Meridian 1 and Succession Communication Server for Enterprise 1000

802.11 Wireless IP Gateway

Description, Installation and Operation

Document Number: 553-3001-206
Document Release: Standard 2.00
Date: April 2002

Printed in Canada

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.

Revision history

April 2002

Standard 2.00. This document is up-issued to include new content associated with the Succession CSE 1000 system. The name of this document is changed from “e-mobility 802.11 Wireless IP Gateway for Meridian 1” to “802.11 Wireless IP Gateway”.

September 2001

Standard 1.00. This document is issued for the first release of the e-mobility 802.11 Wireless IP Gateway for Meridian 1.

Contents

Administration 115

I/O, maintenance and extender cable description 195

Product integrity 201

About this document

This document provides information on the 802.11 Wireless IP Gateway for Meridian 1 and Succession Communication Server for Enterprise 1000 systems. For purposes of readability, the product name in this document is referred to as the Wireless IP Gateway. The hardware is referred to as the ITG Wireless card.

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.

Description

Contents

This section contains information on the following topics:

Product overview

The Wireless IP Gateway provides the communication between the circuit switched telephony network and H.323 Wireless IP handsets on a corporate IP network in the Enterprise environment. Figure 1 on page 18 illustrates a typical scenario using Wireless IP Gateway.

> ***Note:*** The H.323+ protocol used in this application is an enhancement to the standard protocol to support access to Meridian 1 and Succession Communication Server for Enterprise 1000 features through the Wireless IP Gateway

The Wireless IP Gateway consists of an ITG Wireless card with specific Wireless Voice Over IP firmware. This combination of hardware and firmware provides a mobility gateway to telephony features on the Meridian 1 switch.

A subset of the Meridian 1 and Succession CSE 1000 feature set is available to the mobile end users, much like a regular digital telephone on the Meridian 1 switch. This feature subset includes the following:

- Calling Line ID
- Called/Calling Party Name Display
- Conference
- Call Transfer
- Call Park and Retrieve

- Visual Message Waiting Indication
- Call Forward All Calls
- Make Set Busy
- Dialed Access to Group Call
- Speed Call
- Ring Again
- Call Pickup
- Multiple Appearance Directory Number with optional Privacy Override
- Dial Access to Paging

Note: The Wireless IP Gateway displays text prompts on the screen of a Wireless IP handset as features are activated.

The ITG Wireless Card is the H.323 gateway between the switch and the H.323 mobile handsets and provides gatekeeper functionality. To the Meridian 1 and Succession Communication Server for Enterprise 1000 systems, the H.323 Wireless card is seen as an Extended Digital Line Card (XDLC). To the Wireless IP handsets, it is the H.323 Gateway.

The Wireless IP handset emulates an M2616 digital telephone, providing the translation of signalling messages between the Wireless IP handset and the Gateway. Figure 2 on page 18 illustrates the signalling path between the components in this system. A Wireless IP handset can be twinned with a wired telephone using a Multiple Appearance Directory Number. The Wireless IP handset user can access all Meridian 1 and Succession CSE 1000 call routing and networking features.

In the Wireless IP Gateway, the ITG Wireless Card is connected to a LAN to which Access Points are attached. Access points provide a bridge between the H.323 gateway and the Wireless IP handset user. These access points provide transparent access between the Ethernet (IP Network or LAN) and the Wireless IP handset user.

Figure 1
Typical Wireless IP Gateway scenario

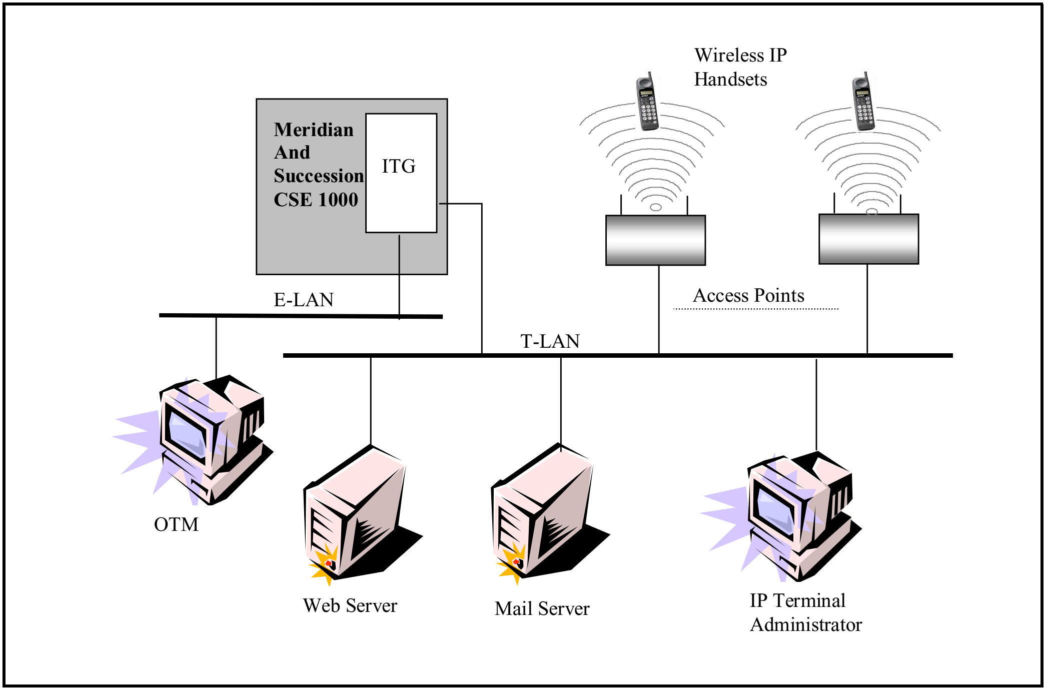
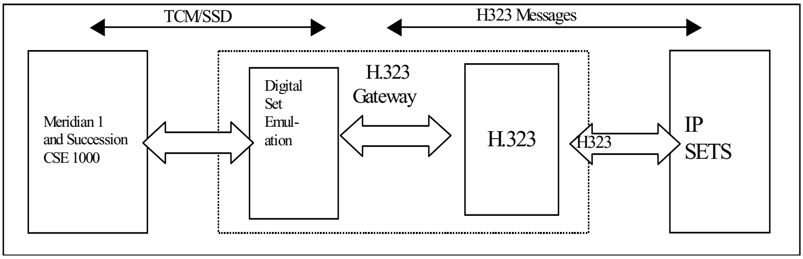


