enter Menu Selection Number:

                          Menu 14.1 - Edit Dial-in User

                    User Name= itgadmin
                    Active= Yes
                    Password= ********
                    Callback= No
                      Phone # Supplied by Caller= N/A
                      Callback Phone #= N/A
                    Rem CLID=
                    Idle Timeout= 500

                    Press ENTER to Confirm or ESC to Cancel:
```

```
                    Menu 21 - Filter Set Configuration

   Filter                                  Filter
   Set #        Comments                   Set #        Comments
   ------  -----------------               ------  -----------------
     1      NetBEUI_WAN                      7      _________________
     2      NetBEUI_LAN                      8      _________________
     3      _________________                9      _________________
     4      _________________               10      _________________
     5      _________________               11      _________________
     6      _________________               12      _________________


                  Enter Filter Set Number to Configure= 0

                  Edit Comments=

                  Press ENTER to Confirm or ESC to Cancel:

                      Menu 21.1 - Filter Rules Summary

# A Type                        Filter Rules              M m n
- - ---- ------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0           N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=138, DA=0.0.0.0           N D N
3 Y IP   Pr=17, SA=0.0.0.0, SP=139, DA=0.0.0.0           N D N
4 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0            N D N
5 Y IP   Pr=6, SA=0.0.0.0, SP=138, DA=0.0.0.0            N D N
6 Y IP   Pr=6, SA=0.0.0.0, SP=139, DA=0.0.0.0            N D F

                Enter Filter Rule Number (1-6) to Configure:

                          Menu 23 - System Password

                  Old Password= ?
                  New Password= ?
```

```
                    Retype to confirm= ?

                     Enter here to CONFIRM or ESC to CANCEL:

                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  Terminal Baud Rate
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Software Update
                         8.  Command Interpreter Mode
                         9.  Call Control

                          Enter Menu Selection Number:

                    Menu 24.1 -- System Maintenance - Status

Port Status   Speed  TXPkts  RXPkts  Errs  Tx B/s  Rx B/s   Up Time
 1    Idle    0Kbps   16206   12790     0       0       0    0:00:00

     Total Outcall Time:     0:00:00

     Ethernet:                    Name: Room_304_RCH_Traini
       Status:  10M/Half Duplex  RAS S/W Version: V2.13 | 9/25/98
      TX Pkts: 135579          Ethernet Address:00:a0:c5:e0:5b:a6
       RX Pkts: 662866
       Collisions: 49

     LAN Packet Which Triggered Last Call:

                                  Press Command:

               COMMANDS: 1-Drop Port 1  9-Reset Counters   ESC-Exit
```

```
    Menu 24.2 -- System Maintenance - Change Terminal Baud Rate

Terminal Baud Rate: 9600

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                Menu 24.3 == System Maintenance - Log and Trace

                   1. View Error Log
                   2. Syslog and Accounting

                            Please enter selection:

   0     179754 PINI  INFO  SMT Session End
   1     179761 PP09  INFO  Password pass
   2     179761 PINI  INFO  SMT Session Begin
   3     179763 PINI  INFO  SMT Session End
   4     179772 PP09  INFO  Password pass
   5     179772 PINI  INFO  SMT Session Begin
   6     179775 PINI  INFO  SMT Session End
   7     179783 PP09  INFO  Password pass
   8     179783 PINI  INFO  SMT Session Begin
   9     179788 PINI  INFO  SMT Session End
  10     179796 PP09  INFO  Password pass
  11     179796 PINI  INFO  SMT Session Begin
  12     179798 PINI  INFO  SMT Session End
  13     179812 PP09  INFO  Password pass
  14     179812 PINI  INFO  SMT Session Begin
  15     179815 PINI  INFO  SMT Session End
  16     179830 PP09  INFO  Password pass
  17     179830 PINI  INFO  SMT Session Begin
  18      179834 PINI  INFO  SMT Session End
```

```
        Menu 24.3.2 -- System Maintenance - Syslog and Accounting

                    Syslog:
                    Active= No
                    Syslog IP Address= ?
                    Log Facility= Local 1

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                  Menu 24.4 - System Maintenance - Diagnostic

     MODEM                                  System
       1.  Drop MODEM                         21. Reboot System
       2.  Reset MODEM                        22. Command Mode
       3.  Manual Call
       4.  Redirect to MODEM

     TCP/IP
       11. Internet Setup Test
       12. Ping Host

                          Enter Menu Selection Number:

                    Manual Call Remote Node= N/A
                    Host IP Address= N/A

                Menu 24.7 -- System Maintenance - Upload Firmware

                    1. Load RAS Code
                    2. Load ROM File

                          Enter Menu Selection Number: 1
```

Administration

This section contains:

The ITG OA&M access is provided through:

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 165. The MAT ITG application is accessed by clicking the "ITG IP Telecommuter" 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 158.

Command Line Interface

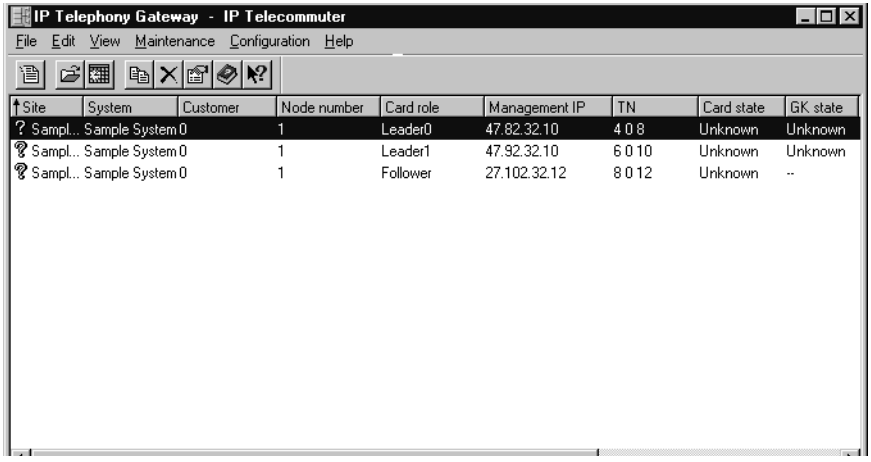
- The RS-232 MMI port on an IP Line card, which is connected directly to a VT-100 type terminal or to a PC running a terminal emulation program. Once connected, a command-line interface referred to as the ITG shell is available. ITG shell commands are described in "ITG shell command-line interface access via Telnet or maintenance port" on page 194, 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 201.
  The IP Line card uses the existing commands and messages used for the digital line (XDLC) card.

Basic interface of common MAT ITG windows

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



The “IP Telephony Gateway - IP Telecommuter” window lists all IP Line cards defined by the user. Information listed includes the card’s associated Site, System, Customer, IP/MAC addresses, TN, synch status, and the SNMP community name.

When the window is launched, the application sends an SNMP “get” message to the IP Line card. The application uses the SNMP community name stored for each card. If the SNMP “get” message is successful, it retrieves the card states and displays this information. If the “get’ message is unsuccessful, the card state field indicates this condition, and an alarm icon is displayed in the first column.

"IP Telephony Gateway - IP Telcommuter" 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 IP Line card.

Card state •Card state received from the card from SNMP.
Card state can be:

- "Enabled": enabled via the overlays. Leader cards have Active/Standby appended.
- "Disabled": disabled via the overlays. Alarm icon is displayed in the list.
- "Not responding": card does not respond to the SNMP get or MAT has an invalid community name. Alarm icon is displayed in the list.
- "Not equipped": card is responding, but no units have been configured in the overlays. Alarm icon is displayed in the list.
- "Unknown": the ITG window has automatic refresh turned off and the card has never been refreshed manually. A question mark icon is displayed.

GK state Gatekeeper state received from the card from SNMP. The GK state is the same as the card state of the leader cards on which they reside. This includes the Active/Standby status. There is one exception: when an external Gatekeeper is used, the GK state is set to "External GK" regardless of the leader card state.

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

- "Undefined": a new IP Line card has been added in "ITG node properties," but the card properties have not been configured.
- "Transmitted": the node properties has been transmitted to the Leader card from MAT successfully.
- "New": a new IP Line 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 IP Line card has been deleted from the "ITG Node Properties" window, but not download to the Leader card has occurred.

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

- "Transmitted": the GK properties has been transmitted to the Leader card from MAT successfully.
- "New": a new ITG node has been added, but the Gatekeeper properties have not been transmitted.
- "Changed": the Gatekeeper properties have been changed, but have not been transmitted.

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

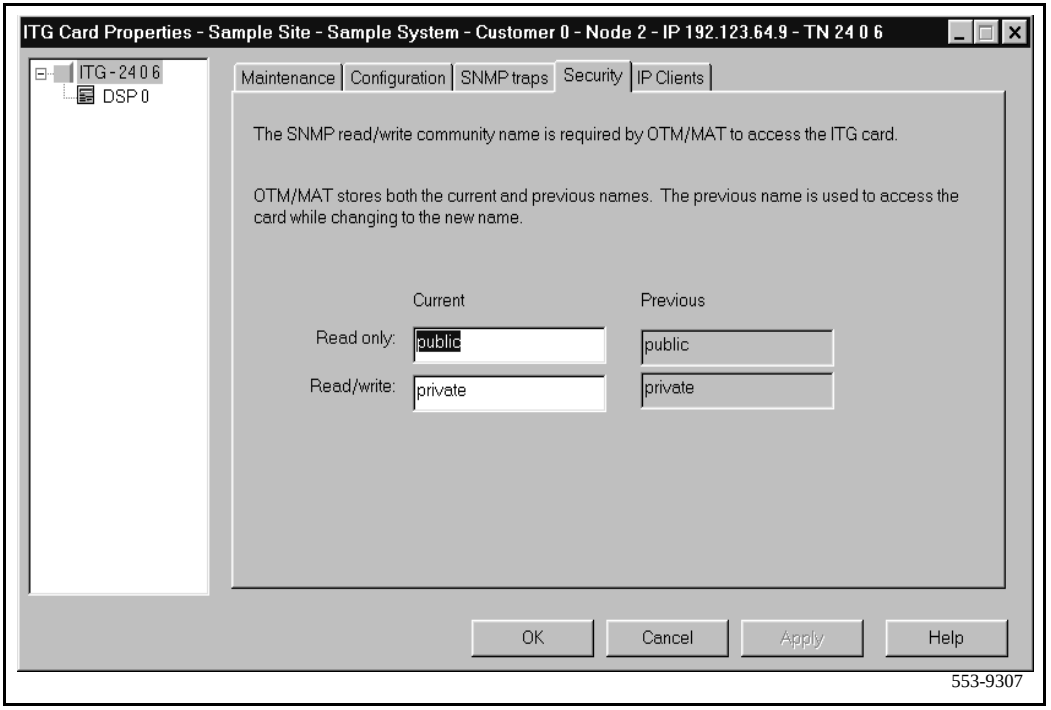
- "Not defined": card has been added via the node properties, or by retrieving the node properties from a Leader, but the user has never opened the card properties and made a change.
- "New": once the user opens a card with the state of "Not defined" and makes a change, the status changes to "New".
- "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 - ITG IP Telecommuter" window, and the "Node synch status" is set to "Changed."

Changing the SNMP Community Names to maintain access security in MAT ITG

Note: Good security requires changing passwords. The SNMP community names in MAT ITG act as the passwords for MAT ITG access to cards in the ITG node. You must change SNMP community names 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.

Note: 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 IP Line 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 IP Line cards. Call your Nortel Networks technical support representative for assistance.

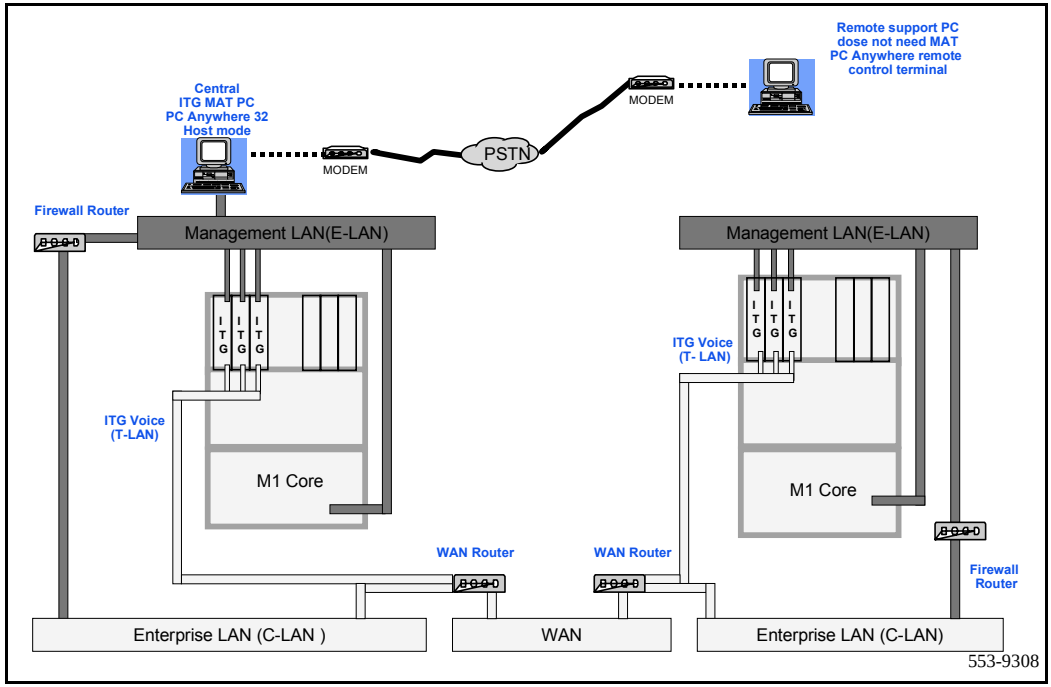


If a failed card has been replaced with a spare card try the default community names. The default "Read only" community name is **public**. The default "Read/write" community name is **private**. (MAT ITG only uses the "Read/write" community name).

Remote Access

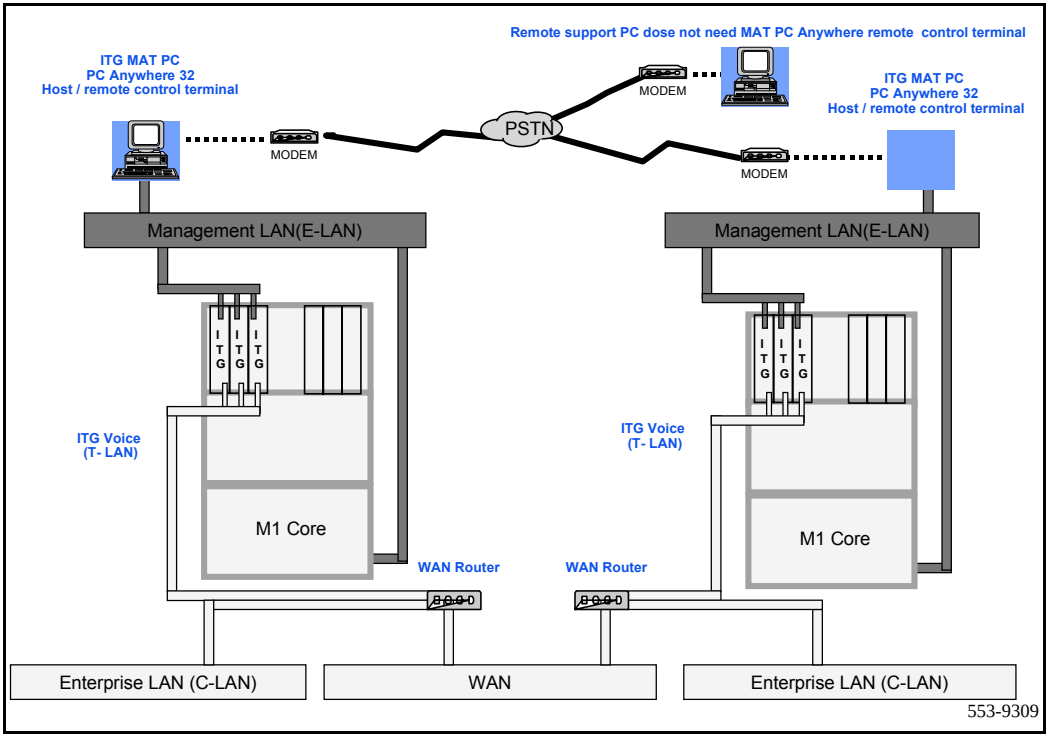
Support for remote access can be covered in two scenarios that vary according to the support organizations access to the customer's data network - LAN or WAN. In the first scenario, the support organization has full access to the customer LAN/WAN network and a single remote support and administration 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.

Figure 24
Remote access with full access to the customer's LAN/WAN network



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 25
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:

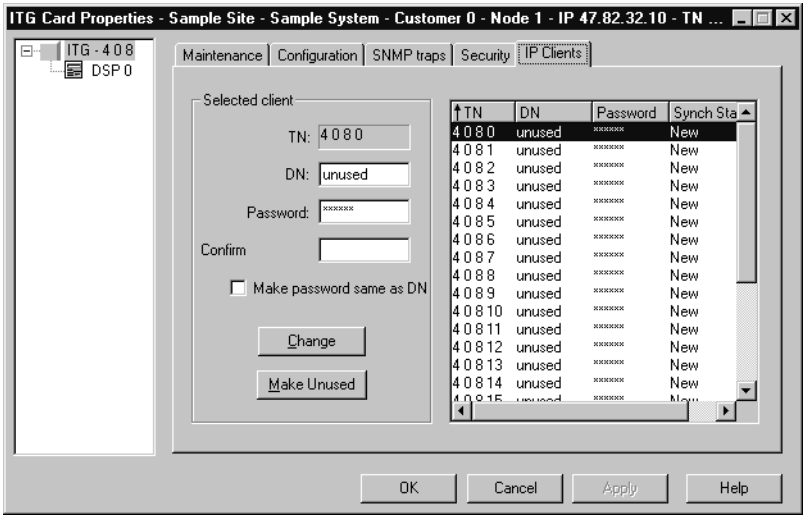
Changing the IP Telecommuter password and transmitting a new Gatekeeper Properties file

To update a user's IP Telecommuter password you must change the password in the card properties and transfer a new Gatekeeper Properties file.

Note: Cards do *not* need to be disabled to perform this procedure.

1 In the "IP Telephony Gateway - IP Telecommuter" window, double-click the IP Line card where the user's data and password are stored to display the "IP Line card Properties" window.

2 Click the "IP Clients" tab.



3 Select the user's TN in the list.

4 Change the "Password" field to the new user password.

5 Click the **Change** button then **Apply**.
The "Synch status" becomes "Changed."

6 Click **OK**.

When the password change in the Card Properties is completed, the GateKeeper Properties file must be transmitted to the IP Line card.

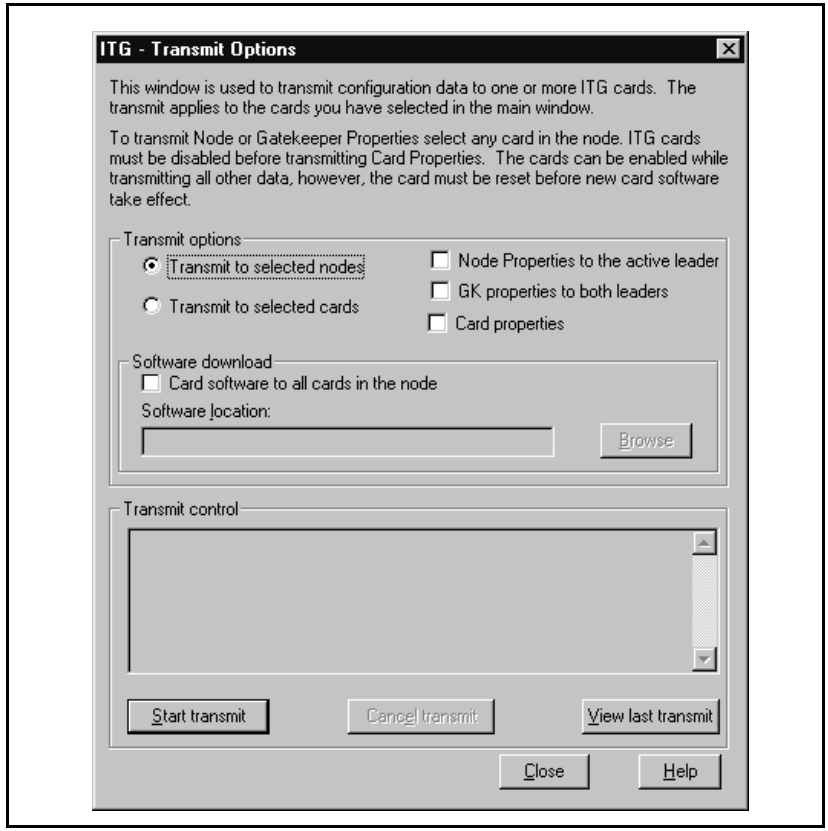
7 Select the IP Line card from the main window.

8 Click **Configuration** | **Synchronize** | **Transmit.**

The “ITG - Transmit Options” window appears.

9 Leave the radio button defaulted to “Transmit to selected nodes". Check the "GK Properties to both leaders" box only.

10 Click the **Start Transmit** button.



The transmission status is displayed in the “Transmit control” box. Confirm that the Gatekeeper Properties file is successful transferred to the card.

11 Communicate the new password to the user.

The procedure is complete.

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.

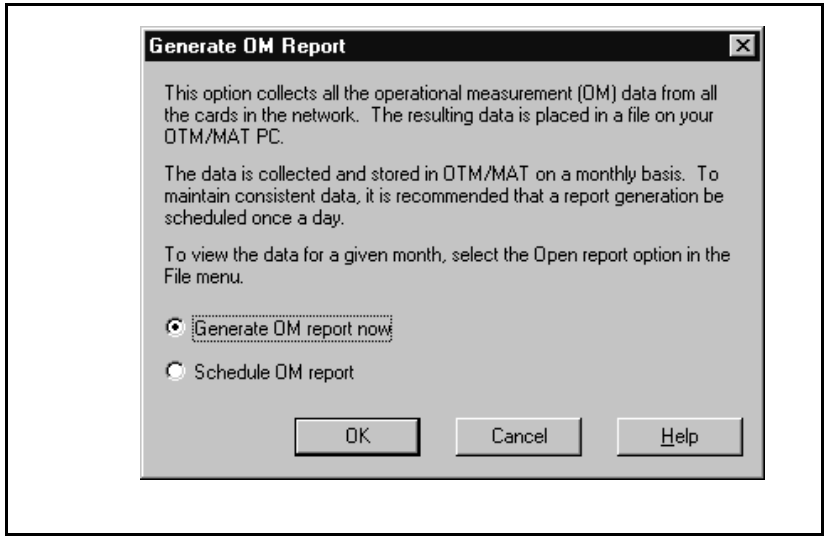
The OM reports are a collection of data from all the IP Line cards in the network. On an hourly basis, the OM data is written to a file. At midnight, the OM file will be copied to a backup file and the new day will start with a clean file.