Figure 2
Wireless IP Gateway block diagram



System architecture

In the H.323 Meridian Wireless network, each ITG Wireless Card is equivalent to one H.323 zone, supporting a maximum of 24 Wireless IP handsets. In the Wireless IP Gateway, each Meridian 1 or Succession CSE 1000 system may have multiple H.323 zones, but each terminal is dedicated to one specific card or zone.

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.

Applicable systems

The Wireless IP Gateway is available for Meridian 1 Option 11C Mini, Option 11C, Option 51C/61C/81 and 81C systems running X11 release 25.30 or later software.

The Wireless IP Gateway is also available for Succession CSE 1000 systems running release 1.1 or later.

System requirements

The Wireless IP Gateway requires OTM 1.20 (or later). Table 1 lists required Wireless IP Gateway packages:

Table 1
Required packages for Meridian 1

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

Note: The required Wireless IP Gateway packages for Succession CSE 1000 are included in the Basic Service Software package.

Software delivery

The Wireless IP gateway software is shipped with each ITG Wireless card.

New or upgraded software is downloadable to the OTM PC through the Meridian 1 and Succession CSE 1000 website for the Wireless IP Gateway. This is the preferred method to upgrade the software. Refer to the product release bulletin for details on how to access this site.

System components provided by Nortel Networks

The following components comprise the Wireless IP Gateway: Meridian 1 and Succession CSE 1000, and the Optivity Management (OTM) System.

ITG Wireless card

The dual slot Pentium ITG Wireless card platform is based on an adaptation of IP Telecommuter. It emulates an Extended Digital Line Card (XDLC) using the H.323 standard with Nortel extensions (H.323+).Twenty-four users can be configured on each ITG Wireless Card.

The Pentium ITG Wireless card platform provides dual functionality, operating as both the Gatekeeper and the Gateway to the Meridian 1 and Succession CSE 1000 Wireless IP network. It performs the necessary conversion for both call signaling and voice stream/packets across the two interfaces.

Meridian 1 and Succession CSE 1000

The Meridian 1 and Succession CSE 1000 system provides the telephony features and call routing in the Wireless IP Gateway.

OTM

OTM is used for the installation, configuration and administration of the ITG Wireless Card(s) on the Meridian 1 and Succession CSE 1000.

System components provided by third party suppliers

In addition to the components provided by Nortel Networks, suitable LAN and WLAN infrastructure plus Wireless IP handsets, Wireless IP Administration are required from third parties.

Wireless IP handsets

The Wireless IP handset is an H.323+ Voice over IP terminal used with the Pentium-based ITG Wireless Card. Wireless IP handsets must be configured as Aries M2616 proprietary digital sets on the Meridian 1 side. Please refer to the vendor of the Wireless IP handsets for detailed installation, administration and maintenance procedures.

Access points

Access points provide a transparent bridge between the H.323+ gateway and the end mobile user. Multiple access points are used to meet network coverage requirements.

Package components

Table 2 on page 21 lists the Wireless IP Gateway package components for Meridian 1 and Succession CSE 1000 systems.

> *Note:* OTM 1.2 (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 package components for Meridian 1 and Succession CSE 1000 (Sheet 1 of 2)

Component	Code
802.11 Wireless IP Gateway for Meridian System Package (NTEZ01AA Wireless IP Gateway and required software licences, NTAG81CA PC Maintenance Cable, NTMF94EA ELAN, TLAN, RS232 Ports Cable, NTCW84JA ITG-specific 50-pin I/O Panel filter connector)	NTEZ01AA A0840932
I/O Panel ELAN, TLAN, RS232 Ports cable	NTMF94EA A0783470

Table 2
List of package components for Meridian 1 and Succession CSE 1000 (Sheet 2 of 2)

Component	Code
PC Maintenance cable	NTAG81CA A0655007
Meridian 1 100 Mbit I/O Backplane filter	NTCW84JA A0783483
IPE Shelf Backplane Tip Ring Cable	NT8D81AA A0359946
802.11 Wireless IP Gateway NTP CD-Rom	NTLH21AA A0845846
Large systems filter	
Meridian 1 ITG-specific 50-pin I/O panel filter connector	NTCW84JA A0783483

Ordering rules

- The OTM general package is a required pre-requisite that must be ordered separately.
- The Alarm and Notification application package is not included in OTM and must be ordered separately. (The OTM Premium Package is required to perform the upgrade.)
- The ITG Wireless Card requires two IPE card slots. In Europe, the left slot that the card occupies in an IPE shelf must be slot 0, 4, 8 or 12. To enable any IPE slot to be used, an IPE expansion kit (NT8D81AA) must be ordered.
- ISM system-limit parameters must be ordered. Refer to "ISM limits" on page 33.

ITG Wireless Card physical description

The Pentium-based ITG Wireless Card requires two card slots in an IPE shelf. Each ITG Wireless Card supports 24 configurable TNs. EMC limits the amount the number of ITG Wireless Cards that can be installed in the IPE module, or Option 11C system. See “ITG Wireless card provisioning rules for EMC compliance” on page 202.

Physical assembly

The ITG Wireless card assembly consists of a two-slot motherboard/ daughterboard combination. A PCI interconnect board connects the ITG motherboard and DSP daughterboard.