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 IP Line 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**.

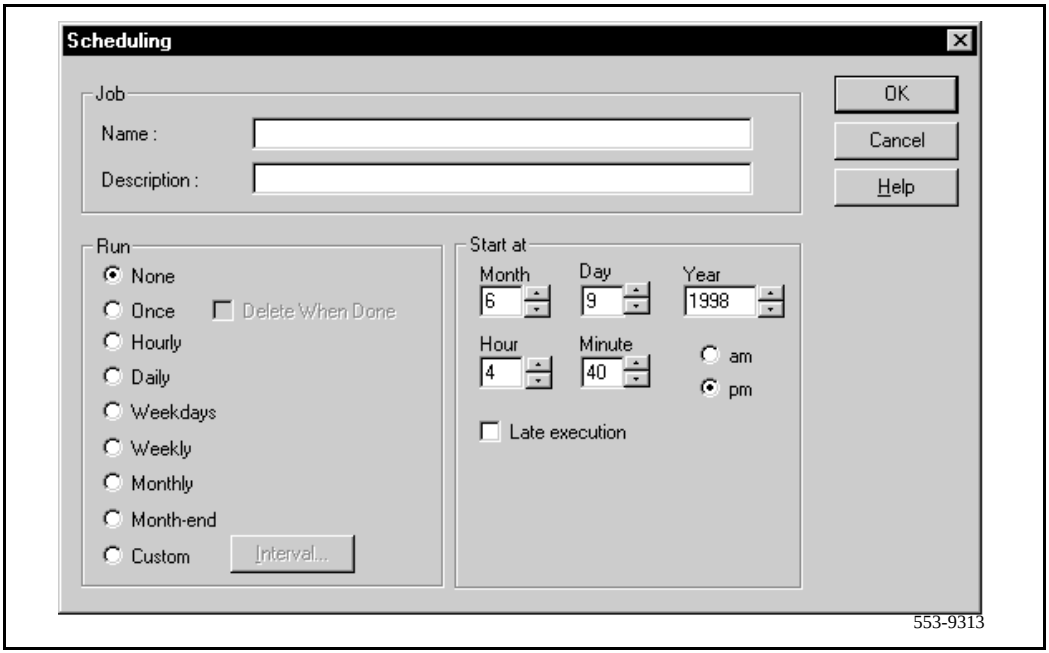
It is recommended that the user schedule report generation once a day. To schedule a report:

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.


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

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**.

To generate a report:

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

9 Click **OK**.

Viewing the ITG info and 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 IP Telecommuter** icon from the "Services" folder.
2. In the "IP Telephony Gateway - IP Telecommuter" 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 IP Line 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.

Backing up and restoring 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.*

Updating ITG node properties

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

1. In the MAT Navigator window, select the **ITG IP Telecommuter** icon from the "Services" folder. The system displays the "IP Telephony Gateway - IP Telecommuter" window.
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 IP Line cards are to be added or deleted from the node or changed (refer to the Maintenance section for the procedure to replace an IP Line card), then use one of the following procedures:

- “Adding an IP Line card to the node” on page 172
- “Deleting an IP Line card from the node” on page 182
- “Changing an IP address” on page 183

Adding an IP Line card to the node

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

2 In the “IP Telephony Gateway - IP Telecommuter” 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 IP Line card.

Note: Refer to and update the IP Line card MAC and IP addresses on the IP Line card 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 IP Line card in the Meridian 1 overlay 11. Refer to the *Installation* section for Meridian 1 configuration information.

Physical card installation

8 Identify the IPE card slots selected for the new IP Line card.

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

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

10 Pull the top and bottom locking devices away from the IP Line card faceplate.

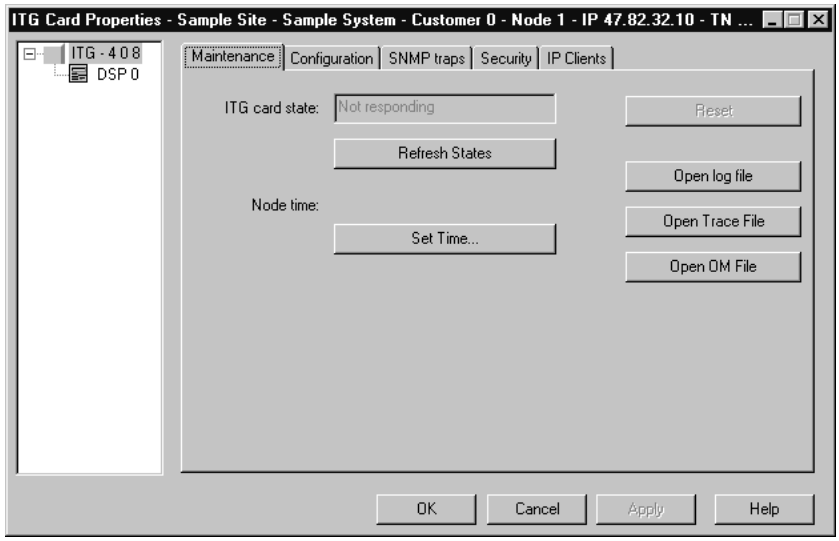
11 Insert the IP Line card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When IP Line cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in software, at which point it 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.

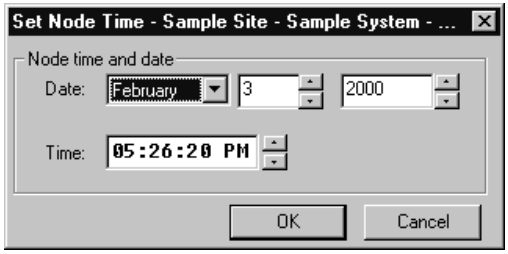
Note 2: Observe the IP Line card faceplate maintenance display to see start-up selftest results and status messages. A display of the type "F:xx" indicates a failure. Some failures indicate that the card must be replaced. "F:10" indicates Security Device test failure: check for presence of Security Device on the card. Refer to "Faceplate maintenance display codes for card reset" on page 208 for a listing of display codes.

To configure the new IP Line card, do the following:

12 In the "IP Telephony Gateway - IP Telecommuter" window, double-click on the IP Line card to display the "IP Line card Properties" window. Leave the IP Line card icon selected in the left side of the window.



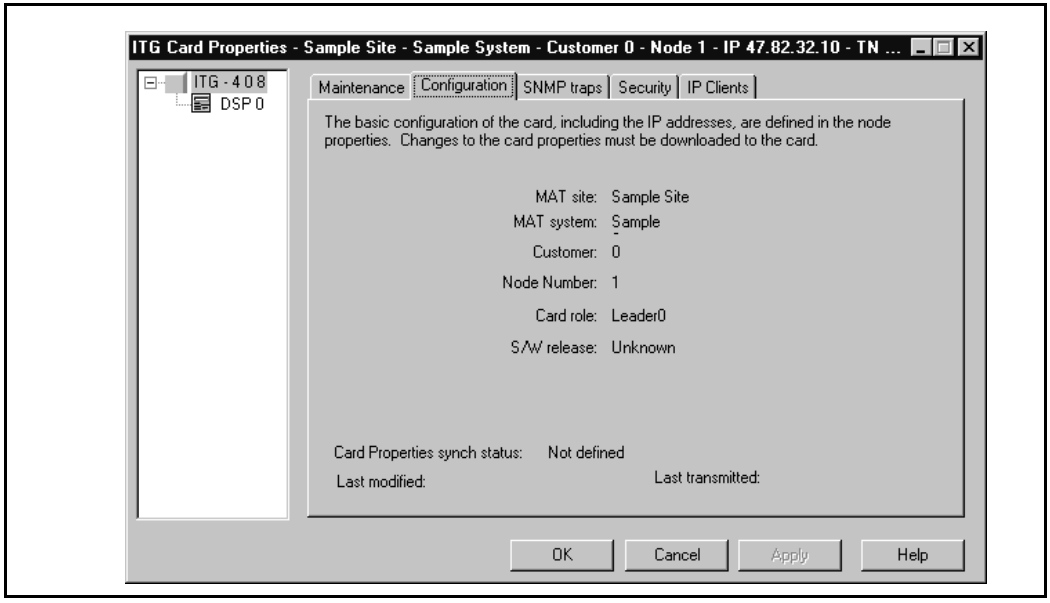
13 If the Leader 0 IP Line card is present and responding, you should set the time on the "Maintenance" tab of.the card properties for Leader 0. If not, you must remember to come back and set the time on the Leader 0 card after the card is physically installed.



14 Click the **Configuration** tab.

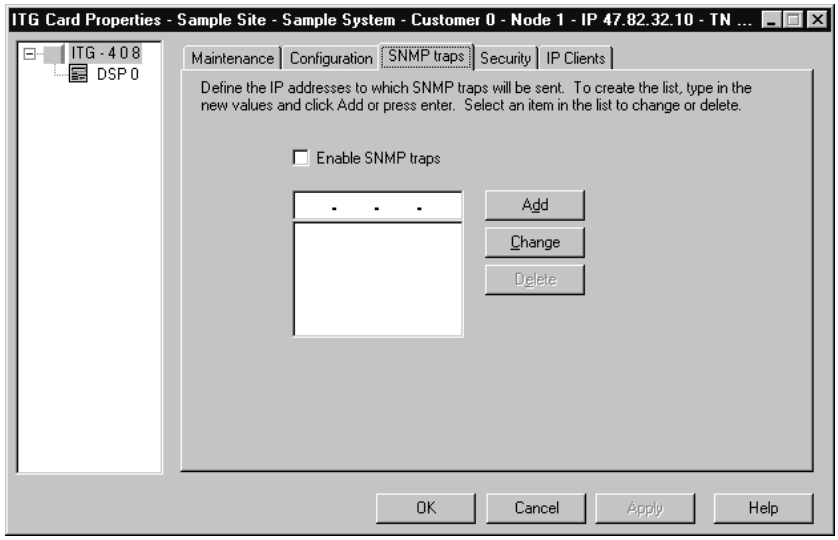
15 Verify that all cards in the same ITG node are running the same software version, and that the "S/W release" shows the latest recommended software version.

- If the software needs to be updated, refer to "Upgrading IP Line card software (if required)" on page 127.
- If the cards are not present and responding, you must remember to come back and verify the software version.



16 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.

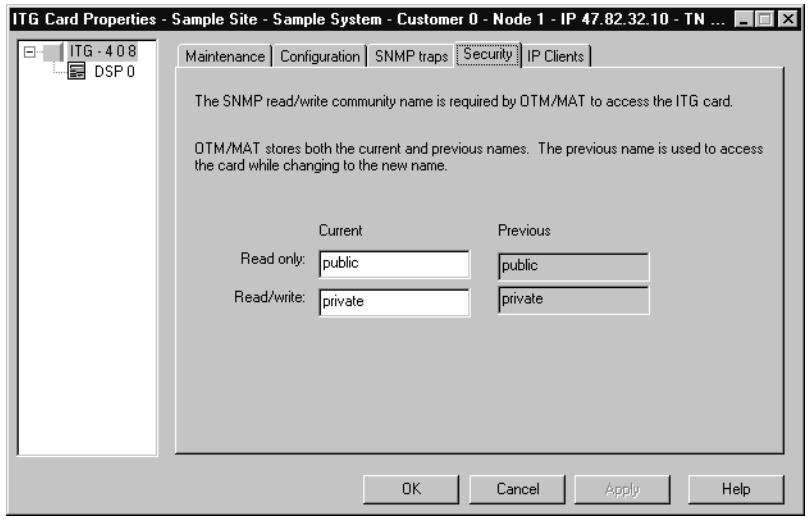


17 To add an SNMP Manager IP address, type the address in the entry field, and click **Add**. You should add SNMP Manager IP addresses for:

- 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.

18 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,



19 Click the **IP Clients** tab.

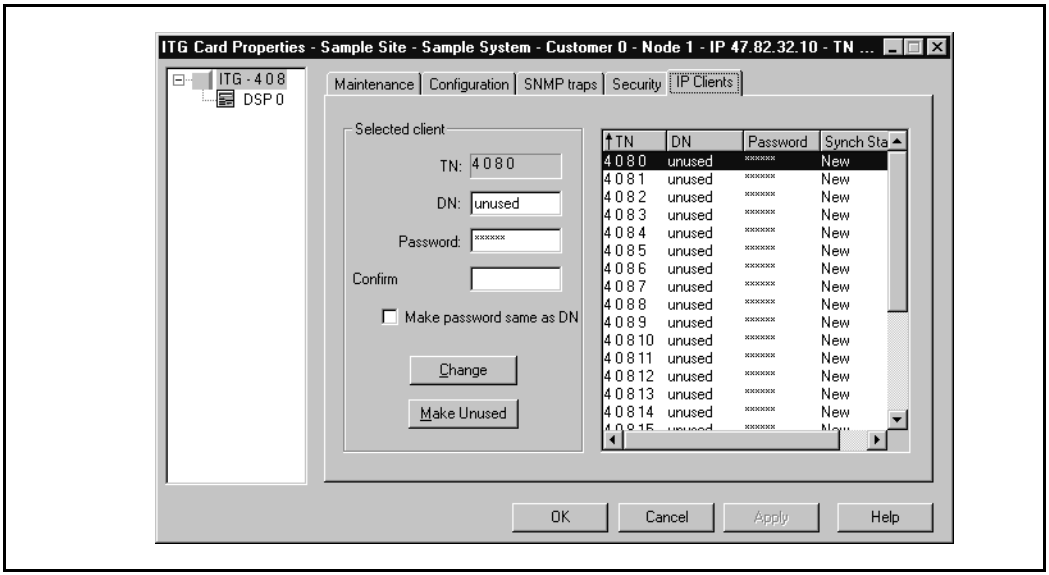
The "IP Clients" tab is used to define the DN and password for each of the 24 configurable TNs on the IP Line card. The list of TNs is built by MAT when the card is added via the Node Properties. This MAT configuration must be coordinated with the overlay 11 Meridian 1 configuration.

20 Select the first TN in the list.

21 Enter the "DN" and "Password" fields. Check the "Make password same as DN" field if the default password is to be the DN.

22 Click the **Change** button. The "Synch status" becomes "Changed."

23 Repeat the DN and password configuration for each port in the list.



Configuring IP Line card DSP properties

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

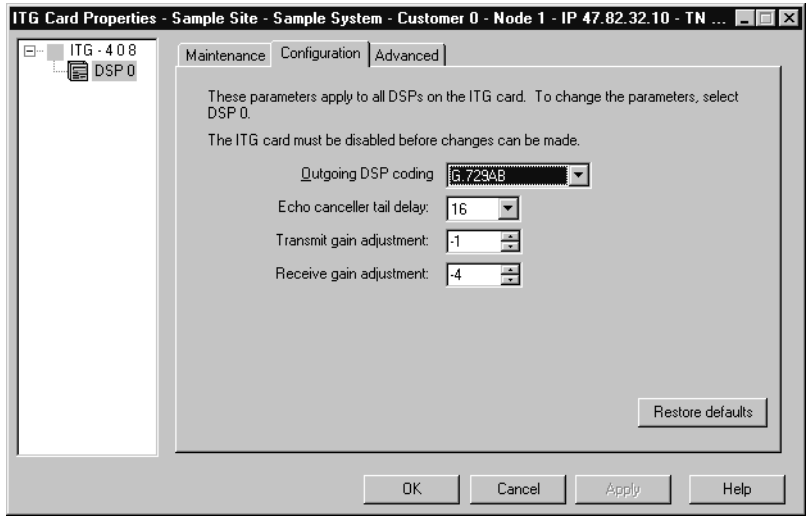
CAUTION

The default DSP parameters for the 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.

24 Click to select the **DSP 0** icon underneath the IP Line card.

25 Click the **Configuration** tab.

26 Select the "G.729AB" codec from the "DSP coding algorithm" pull-down menu.

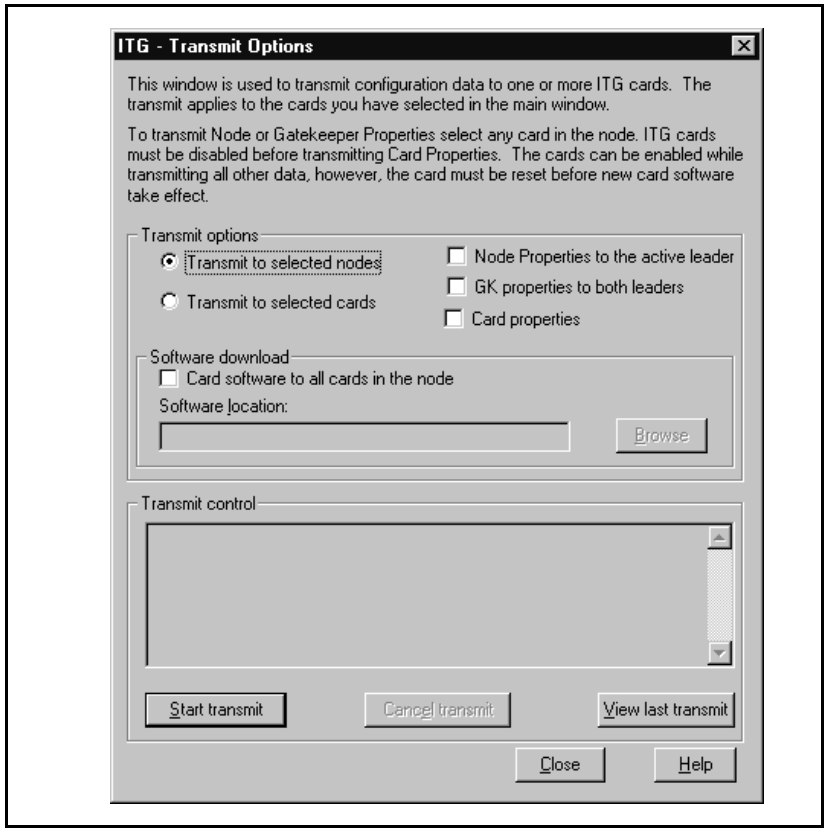


27 Click **Apply** then **OK**.

Transmitting the card properties

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

The "ITG - Transmit Options" window appears.



29 Leave the radio button defaulted to "Transmit to selected nodes". Check the "Card properties to both leaders" box only.

30 Click the **Start Transmit** button.

The transmission status is displayed in the "Transmit control" box. Confirm that card properties are transmitted to all cards successfully.

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

32 Use the overlay 32 ENLC command to re-enable the IP Line cards.

33 In the "IP Telephony Gateway - IP Telecommuter" main window, select **View | Refresh**. The card status should now show "Enabled."

34 Verify the TN, management interface MAC address, and IP addresses of each IP Line card. Compare the displayed values with those on the IP Line card Installation Summary Sheet.

Meridian 1 Configuration

LD 11 – Configure the IP Line cards.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	2616	Type of telephone set.
TN	l s c u	Terminal Number (corresponding to TNs on the IP Line card, u = 0-23 for the 24 configurable TNs on each IP Line card).
DES	ITG	To identify the IP Line card.
CDEN	4D	Card density.
...	...	...
CUST	0-99	Customer Number (All sets corresponding to the same IP Line card must have the same customer number).
AOM	0	Number of Add-On Modules.
FDN	xxxxxxx	Flexible CFNA DN (Configure with Voice Mail DN).
...	...	...
CLS	ADD	Automatic Digit Display.
	CNDA	Call party Name Display Allowed
	FLXA	Flexible voice/data Allowed.
	FNA	Forward No Answer Allowed.
	MWA	Message Waiting Allowed.
	VCE	Voice Terminal. (for unit 16 and up).

...	...	...
KEY	00 MCR xxxxxxx	Multiple call ringing DN key. (Must be configured on key 0. xxxxxxx is the IP Client's DN, and can be a multiple appearance of the associated desktop set's DN).
- CPND	NEW	
- NAME	aaaa, bbbb	CPND name (First name, Last name).
- XPLN	xx	Expected name length.
-DISPLAY _FMT	Last, FIRST/(FIRST, LAST)	Display format for CPND Name.
KEY	01 TRN	Transfer key.
KEY	02 AO6	6 party Conference key.
KEY	03 MWK xxxxxxx	Message Waiting key. xxxxxxx is the Voice Mail DN.

The procedure is complete.

Deleting an IP Line card from the node

1. In the "MAT Navigator" window select the **ITG IP Telecommuter** icon from the "Services" folder.
2. If the IP Line 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 - IP Telecommuter" window, select **Node | Properties** from the popup menu. The ITG Node Properties window is displayed.
4. Click the "Configuration" tab.
5. Select the IP Line card to be deleted from the list.
6. Click the **Delete** button.

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

8 Remove the IP Line cards 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 overlay 11.

Changing an IP address

1 To change the IP address of IP Line card(s): Click **Configuration|Node|Properties**. Update the IP Line 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 Leader 0 IP Line card in the IP Telephony Gateway - IP Telecommuter 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.

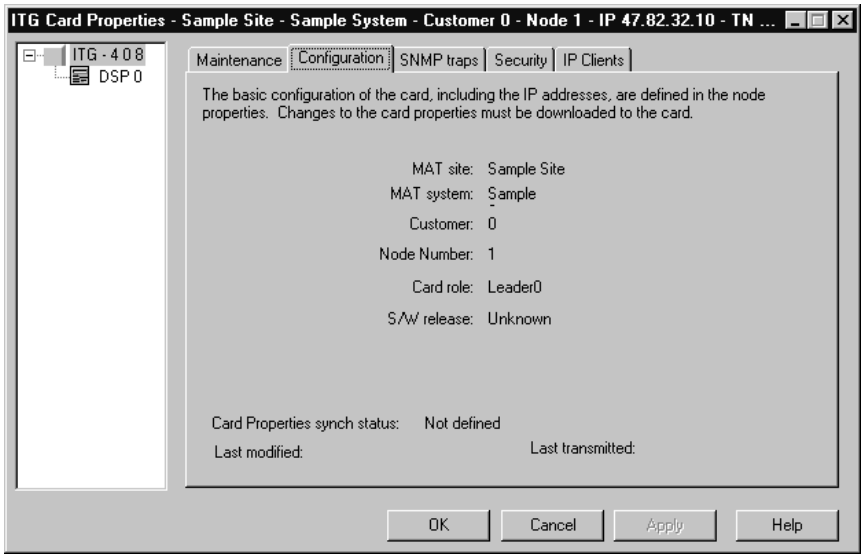
Update IP Line card properties

Note: Some basic IP Line card configuration, including IP address configuration, must be performed from the ITG Node Properties window, as described in "Updating ITG node properties" on page 171.

1. In the "MAT Navigator" window, select the **ITG IP Telecommuter** icon from the "Services" folder.
2. In the "IP Telephony Gateway - IP Telecommuter" window, select the IP Line card to be modified.
3. Select the IP Line card to be updated and click the right mouse button to select **Cards | Properties** from the pop-up menu. The "IP Line card Properties" window appears. The "Configuration, SNMP traps, and Security" tabs are described following step 3.
4. Make the required changes to the IP Line card configuration. Click **Apply** then **OK**.

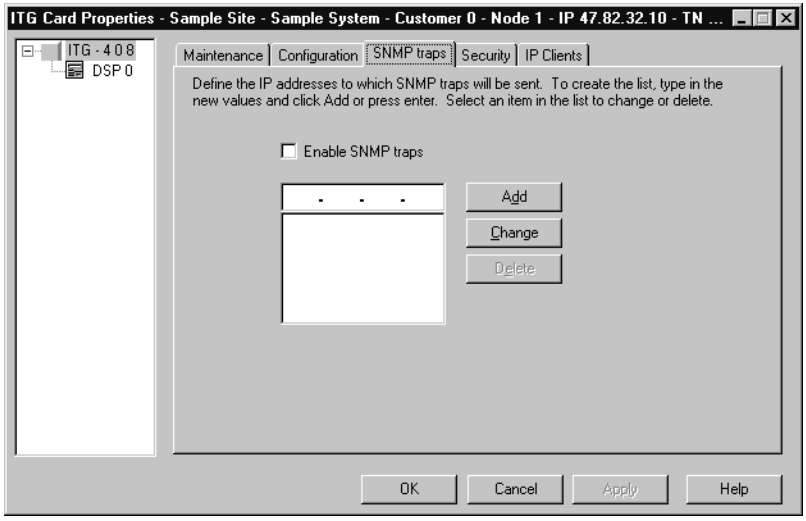
The following pages describe the various card properties tabs.

Configuration tab



The Configuration tab shows IP Line card information.

SNMP traps tab



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

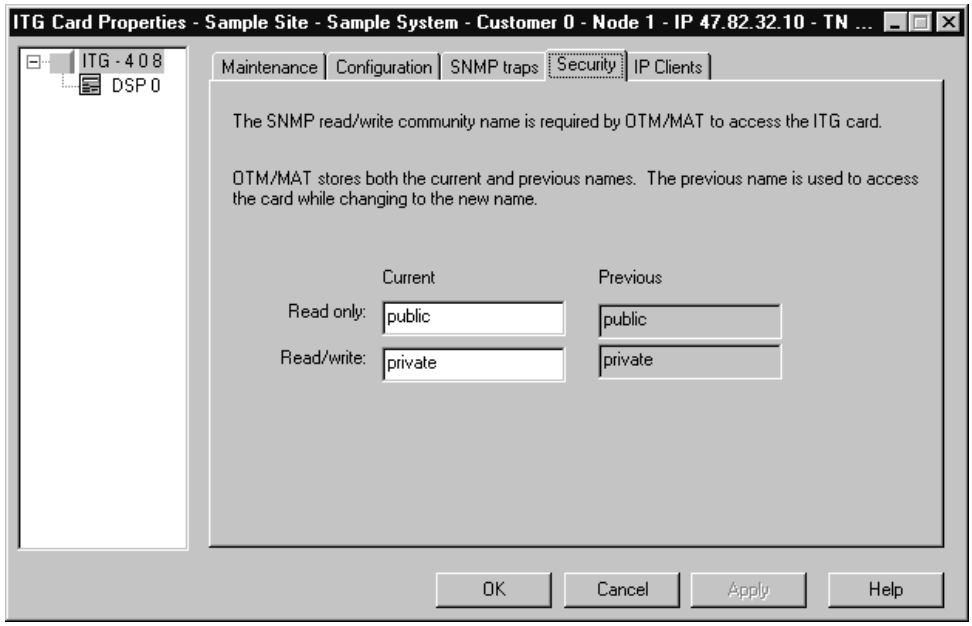
To enable the sending of SNMP traps to receive alarms (error messages) to the hosts specified by the IP addresses in the list, check the “Enable SNMP traps” box.

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 IP Line card. This name is used with all SNMP communication between MAT and the card.

Update IP Line card DSP properties

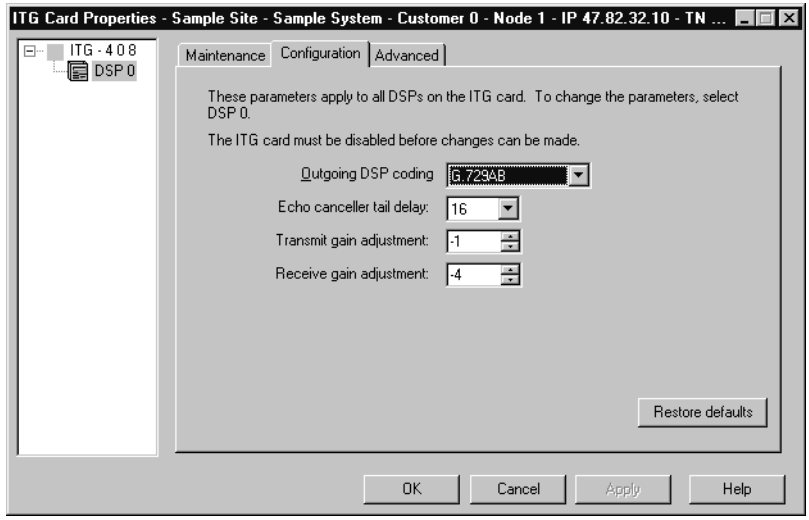
Note: The properties of all DSPs on an IP Line card are modified by configuring the properties for "DSP 0" on an IP Line card. The "Restore defaults" button can be used to restore all default values including restoring the coding algorithm to G.729AB.

CAUTION

The default DSP parameters for the 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 IP Telecommuter** icon from the "Services" folder.
2. In the "IP Telephony Gateway - IP Telecommuter" window select the IP Line 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 "IP Line card Properties" window appears.
4. Click the **DSP 0** icon underneath the IP Line card.

5 Click the **Configuration** tab and configure the parameters as required.



Configuration tab parameters description

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

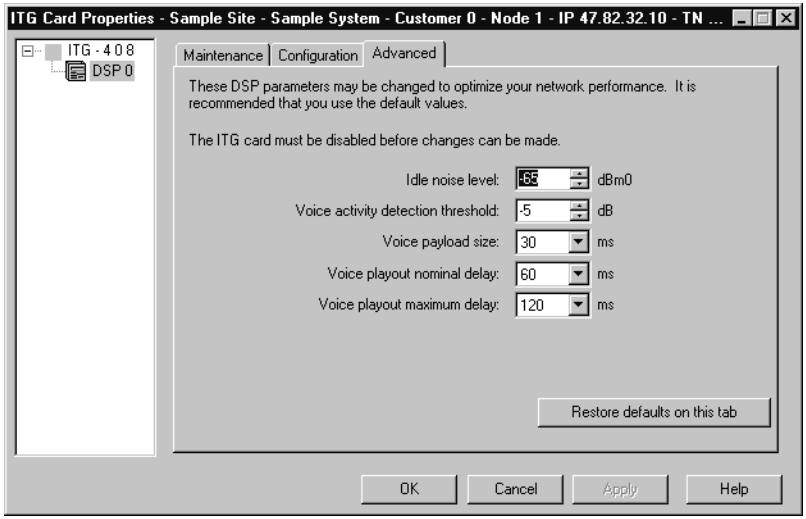
Select the “G.729AB" codec from the “DSP coding algorithm” pull-down menu.

The “Echo canceller tail delay” parameter range is: 8-(16)-32 ms. The default is 32 ms.

The “Transmit gain adjustment” parameter range is -14 to +14 dB. The default is -1 dB.

The “Receive gain adjustment” parameter range is -14 to +4 dB. The default is -4 dB.

6 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 -5 dB.

The “Voice payload size” parameter range is 10-80ms in increments of 10.
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 “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 (ND)*2.

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

Transmit the card properties to the updated IP Line card:

8 Select the updated IP Line card in the IP Telephony Gateway - IP Telecommuter window.

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

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

11 Click the **Start Download** button.

The results of the download appear in the “Transmit control” box.

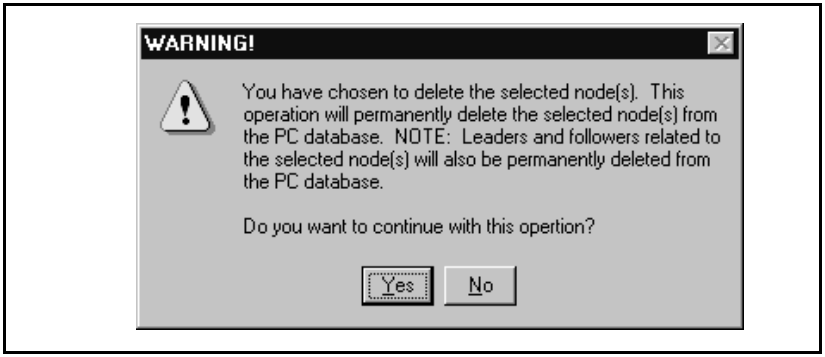
12 Click **Close**.

Delete an ITG node

1 Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.

2 In the “IP Telephony Gateway - IP Telecommuter” window select the Leader 0 IP Line 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 IP Line cards will be deleted.



Displaying ITG node properties

1. Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.
2. Select **Node | Properties** from the popup menu. The ITG Node Properties window will be displayed.

Displaying IP Line card properties

1. Double-click "ITG IP Telecommuter" from the Services folder in the MAT Navigator window. The IP Telephony Gateway - IP Telecommuter window appears.
2. Select the IP Line 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 "IP Line card Properties" window will be displayed.

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

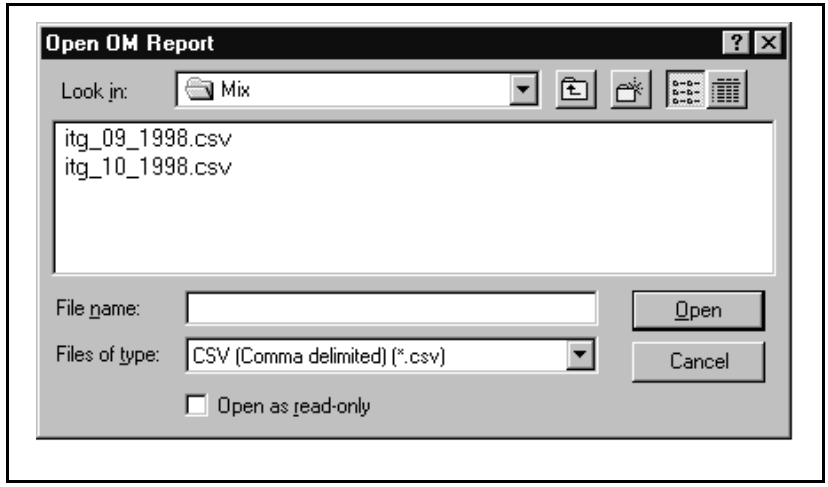
If you select **DSP 0**, the DSP parameters of the IP Line card are displayed.

Opening an Operational Measurement (OM) report

To open an OM report:

1 In the "IP Telephony Gateway - IP Telecommuter" window, click **File | Report | Open**.

2 Select an “ITG_mm_yyyy.csv” file to be opened and click **Open**.



The selected report is opened.

Use the Retrieve command

The Retrieve command sends information from the IP Line 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 IP Line cards and node.

To use the Retrieve command:

1. In the "IP Telephony Gateway - IP Telecommuter" 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 IP Line card maintenance port.

Alternatively, the ITG shell can be accessed from the MAT PC. Refer to "Telnet to an IP Line card" on page 195.

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

- "Telnet to an IP Line card" on page 195.
- Changing the default ITG Telnet password to maintain access security
- "Download the ITG operational measurements through the ITG shell" on page 196
- "Reset the operational measurements" on page 197.
- "Display the number of DSPs" on page 197.
- "Display ITG Node Properties" on page 197.
- "Transfer files via the command-line interface" on page 198.
- "IP configuration commands" on page 200.
- "Download the ITG error log" on page 200.
- "Display the Gatekeeper Properties" on page 201.

Telnet to an IP Line card

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

1. In the "MAT Navigator" window select the **ITG IP Telecommuter icon** from the "Services" folder.
2. In the "IP Telephony Gateway - IP Telecommuter" window click the right mouse button on the IP Line card that you wish to access and select **Card | Telnet to IP Line 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 IP Line 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 IP Line 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 IP Line 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 IP Line 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 IP Line card operational measurements file contains counts of incoming and outgoing calls, call attempts, calls completed, and total holding time for voice calls. To download this file from the MAT PC to the IP Line 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.