The core processor is an Intel Pentium II processor. The Intel 440BX chipset provides the system interface. The ITG Wireless Card has 32 MB of SDRAM memory, 4MB of file storage flash memory, 4MB of application flash memory, and 512 KB of BIOS flash memory. The BIOS loads the application memory. The ITG Wireless card has no switches or jumpers.

CAUTION
Damage to Equipment

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 must point toward the motherboard. Inserting the PCI Interconnect Board incorrectly may cause damage.

ITG Wireless card controls, indicators and connectors

Figure 3 on page 25 shows the ITG Wireless card faceplate components. The information in this section describes the components.

Faceplate components

Maintenance LED (Card Status)

The red status LED on the faceplate indicates the enabled/disabled status of the 24 card ports. The LED is lit during the power-up or reset sequence. The LED remains lit until the card is enabled by the Meridian 1 and Succession CSE 1000, then turns off. The LED remains lit if the self-test failed, the card is disabled, or the card is rebooted.

Reset switch

Press the Reset switch to reset the card without having to cycle power to the card. This switch is normally used after a card software upgrade to the card, or to clear a fault condition.

Ethernet Activity LED

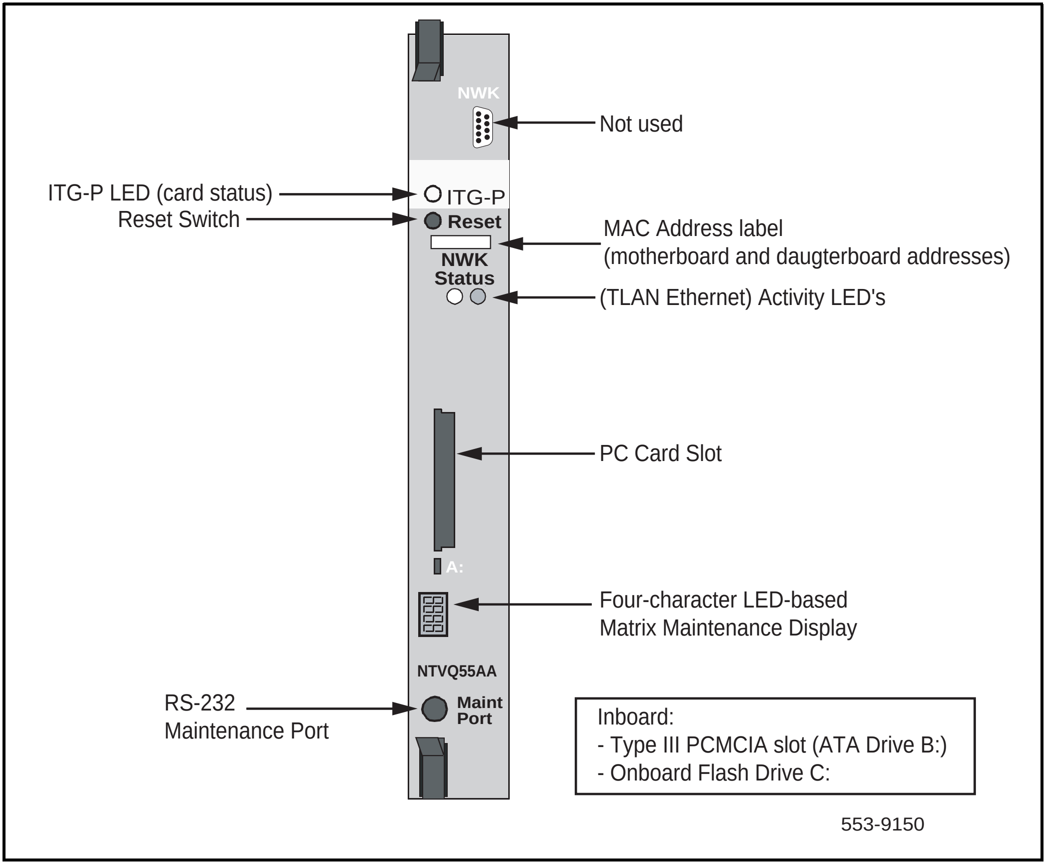
Ethernet Activity LEDs display the TLAN Ethernet activity.

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

PC Card slot

The ITG Wireless Card has one faceplate PC card slot (designated drive A:) on the faceplate. It is used for optional maintenance (backup and restore). The ITG Wireless also has one unused inboard slot (designated drive B:). The PC Card slot support PC-based hard disks (ATA interface) or high-capacity PC flash memory cards.

Figure 3
ITG Wireless Card faceplate



Maintenance display

A four character, LED-based, dot matrix display shows the maintenance status fault codes and other card state information.

RS-232 Maintenance Port (Maint Port)

The ITG Wireless Card faceplate provides a female DIN-8 serial maintenance port connection (labeled Maint Port). An alternative connection to the faceplate serial maintenance port exists on the NTMF94EA I/O panel breakout cable. **Do not** connect maintenance terminals or modems to the faceplate and I/O panel dB-9 male serial maintenance port at the same time.

Backplane Interfaces

The backplane connector provides the following interfaces:

- Network Interface
- ELAN (10BaseT).
  Inter-ITG Wireless Card communications for OA&M-related information are routed through the 10BaseT interface on the ITG host module.
- TLAN (10/100BaseT). Communications for voice and H.323 related information are routed through the 10/100BaseT interface on the DSP daughterboard.
- An alternate connection to the serial maintenance port.
  A serial device can only be connected through one port at a time. A TTY can be connected using an NTAG81CA cable for access to the ITG shell command line interface.
- Card LAN

ITG Wireless card functional description

The Pentium-based ITG Wireless card provides terminal and Gateway management such as registration/unregistration, and address resolution (DN to IP, and endpoint to gateway). The ITG Wireless card also maintains a list of terminals currently active on the network.

The ITG Wireless card controls the following:

- address translation
- admissions control
- call authorization
- call control signaling

- call management
- H.323 zone management

IMPORTANT

In the Wireless IP Gateway, every ITG Wireless card is a Leader card, providing both Gateway and Gatekeeper functionality.

The ITG Wireless card provides the following operational measurements specifically related to the Gatekeeper:

- Discovery request attempted
- Discovery confirmed
- Location request attempted
- Bandwidth request attempted
- Registration request attempted
- Registration confirmed
- Unregistration due to time-out
- Unregistration request attempted
- Admission request attempted
- Admission confirmed
- Disengage request attempted
- Authentication failures

Registration

The Wireless IP handsets must register with the designated ITG Wireless card. During the terminal registration process, the ITG Wireless card obtains the DN, and the associated IP address, from the registering IP terminal, and populates the terminal address translation database with entries of these active IP terminals.

Admission

Admission occurs when a Wireless IP handset or Gateway attempts to make a call. Admission occurs between both the originating and terminating sides and the Gatekeeper per H.323 line card.

The Gatekeeper function provides the mapping between the originating and terminating sides of the call (address translation). The mapping is a simple dynamic mapping between the Gateway and terminal.

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

Unregister and disengage

The Gatekeeper function also allows a terminal or Gateway to unregister and disengage. This allows terminals and Gateways to inform the Gatekeeper when they are finished using services.

Registration renewal: Time To Live

As the Gatekeeper confirms the terminal and Gateway registration in the initial registration request, the Gatekeeper specifies a *Time To Live* message for the terminal and Gateway. This is a deadline by which the terminals and Gateways must re-register in order to maintain registration. The purpose of *Time To Live* is to allow Gatekeepers, terminals, 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 if the Gatekeeper goes out of service. The Gatekeeper unregisters an endpoint that misses two consecutive registration renewals. If a call is active 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 IP Telecommuter). The terminals and Gateways are required to renew the registration with *keepAlive* indications within the specified time.

Management

The Gatekeeper requires one file, the Gatekeeper Table file, for management. Download this file to the card using the OTM “IP Telecommuter” application to the card.

Administration and maintenance

The Wireless IP Gateway provides two management interfaces:

- A Graphical User Interface (GUI) through the OTM 1.2 (or later)
- A Command-Line Interface (CLI) through Overlays

IP Telecommuter application

A PC configured with the OTM “IP Telecommuter” application is used to perform ITG Wireless card maintenance and administration. These functions include creating a node, adding cards, transmitting software to the cards, upgrading software, defining alarms, and other related tasks.

Command Line Interface

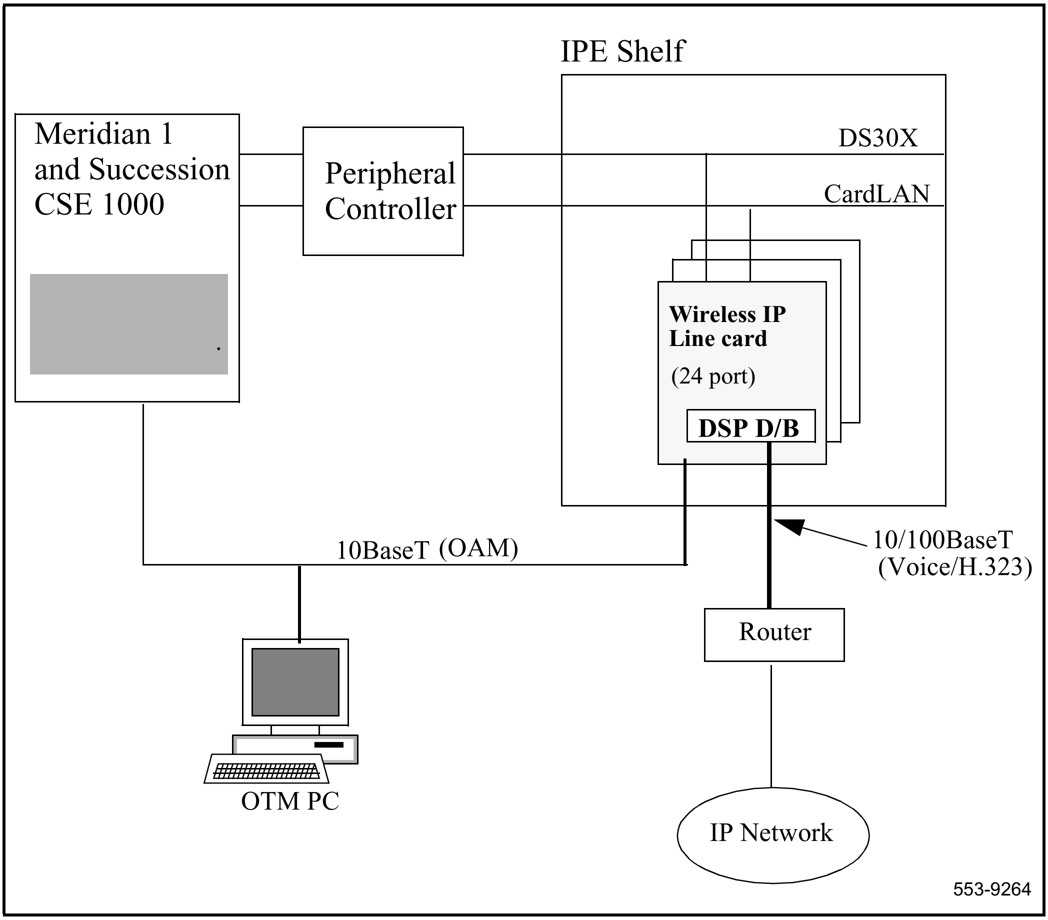
The ITG Command Line Interface (CLI) provides a text-based interface to perform some specific ITG Wireless card functions, including installation, configuration, administration and maintenance. The ITG CLI is normally accessed from the OTM ITG application by invoking the “Telnet to the card” from the **Maintenance|Card** menu.