The Gatekeeper OM file contains information about the Gatekeeper and its endpoints' activities.

At the ITG shell prompt, type: **currGKOMFilePut** <*hostname, username, password, directory path, filename*> for the current file, or **prevGKOMFilePut** <*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 IP Line card: **DSPNumShow**

Display 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 IP Line card: **itgCardShow**

The following commands give additional information about an IP Line card:

- ldrResTableShow
- ifShow
- dongleIDShow
- serialNumShow
- firmwareVersionShow
- swVersionShow
- emodelSim

Transfer files via the command-line interface

To transfer a file from the IP Line card to the MAT PC or from the MAT PC to the IP Line 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 IP Line card: that is, commands containing “Get” as part of the command refer to file transfer from the MAT PC to the IP Line card, while commands containing “Put” as part of the command refer to file transfer from the IP Line card to the MAT PC:

The “bootptab.1” file (transferred by the “bootPFileGet” and “bootPFilePut” commands) contains node properties 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 IP Line 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 IP Line card itself or another IP Line card when a PC card in the A: drive or C: drive (the swDownload command must only use the A: drive), of the IP Line card contains the software binary file.

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

This command updates the software on the IP Line card with the binary file received from an FTP server or IP Line card (from the drive A: PC card) corresponding to the *hostname* IP address. The IP Line 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 IP Line card must be rebooted with cardReset in order to run the new software.

- 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*>
- 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

Display the Gatekeeper Properties

To display information about the gatekeeper properties, use the following commands:

- GKGenInfoShow
- GKGWInfoShow

Meridian 1 system commands - LD 32

The following Meridian 1 system administration commands can be performed:

- "Disable the specified IP Line card" on page 203.

Note 1: The IP Line card must be disabled before card properties can be transmitted from the MAT ITG application to the card.

Note 2: The card reset button is only available in the MAT ITG application when the card is disabled.

Note 3: Disabling the IP Line card in overlay 32 does not disable the active leader or backup leader functions.

- "Disable the specified IP Line card when idle" on page 203.

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

- "Disable a specified ITG port" on page 204.
- "Enable a specified IP Line card" on page 204.
- "Enable a specified ITG port" on page 204.
- "Display IP Line card ID information" on page 204.

Note 1: This command will display the PEC (Product Engineering Code) for the card. The ITG PEC is NTCW80AA.

Note 2: The IP Line card information displays the same IP Line card serial number that is displayed from the ITG shell using the **serialNumShow**.

- "Display IP Line card status" on page 205.
- "Display IP Line card port status" on page 205.

A summary list of ITG Meridian 1 system commands is shown in Table 10 on page 202.

Table 10 summarizes the Meridian 1 system administration commands available in overlay 32.

Table 10
Overlay 32 - ITG maintenance commands (Part 1 of 2)

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 IP Line card instead of the DISC command. . The disablement of the IP Line card is indicated by the NPR001 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

Table 10
Overlay 32 - ITG maintenance commands (Part 2 of 2)

Command	Function
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

Disable the specified IP Line card

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

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

Disable the specified IP Line card when idle

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

DISI l s c	Disable the specified IP Line 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 IP Line card

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

ENLC l s c	Enable the specified IP Line 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 IP Line card ID information

To display the IP Line card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the IP Line card, where: l = loop, s = shelf, c = card

Display IP Line card status

To display the status of a specified IP Line card in LD 32, use the following command:

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

Display IP Line card port status

To display the status of a port on the IP Line 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.

Maintenance

Introduction

This section provides information on maintenance functions of the IP Line card:

- “Faceplate maintenance display codes for card reset” on page 208.
- “System error messages (alarms)” are described on page 211.
- “Replacing an IP Line card” on page 214.
- “Meridian 1 system level maintenance of the IP Line card” on page 222.
- “ITG shell commands” on page 223.
- “IP Line card selftests” on page 240.
- “Troubleshooting a software load failure” on page 241.
- “Warm rebooting the IP Line card” on page 245.
- “Testing the IP Line card DSPs” on page 245.
- “Working with alarm and log files” on page 245.

Faceplate maintenance display codes for card reset

The IP Line 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 11 gives a list of display messages.

Table 11
ITG faceplate maintenance display code messages

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 11
ITG faceplate maintenance display code messages

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, transmitting bootp requests. If this display persists, then the IP Line card is running in BIOS ROM mode due to IP Line card software failure.
T:21	CardLAN operational, A07 enabled, display now under host control. 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. Enter '+++' to escape from bootp request mode and start ITG shell.
T:22	The IP Line card is attempting to start the IP Telecommuter application.
LDR	Card is running active leader tasks.

Table 11
ITG faceplate maintenance display code messages

Hex display code	Message
BLDR	Card has detected existing active leader, and is running backup leader tasks.
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.

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 IP Line card properties; it also puts the system error message into the error log file containing error messages, which is available through the MAT IP Line card properties by clicking on the 'Open Log File' button on the "Maintenance" tab of the IP Line 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 12 lists the ITG messages by severity.

Table 12
ITG system error messages (alarms)

Alarm Clearance - No intervention required	
ITG0100	Successful bootup. All alarms cleared.
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.
ITG0204	DSP device reset.
ITG0205	Not used.
ITG0207	Unknown H.323 message received. Message discarded/rejected.

Table 12
ITG system error messages (alarms)

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.
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.
ITG0350	Gatekeeper RAS reject threshold exceeded.
ITG0351	Can’t open gatekeeper configuration file. Using default settings.