The ITG CLI can also be accessed by connecting the COM port of a PC running a TTY or VT-100 terminal emulation program to the maintenance port on an ITG Wireless card through an NTAG81CA Faceplate Maintenance cable. Alternatively, a connection to the maintenance port can be made through the female dB9 connector on the NTMF94EA I/O Panel Ethernet and Serial Adaptor cable assembly, using the NTAG81BA Maintenance Extender cable.

With a CLI session established, the IP address of each ITG Wireless card can be entered. OTM uses the card’s IP address to carry out configuration and software download functions.

A list of ITG shell commands and Meridian 1 and Succession CSE 1000 system commands is described in Appendix F: “ITG Wireless commands” on page 219.

Figure 4
ITG Wireless card connectivity



Engineering Guidelines

Contents

This section contains information on the following topics:

Overview

This chapter provides guidelines and recommendations to help plan and engineer Meridian 1 and Succession Communication Server for Enterprise 1000 to support the Wireless IP Gateway card. It includes ITG Wireless card provisioning for EMC compliance, capacity engineering guidelines, and resource considerations.

System software requirements

The Wireless IP Gateway requires either Meridian 1 Release 25.30 software (or later) or Succession CSE 1000 Release 1.1 (or later).

The following packages are also required (when using Meridian 1):

Table 3
Required packages

Software Package	Package number
Digital Set (DSET)	88
Aries terminal (ARIES)	170

OTM version requirements

The Wireless IP Gateway requires OTM version 1.20.26 or later software.

ISM limits

Customers must purchase standard digital set M2616 ISM parameters. Meridian 1 uses one “Digital Telephone” ISM for each Wireless IP handset configured. Succession CSE 1000 uses one “E-mobility Extension” ISM for each Wireless IP handset configured.

Table 4 on page 34 describes the ISM parameters required to support the Wireless IP handsets on Succession CSE 1000.

Table 4
ISM parameters for Succession CSE 1000

Parameter	Code
8 Basic Services eMobility Extension ISM	NTM450CA A0861138
8 Advanced Services eMobility Extension ISM	NTM451CA A0861139
8 Premium Services eMobility Extension ISM	NTM452CA A0861140
Expansion 8 Basic Services eMobility Extension ISM	NTM453CA A0861153
Expansion 8 Advanced Services eMobility Extension ISM	NTM454CA A0861154
Expansion 8 Premium Services eMobility Extension ISM	NTM455CA A0861155

Wireless IP Gateway capacity

The maximum number of simultaneous calls per access point depends upon the codec used, the radio protocol used, and the manufacturer of the access point.

Each Pentium-based ITG Wireless card supports a maximum of 24 users. There is a one-to-one mapping between a Wireless IP handset and a unit on the ITG Wireless card. This is a non-blocking system. Each terminal has its own physical resource associated with it.

In Meridian 1 and Succession CSE 1000, IP Wireless IP handset register with one specific ITG Wireless card. There is no communication between ITG Wireless cards in the system.

Meridian 1 large system hardware capacity

On Meridian 1 Options 51 – 81C systems, there is no limit to the number of pentium-based ITG Wireless cards that can be installed, (other than physical limitations such as the physical size of the Meridian 1 switch and the number of IPE shelves).

The maximum number of ITG Wireless cards per IPE shelf = 8.

Meridian 1 small system hardware capacity

On Option 11C systems, there is a limit of 2 Pentium ITG Wireless cards per cabinet, if EMC Class B compliance is required. If EMC Class A is acceptable, there is no restriction imposed on the number of ITG Wireless cards per cabinet, other than the number of physical slots available. In summary,

- EMC Class A: Maximum ITG Wireless cards per cabinet = 5
- EMC Class B: Maximum ITG Wireless cards per cabinet = 2

On Option 11C Mini systems, there are no restrictions on the number of Pentium ITG Wireless cards, other than the physical limitations of card slot availability. There is no additional restriction if Class B compliance is required, as in the case of Option 11C systems.

Succession CSE 1000 hardware capacity

On Succession CSE 1000 each Media Gateway or Media Gateway expansion can support a maximum of two ITG Wireless cards.

Equipment considerations

The list of hardware components required in the Wireless IP Gateway is provided in Table 2, “List of package components for Meridian 1 and Succession CSE 1000,” on page 21. Additional information on the cables and their assembly is provided in Appendix A: “I/O, maintenance and extender cable description” on page 169.

ITG-specific I/O filter connectors

For Meridian 1 large systems, the standard IPE module filtering is provided by the 50-pin I/O panel filter connectors mounted on the back of the IPE shelf. The filter connector mounts externally to the MDF cables and internally to the NT8D81AA Backplane to I/O panel ribbon cable assembly.

Within the connector, all Tip and Ring pairs, including TLAN pairs, are filtered. For 100BaseT operation, replace the standard connector with the NTCW84JA connector, which is similar to the existing connectors, but instead has unfiltered TLAN Tip and Ring pairs.

For small Meridian 1 and Succession CSE 1000 systems, the standard I/O filter connector already supports 100BaseT operation.

Refer to "ITG-specific I/O panel filter connector" on page 75 for installation instructions.

CAUTION
For Meridian 1 large systems manufactured during the period of 1998 - 1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon assembly with a non-removable Filter Connector. The NT8D81BA is compatible with 10BaseT TLAN, but if you require a 100BaseT TLAN connection, you need to order and install the NT8D81AA Backplane to I/O Panel ribbon cable assembly. Do NOT try to install the NTCW84JA Filter Connector onto the existing non-removable Filter Connector.

ITG Wireless card resources

Every Wireless IP handset is controlled by one of the Pentium ITG Wireless cards. Allocate up to a maximum of 24 Wireless IP handsets to a single pentium ITG Wireless card. The following is found in the Wireless IP Gateway:

- Every Wireless IP handset can call every other Wireless IP handset, like any telephone connected in the Meridian 1 and Succession CSE 1000 systems.

- Every pentium ITG Wireless card is configured as a Leader card in OTM.
- There is a one-to-one correspondence between a Wireless IP handset and a particular unit on the ITG Wireless card.

Voice parameters

The perceived quality of a voice transmission is dependent on many factors, such as CODEC characteristics, echo canceller, jitter buffer size, and the perception of the individual listener.

Codecs

Both G.729A and G.711 codecs are supported on the Wireless IP Gateway.

Echo canceller

The echo canceller tail delay default setting is 32 ms. Always use the default tail delay of 32 ms.The voice activity detection is -20 to +10 dB. The default setting is -17. The default setting is “Enable echo canceller”. Always enable the echo canceller.

Transmit and receive gain adjustment

The transmit gain specifies the amount of gain applied in the Core switch-to-IP Network direction. The receive gain applies to the opposite direction. The default values emulate standard linecard behavior.

Increasing the Transmit Gain increases the volume in the Wireless IP handset ear piece. Increasing the Receive Gain increases the volume from the Wireless set mouthpiece.

> ***Note:*** Refer to *Read Me First* (P0992423) for specific values for supported Wireless IP handsets.

Voice payload size

This parameter controls the amount of voice data (specified in milliseconds) in each IP packet. For IP networks with a high packet loss rate, set the payload size as small as possible. If bandwidth is limited, increase the size of the payload.

Note: Refer to *Read Me First* (P0992423) for specific values for supported Wireless IP handsets.

Voice playout nominal delay (jitter buffer)

The jitter buffer parameters directly affect the end-to-end packet delay. Lowering the “voice playout” settings decreases one-way delay, but at the expense of giving less waiting time for voice packets that arrive late. Decreasing the nominal delay too much can cause unnecessary discard of late-arriving packets.

The size of the jitter buffer is statically configured, and is consistent for all devices in the network. The jitter buffer range is 0 – 200 ms.

Note: Refer to *Read Me First* (P0992423) for specific values for supported Wireless IP handsets.

Voice playout maximum delay

The maximum voice playout delay is the threshold value beyond which the jitter buffer must be re-centered. The recommended value is 120 ms for G.711 and G.729A codecs.

Voice Activity Detection threshold

The Voice Activity Detection (VAD) threshold parameter controls the sensitivity of the voice activation detection module.

Note: The voice activity detection is not recommended and is disabled by default. Modifying the VAD threshold has no effect.

Idle noise level

The idle noise level parameter controls the level of the comfort noise generated during periods of silence on voice calls. The recommended value is –65 dB.

Silence suppression

This parameter cannot be adjusted. By default, silence suppression is always turned off in order to maximize voice quality.

Audio Quality

Many factors affect audio quality with the ITG Wireless card. Refer to "ITG Network engineering guidelines" on page 41 for IP network aspects of audio quality.

Wireless transmission can introduce impairments to the audio quality which are not present on wireline calls. Minor fluctuations in RF quality, can degrade voice performance; this can be tolerated for short periods of time.

Nortel Networks uses transmission rating (R), as computed using the ITU E-Model, to characterize the voice performance of its voice-over-packet equipment. In general, values of R above about 60 are quite usable, although they fall in the lower range of quality obtained over wireline networks.

There is a potential to degrade the voice quality if codecs are cascaded. This can occur when there are multiple compression and decompression stages on a voice call. The more IP links utilized in a call, the more delay is added, and therefore the greater the impact on the voice quality. The following lists a few applications and devices which can impact voice quality:

- Voice Mail, for example, CallPilot, introduces another stage of compression and decompression
- Conferences can double the number of IP links
- IP Trunks can add additional stages of compression and decompression

To ensure optimal voice quality, it is recommended to minimize the number of compression and decompression stages and wherever bandwidth permits, use G.711 codec.

Voice messaging in conjunction with G.729A affects some listeners. For example, CallPilot uses a Nortel Sub Band Coding codec and CallPilot Mini uses G.723.1. If a Wireless IP handset is using G.729A and records a message, when another Wireless IP handset using G.729A retrieves the message there is additional distortion from cascading more than one codec type. Some users are satisfied with the resulting audio quality; however, others may prefer using G.711 for the Wireless IP handset when used in conjunction with CallPilot. Delay is not a factor when quantifying the quality because voice mail is not a two-way exchange.

During a call, tones that are inbound to the Wireless IP handset are carried inband, within the RTP audio packets. These tones are transcoded with the same codec as the speech and some people detect audible distortion. The distortion is potentially more noticeable with G.729A than with G.711.

In situations where bandwidth is a constraint (refer to "Bandwidth" on page 59), G.729A can be a suitable alternative to G.711.

The choice of codecs also affects the call carrying capacity of the associated Wireless LAN Access Points due to the shared bandwidth nature of that technology. The higher bandwidth required for the G.711 codec reduces the number of simultaneous calls that a given Wireless LAN Access Point can support compared to utilizing the G.729A codec. With either codec, increasing the packet size increases the call carrying capacity while adding delay. Refer to the vendor of the Wireless LAN and/or Wireless IP handsets for engineering guidelines on Access Point call carrying capacity.

ELAN and TLAN configuration

> ***Note:*** OTM refers to Telephony LAN (TLAN) as "Voice LAN" and Embedded LAN (ELAN) as "Management LAN".