Major Alarms - Immediate Intervention Required	
ITG0400	Fatal self-test failure. Card is out of service.
ITG0401	Reboot threshold exceeded. Manual intervention required.

Table 12
ITG system error messages (alarms)

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).
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.
ITG0452	Meridian-1 messaging failure. Unable to process calls.
ITG0453	Bad gateway DN file. Reverting to previous version (if any).
ITG0454	Bad gatekeeper password file. Reverting to previous version (if any).
ITG0455	Can’t open gateway DN file.
ITG0456	Can’t open gatekeeper password file.

Replacing an IP Line card

The IP Line card should be replaced when the following conditions occur:

- If, following a reboot, the IP Line 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 IP Line 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 IP Line 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 IP Line Card:

1 Locate the faulty card in the MAT ITG database by the TN, MAC address, and IP address.

2 Disable the faulty IP Line card in overlay 32 with the **DISI** command. The Meridian outputs "NPR001" when the card has been completely disabled by the DISI command.

3 Disconnect the T-LAN Ethernet cable from the faceplate of the faulty IP Line 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 IP Line card.

WARNING

In the Option 11 cabinet the T-LAN cable is hidden behind the faceplate of the IP Line 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 IP Line card in the option 11 cabinet.

4 Remove the faulty IP Line card from the Meridian 1.

5 Remove the Security Device from the faulty IP Line 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 IP Line 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 IP Line card from the list of cards in the node.

10 Change the "Management MAC" to the MAC address of the replacement IP Line card. The MAC address is labeled on the faceplate of the replacement IP Line card.

11 Click **OK**.

12 Select Leader 0 or any IP Line card in the node.

13 Use the **Configuration | Synchonize | 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 IP Line card.

14 Install the Security Device that was removed from the faulty IP Line card into the replacement IP Line 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 IP Line 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 IP Line card in the Option 11 cabinet.

- Pull the top and bottom locking devices away from the ITG faceplate.
- Insert the IP Line card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When IP Line 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 241 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 IP Line card.

Note: Refer to Appendix A for detailing instructions on connecting the T-LAN cable to the IP Line card in the Option 11 cabinet.

Note: When connecting the IP Line 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 IP Line card.

17 In the MAT "IP Telephony Gateway" main window, select **View | Refresh** and verify that the replacement IP Line card status is showing "Unequipped."

Verifying card software

18 In the "IP Telephony Gateway" window, double-click the replacement IP Line card to open the “Card Properties”. Leave the default selection of the IP Line card in the "Card Properties" window, and click the “Configuration” tab.

19 Verify that the “S/W release” shows the latest recommended IP Line 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.”

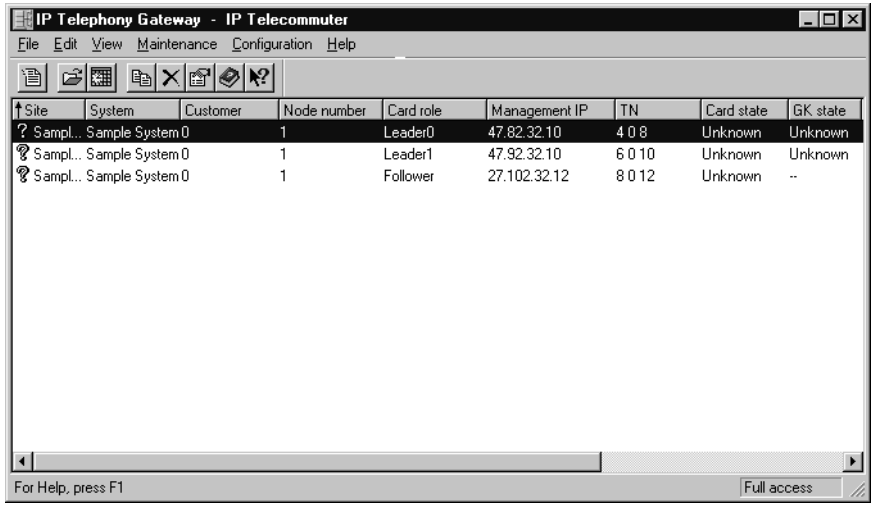
The default user name is **usa**. The default password is **usa**. See your Nortel Network representative to register for a new default name and password if the default does not work.

If the replacement card requires a software upgrade, refer to the next procedure, *Upgrading IP Line card software.*

Transmitting Card Properties and Gatekeeper Properties

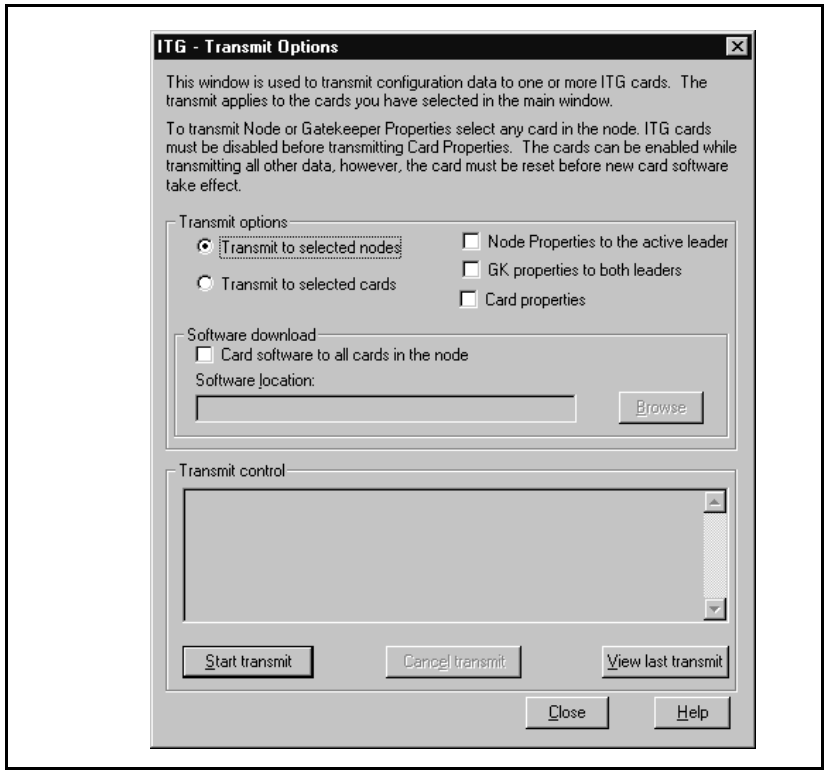
Note: It is not necessary to disable IP Line cards when transmitting Gatekeeper Properties alone.

20 In the "IP Telephony Gateway - IP Telecommuter" window, select the replacement IP Line card.



21 Click **Configuration** | **Synchronize** | **Transmit.**

The “ITG - Transmit Options” window appears.



22 Select the radio button “Transmit to selected cards”. Check the “Card properties to both leaders” and “Gatekeeper Properties to both leaders” boxes only.

23 Click the **Start Transmit** button.

The transmission status is displayed in the “Transmit control” box. Confirm that Card Properties and Gatekeeper Properties are transmitted successfully.

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

25 Use the overlay 32 ENLC command to re-enable the IP Line card.

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

27 Update the Installation Summary Sheet with the new MAC address.

28 Verify the TN, management interface MAC address, IP addresses, the NT-SDID, and keycode for each IP Line card. The NT_SDID and keycode are verified by double-clicking each IP Line 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 IP Line 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 IP Line 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 IP Line card

The IP Line card system level maintenance can be performed in overlay 32, in the same manner as with the NT8D14 Universal Trunk card. Table 13 lists the commands supported on the IP Line card.

Table 13
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 223.

ITG shell commands

The ITG shell commands are accessed by connecting a TTY to the MMI port on the IP Line 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 14 through 22.

Table 14
ITG Shell Commands

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.**
itgMemShow	**Show memory usage**
ifShow	**Show detailed IP information, including MAC addresses.**
IPInfoShow	**Prints IP information.**
dongleIDShow	**Prints out dongle ID.**
serialNumShow	**Prints out card serial number.**
firmwareVersionShow	**Prints out firmware version number.**
numChannelsShow	**Prints out number of available channels.**

Table 14
ITG Shell Commands

Command	Description
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 IP Line card.**
configFileGet	**Sends an updated config.ini file from MAT to ITG.The config.ini file also contains the gatekeeper IP address, gateway password, and gateway DN-port mapping table.**
DNPortTableGet	**Sends an updated DN to Port file from MAT to the IP Line card.**
bootpFileGet	**Sends an updated bootptab file from the MAT PC to the IP Line card.**
GKTableGet	**Sends an updated gatekeeper information file from MAT PC to the IP Line card.**
hostFileGet	**Transfers any file from the MAT PC to the IP Line card.**
currOmFilePut	**Sends the current OM file from ITG to MAT.**

Table 14
ITG Shell Commands

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.**
currGKOmFilePut	**Sends the current gatekeeper OM file from the IP Line card to the MAT PC.**
prevGKOmFilePut	**Sends the previous gatekeeper OM file from the IP Line card to the MAT PC.**
currGKLogFilePut	**Sends the current gatekeeper log file from the IP Line card to the MAT PC.**
prevGKLogFilePut	**Sends the previous gatekeeper log file from the IP Line card to the MAT PC.**
GKTablePut	**Sends the gatekeeper information file from the IP Line card to the MAT PC. This contains the TimeToLive values for the client and gateway, and the alias-password table.**
hostFilePut	**Transfers any file from the IP Line card to the MAT PC.**
GKEndptInfoPut	**Transfers endpoint information from the IP Line card to the MAT PC.**