Each ITG Wireless card has two ethernet ports, one for the TLAN and one for the ELAN. The ELAN and TLAN must be in separate subnets. The advantages of this configuration are:

- Optimization of VoIP performance on the TLAN segment by segregating it from ELAN traffic and connecting the TLAN as close as possible to the WAN router.
- Making the amount of traffic on the TLAN more predictable for QoS engineering.
- Optimization of ELAN performance. For example, for Symposium Call Center Server (SCCS) and CallPilot functional signaling, segregating the ELAN from ITG TLAN VoIP traffic.

- Enhanced network access security by allowing the modem router to be placed on the ELAN, which can be isolated from the customer's IP network, or have access to and from the IP network only through a firewall router.
- Meridian 1 and Succession CSE 1000 ELAN secure from unauthorized access

ITG Network engineering guidelines

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

In the data world in the late 1960s, IP evolved from a protocol that allowed multi-vendor hosts to communicate. The protocol adopted packet switching technology, providing bandwidth efficiency for data traffic that can tolerate high latency and jitter (variation in latency). Since IP supported the TCP transport layer, which provided connection-oriented and reliable transport, IP took on the properties of being connectionless and a best-effort delivery mechanism. The TCP/IP paradigm worked well in supporting data applications at that time.

New considerations come into play now when the same corporate network is expected to deliver voice traffic. The intranet introduces impairments, delay, delay variation, and data packet loss, at levels that are higher than those delivered by voice networks. Delay between talker and listener changes the dynamics and reduces the efficiency of conversations, while delay variation and packet errors introduce glitches in conversation. Connecting the ITG nodes to the corporate intranet without preliminary assessments can result in unacceptable degradation in the voice service; instead correct design procedures and principles must be considered.

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

1 Calculate ITG traffic. The technician must estimate the amount of traffic that the Meridian 1 and Succession CSE 1000 route through the ITG network. This in turn places a traffic load on the corporate intranet.

2 Assess WAN link resources. If resources in the corporate intranet are not enough to adequately support voice services, it is normally caused by not enough WAN resources.

3 Measure existing intranet's Quality of Service (QoS). The technician must estimate the quality of voice service the corporate intranet can deliver.

After the assessment phase, you can design and implement the ITG network. This design not only involves the ITG elements, but can also require making design changes to the existing customer intranet.

Traffic Engineering Guidelines

Note: OTM refers to “TLAN” as “Voice LAN” and “ELAN” as “Management LAN”.

TLAN traffic

Complete the following steps to determine the TLAN bandwidth in kbps:

1 Multiply CCS per Wireless IP handset by the total number of Wireless IP handsets.

2 Convert total CCS to erlangs by dividing it by 36 CCS.

3 Multiply the resulting erlangs by specific data rate from the Table 5 on page 43.

4 Use the following formula to calculate TLAN bandwidth:

TLAN bandwidth in kbps = CCS/phone*Total Wireless IP handsets*(TLAN kbps from Table 5 on page 43)/36

Table 5
TLAN and WAN data rate from one fully loaded voice channel (1 erlang traffic)

Codec	Frame Size (ms)	TLAN (kbps)	WAN (kbps)
G.711 (64kbps)	20	95	40
G.711	30	85	37
G729A (8kbps)	20	39	12
G729A	30	29	9
G729A	40	24	8
G729A	50	21	7
G729A	60	18	6.7

Example

24 Wireless IP handsets generate 9 CCS each to the ITG. What is the packet data rate these Wireless IP handsets offer to the TLAN? Codec setting: G.711 with 30 ms payload.

Solution

(24*9/36) * 85kbs = 510 kbps = 0.51 Mbps

This is the rate of packet data that the Ethernet TLAN is expected from 24 Wireless IP handsets at 9 CCS each. In other words, a TLAN of 10 Mbps (with 30% loading) can carry traffic from about 124 Wireless IP handsets at this traffic level.

Even if CCS per Wireless IP handset is 36, and codec is G.711 with 30 ms, the TLAN data rate required is still only about 2.3 Mbps, which is within the loading recommendation of a 10 Mbps Ethernet.

Note: When a 10Mbps Ethernet interface is exclusively used to carry voice traffic from 24 Wireless IP handsets to the ITG Wireless card, there is no need to do TLAN data calculation, regardless of codec and payload size used.

WAN Engineering

The main difference in assumptions between TLAN and WAN to produce Table 5 on page 43 bandwidth requirements are as follows:

1 TLAN is the 10 Mbps simplex type Ethernet (it could be a 100 Mbps duplex channel if so desired)

2 WAN channel is duplex; WAN packet size is based on IP packets being stripped off Ethernet overhead. No high level overheads, such as ATM or Frame Relay, are incorporated in the WAN table.

It is assumed that if a WAN is involved in the configuration, it is associated with the IP Trunk. A Wireless call arrives at the ITG Wireless card and is routed to an IP Trunk through a Media Card or ITG Pentium Trunk card in the gateway.

The WAN traffic must exclude Wireless to Wireless traffic and is the through traffic that passes from the Gateway to IP trunks. The following equation accounts for this fact, by including the "1-% intra-wireless" term.

The bandwidth requirement calculation is as follows:

WAN bandwidth = CCS/phone*Total Wireless IP handsets*(1-% intra-wireless)/36 *(Value from Table 5 on page 43)

Example 1

200 Wireless IP handsets, each generate 8 CCS to a CSE1000. 30% of calls are intra-wireless local calls, the rest are routed through IP Trunks (WAN) to terminate on a remote office. What is the WAN bandwidth requirement (assuming G729A and 30ms)?

Solution:

Plug in data to WAN formula:

WAN bandwidth = 200*8*(1-0.3)/36 * 9 kbps = 280 kbps = 0.28 Mbps

The incremental WAN traffic bandwidth is 0.28 Mbps.

When this parcel of traffic is routed through a TLAN before reaching the Gateway and WAN, it must be a part of the TLAN traffic requirement. This was illustrated in the TLAN example.

RF Engineering Issues

The distribution of Access Points (APs) is the customer's responsibility. Contact your wireless hardware supplier for more information.