GKCallInfoPut	**Transfers call information from the IP Line card to the MAT PC.**

Table 14
ITG Shell Commands

Command	Description
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**
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.**
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:	
cardReset	**Warm reboot of IP Line card.**

Table 14
ITG Shell Commands

Command	Description
DSP Commands:	
DSPReset	**Resets the specified DSP**
DSPselfTest	**Runs selftest on the DSP.**
DSPNumShow	**Prints number of DSPs on IP Line 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.**
Gatekeeper Query Commands:	
GKInfoShow	**Prints gatekeeper general information, which includes TimeToLive values for the client and gateway.**
GKClientInfoShow	**Prints all registered Clients with their DN and IP addresses.**
GKGWInfoShow	**Prints all registered Gateways with lists of DNs.**
GKCallInfoShow	**Prints call information for all calls active or in progress.**

User's Manual

Table 15
General-Purpose Commands

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:	**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:	**itgHelp**
Description:	Displays the IP Line card commands and a short description.
Synopsis:	**shellPasswordSet**
Description:	**Change the default ITG shell password.**

Table 15
General-Purpose Commands

Synopsis:	**dongleIDShow**
Description:	**Prints out dongle ID.**
Synopsis:	**serialNumShow**
Description:	Prints out card serial number. This command displays the same IP Line 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.**
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.**

Table 15
General-Purpose Commands

Synopsis:	**emodelSim**
Description:	**Allows user to interactively determine QoS score.**

Table 16
File Transfer Commands

Synopsis:	**swDownload** hostname, username, password, directory path, filename
Description:	Updates the software on the IP Line card with the binary file received from an FTP server corresponding to the *hostname* IP address. The IP Line 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 IP Line 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 IP Line card itself or another IP Line card when a PC card in the A: drive of the IP Line card contains the software binary file.
Example:	ITG> swDownload “47.82.32.246”, “anonymous”, ”guest”, “/software”, ”vxWorks.mms”
Synopsis:	**configFileGet** hostname, username, password, directory path, filename
Description:	Updates the config.ini file on the IP Line 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. The config.ini file also contains the gatekeeper IP address, gateway password, and gateway DN-port mapping table.
Example:	ITG> ConfigFileGet “ngals042”, “anonymous”, ”guest”, “/configDir”, ”config.ini”
Synopsis:	**bootPFileGet** hostname, username, password, directory path, filename
Description:	Updates the bootptab file on the IP Line 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 “47.82.xx.xxx”,“anonymous”,”guest”,“/bootpDir”, ”bootptab”

Table 16
File Transfer Commands

Synopsis:	**GKTableGet** hostname, username, password, directory path, filename
Description:	Updates the gk_gen_info file on the IP Line card with the gk_gen_info file on the specified host, account and path. The GKTableGet task on the IP Line card initiates an FTP session with the given parameters and downloads the file to the flash file system.
Example:	ITG> GKTableGet “47.82.xx.xxx”,“anonymous”,”guest”,“/gatekeeper”, ”gk_gen_info”
Synopsis:	**hostFileGet** hostname, username, password, directory path, filename, ITGFileName, listener
Description:	Gets any file from the host and does a get via FTP to the IP Line 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 “47.82.xx.xxx”, “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 IP Line card’s operational measurements file to the specified location on the host.
Example:	ITG> currOmFilePut “47.82.xx.xxx”, “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 IP Line card’s operational measurements file to the specified location on the host.
Example:	ITG> prevOmFilePut “47.82.xx.xxx”, “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 IP Line card’s call trace file to the specified location on the host.

Table 16
File Transfer Commands

Example:	ITG> traceFilePut “47.82.xx.xxx”,“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 IP Line card’s logfile the to specified location on the host.
Example:	ITG> currLogFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/currDir”, ”logFile”
Synopsis:	**prevLogFilePut** 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 IP Line card’s logfile the to specified location on the host.
Example:	ITG> prevLogFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/currDir”, ”logFile”
Synopsis:	**currGKOmFilePut** hostname, username, password, directory path, filename
Description:	The omFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the IP Line card’s gatekeeper operational measurements to the specified location on the host.
Example:	ITG> currGKOmFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/currDir”, ”GKomFile”
Synopsis:	**prevGKOmFilePut** hostname, username, password, directory path, filename
Description:	The omFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the IP Line card’s previous gatekeeper operational measurements to the specified location on the host.
Example:	ITG> prevGKOmFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/prevDir”, ”GKomFile”
Synopsis:	**GKtraceFilePut** hostname, username, password, directory path, filename
Description:	The traceFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the IP Line card’s gatekeeper call trace file to specified location on the host.
Example:	ITG> GKtraceFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/trcDir”, ”trcFile”

Table 16
File Transfer Commands

Synopsis:	**currGKLogFilePut** hostname, username, password, directory path, filename
Description:	The logFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the IP Line card's gatekeeper log file to specified location on the host.
Example:	ITG> currGKLogFilePut "47.82.xx.xxx","anonymous","guest","/currDir", "GKlogFile"
Synopsis:	**prevGKLogFilePut** hostname, username, password, directory path, filename
Description:	The logFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the IP Line card's previous gatekeeper log file to specified location on the host.
Example:	ITG> prevGKLogFilePut "47.82.xx.xxx","anonymous","guest","/prevDir", "GKlogFile"
Synopsis:	**hostFilePut hostname, username, password, directory path, filename, ITGFileName**
Description:	Transfers any file on the IP Line 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 IP Line card.
Example:	**ITG> hostFilePut "ngals042", "anonymous", "guest", "/hostDir", "hostFile", "/C:/CONFIG/CONFIG1.INI"**

Table 17
IP Configuration Commands

Synopsis:	**NVRIPSet** "IP address"
Description:	Sets the IP address in NVRAM.
Example:	**ITG> NVRRIPSet "47.23.34.19"**
Synopsis:	**NVRGWSet** "IP gateway"

Table 17
IP Configuration Commands

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:	**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**

Table 17
IP Configuration Commands

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 18
Card Commands

Synopsis:	**cardReset**
Description:	Performs a warm reboot of the IP Line card. The card has to be in OOS state to be able to use this command.

Table 19
DSP Commands

Synopsis:	**DSPReset *DSPNumber***
Description:	**Resets the specified DSP**
Example:	**ITG>DSPReset 0**
Synopsis:	**DSPSelfTest *DSPNumber***
Description:	**Runs selftest on the DSP**
Example:	**ITG>DSPSelfTest 0**
Synopsis:	**DSPNumShow *DSPNumber***
Description:	**Prints number of DSPs on IP Line card.**
Example:	**ITG>DSPNumShow 0**
Synopsis:	**DSPPcmLpbkTestOn *DSPNumber***
Description:	**Stops pcm loopback test on the specified DSP.**
Example:	**ITG>DSPPcmLpbkTestOn 0**
Synopsis:	**DSPPcmLpbkTestOff *DSPNumber***
Description:	**Stops pcm loopback test on the specified DSP.**

Table 19
DSP Commands

Example:	**ITG> DSPPcmLpbkTestOff 0**
Synopsis:	**DSPSndLpbkTestOn *DSPNumber***
Description:	**Starts Send loopback test on the specified DSP.**
Example:	**ITG> DSPSndLpbkTestOn 0**
Synopsis:	**DSPSndLpbkTestOff *DSPNumber***
Description:	**Stops Send loopback test on the specified DSP.**
Example:	**ITG> DSPSndLpbkTestOff 0**
Synopsis:	**DSPRcvLpbkTestOn *DSPNumber***
Description:	**Starts Receive loopback test on the specified DSP.**
Example:	**ITG> DSPRcvLpbkTestOn 0**
Synopsis:	**DSPRcvLpbkTestOff *DSPNumber***
Description:	**Stops Receive loopback test on the specified DSP.**
Example:	**ITG> DSPRcvLpbkTestOff 0**

Table 20
Gatekeeper Query Commands

Synopsis:	**GKInfoShow**
Description:	Prints the following gatekeeper information on the active leader/backup leader IP Line card: • IP Client registration renewal time interval • Gateway registration renewal time interval

Table 20
Gatekeeper Query Commands

Synopsis:	**GKClientInfoShow**
Description:	Prints the following information for all registered IP Clients on the active gatekeeper (active leader card), including: • IP Client transport addresses (i.e., Call Processing and RAS IP addresses) • IP Client alias (i.e., DN) • IP Client endpoint ID
Synopsis:	**GKGWInfoShow**
Description:	Prints the information for all registered ITG IP Line cards (Gateways) on the active gatekeeper (active leader), including: • Gateway transport addresses (i.e., Call Processing and RAS IP addresses) • Gateway alias (i.e., TN) • Gateway DN table (i.e., list of DNs served by the Gateway)
Synopsis:	**GKCallInfoShow**
Description:	Prints the call information for all calls admitted by the gatekeeper (on the active leader card) that are currently active or in progress, including: • IP Client endpoint information • Gateway endpoint information • Direction of call (i.e., Originating from IP Client or Terminating to IP Client). • Start time.

Table 21
Operational Measurement Queries

Synopsis:	**resetOM**
Description:	**This command will reset all operational measurement parameters having been collected since last log dump.**

Table 22
Log File Commands

Synopsis:	**logFile on/off**
Description:	**turn on/off the log file**
Synopsis:	**logStatus**
Description:	**Display the modes of all log files/alarms.**

IP Line card selftests

During power-up, the IP Line card performs diagnostic tests to ensure correct operation. The faceplate RS-232 port on the IP Line 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 IP Line 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 IP Line 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 IP Line 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 IP Line 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 IP Line 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 IP Line card. The faceplate LCD display reads "BIOS."

Problem

the IP Line card has booted the BIOS load.

Diagnosis

in the event of a failure to load and run the ITG software, the IP Line 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 absence 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 IP Line 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 IP Line card.

Case 3: The escape sequence "xxx" is rarely transmitted. Reboot the card.

Warm rebooting the IP Line card

The following ITG shell command performs a warm reboot of an out-of-service IP Line card: **cardReset**

Testing the IP Line 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 IP Line 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 output 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: I/O, maintenance and extender cable description

This appendix describes the NTMF94DA, NTAG81CA and NTAG81BA cables.

NTMF94DA I/O cable

The NTMF94DA provides the E-LAN, T-LAN ports that provide the interface from the IP Line 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 26). Table 23 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 250 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 26
NTMF94DA E-LAN, T-LAN & RS-232 Serial Maintenance I/O cable

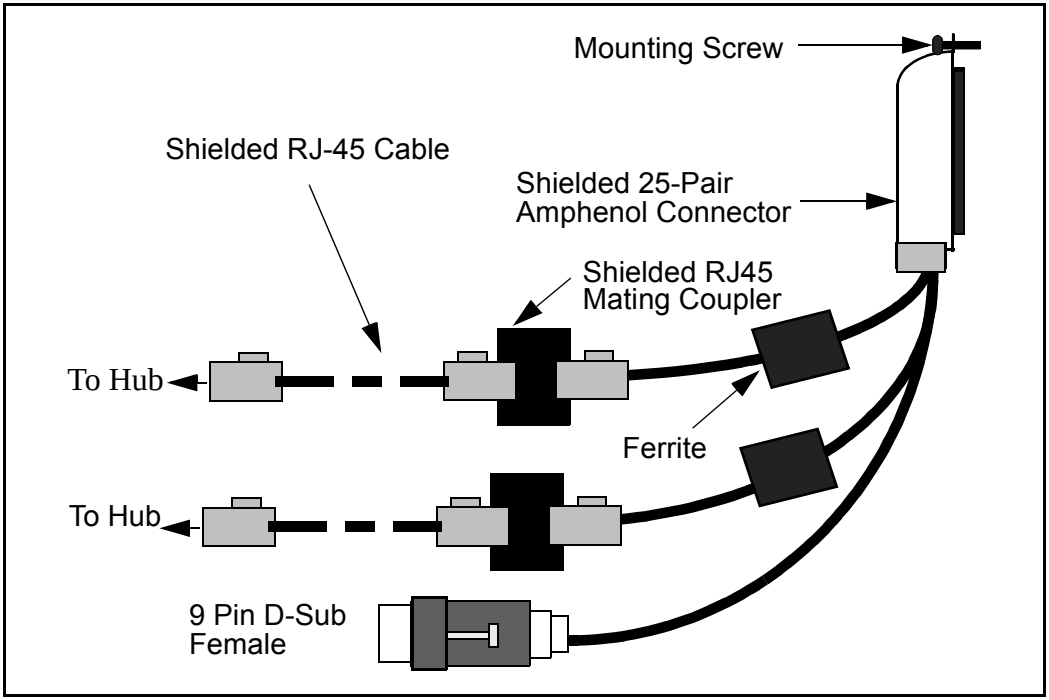


Table 23
NTMF94DA cable pin description (Part 1 of 2)

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 23
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.

WARNING

The NWT port connector on the faceplate is similar to the DB9 maintenance port connector on the NTMF94DA and NTAG81BA cables. Do not connect a serial cable to the faceplate NWT port as this will result in incorrect and unpredictable IP Line card operation.

NTAG81CA maintenance cable description

You connect this cable between the 9-pin D-type RS232 input on a standard PC and the MAINT connector on the NT8R17AB faceplate .

Figure 27
NTAG81CA Maintenance cable

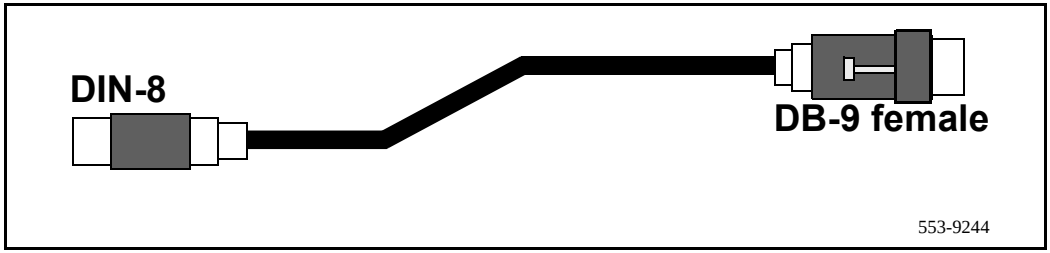


Table 24
NTAG81CA maintenance cable pin description

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 3m cable connects the NTAG81CA cable to a PC or terminal. It has a 9-pin D-type connector at both ends, one male, one female. It can also be used to extend the serial port presented by the NTMF94DA I/O panel cable.

Figure 28
NTAG81BA Maintenance Extender cable

Table 25
NTAG81BA Maintenance cable pin description

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

Appendix B: Product integrity

This chapter presents information about the NT8R17AB Meridian Integrated IP Telephony Gateway (ITG) Line 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 17.68 years. Failures per 10^6 hours of operation are 6.451, based on 40 degrees C (140 degrees F).

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 26 for a display of acceptable temperature and humidity ranges for the IP Line card.

Table 26
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 27 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 27
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 28 lists electro-magnetic emissions regulations met by the ITG card, along with the country's standard that lists each regulation.

Table 28
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 29 lists electro-magnetic immunity regulations met by the ITG card, along with the country's standard that lists each regulation.

Table 29
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: Subnet mask conversion 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 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 30, 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 30, 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, the complete subnet mask in dotted decimal format is 255.255.240.0.

Table 30
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

Index

Meridian 1

Meridian Internet Telephony Gateway (ITG) Line 1.0/IP Telecommuter

Description, Installation and Operation

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits of a Class A digital device pursuant to Part 15 of the FCC rules and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.
SL-1 and Meridian 1 are trademarks of Nortel Networks.
Publication number: 553-3001-119
Document release: Standard 2.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.