There are a few items mentioned here to assist in understanding all the components affecting the operation of the ITG Wireless card and its corresponding Wireless IP handsets. These are as follows:

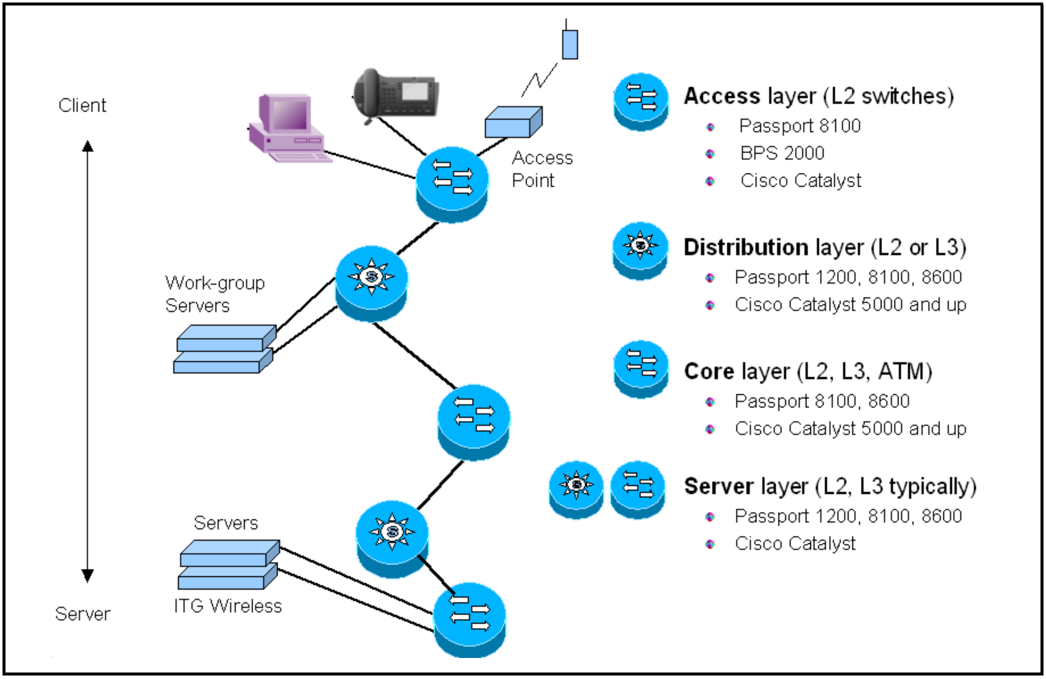
- Direct sequence and frequency hopping wireless systems utilize the same RF spectrum and can cause interference when in the same coverage area.
- RF interference can be detected by checking the RF statistics on the Wireless IP handsets. Check the CRC failures.
- It has been demonstrated that having too much overlap in the range of the APs can result in lost calls and in variable delay in the voice packet transmission. This is expected to be of greater concern with the Wireless IP Direct Sequence Wireless IP handsets.
- When using DS APs with diversity enabled, two antennas at the AP minimizes the impact of multi-path interference when units are in close proximity.

Enterprise IP Network Configuration

Typical network topology

Figure 5 on page 46 provides a reference model for a campus network.

Figure 5
Campus network reference model


Client
Access
Point
Work-group
Servers
Servers
ITG Wireless
Server
Access layer (L2 switches)
- Passport 8100
- BPS 2000
- Cisco Catalyst
Distribution layer (L2 or L3)
- Passport 1200, 8100, 8600
- Cisco Catalyst 5000 and up
Core layer (L2, L3, ATM)
- Passport 8100, 8600
- Cisco Catalyst 5000 and up
Server layer (L2, L3 typically)
- Passport 1200, 8100, 8600
- Cisco Catalyst

The following figures provide examples of logical connection diagrams for small, medium, and large campus networks. Other network designs can also be used. The actual design that is implemented depends on many factors, including physical locations, size, and scalability.

Figure 6 on page 47 is an example of a small campus network design.

Figure 6
Small campus network example

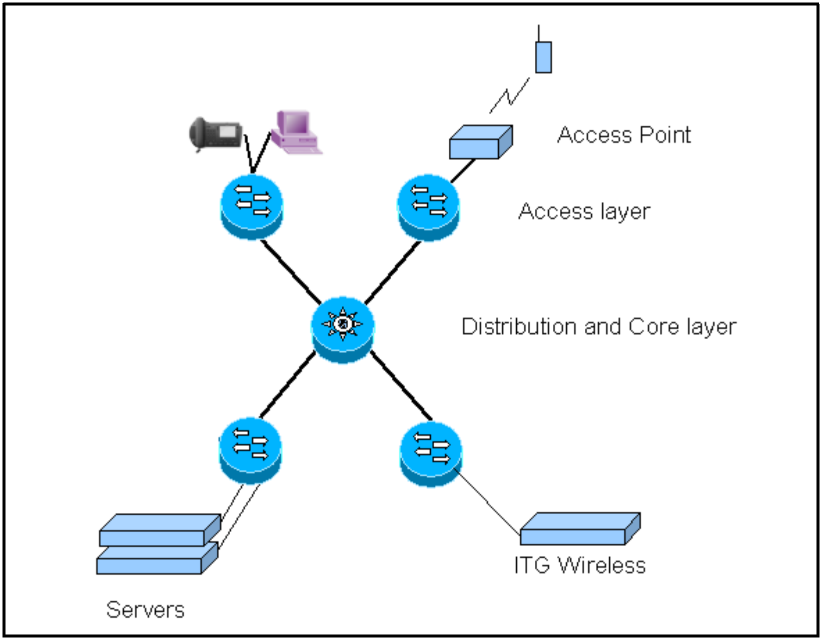


Figure 7 on page 48 is an example of a mid-size campus network design.

Figure 7
Mid-size campus network example

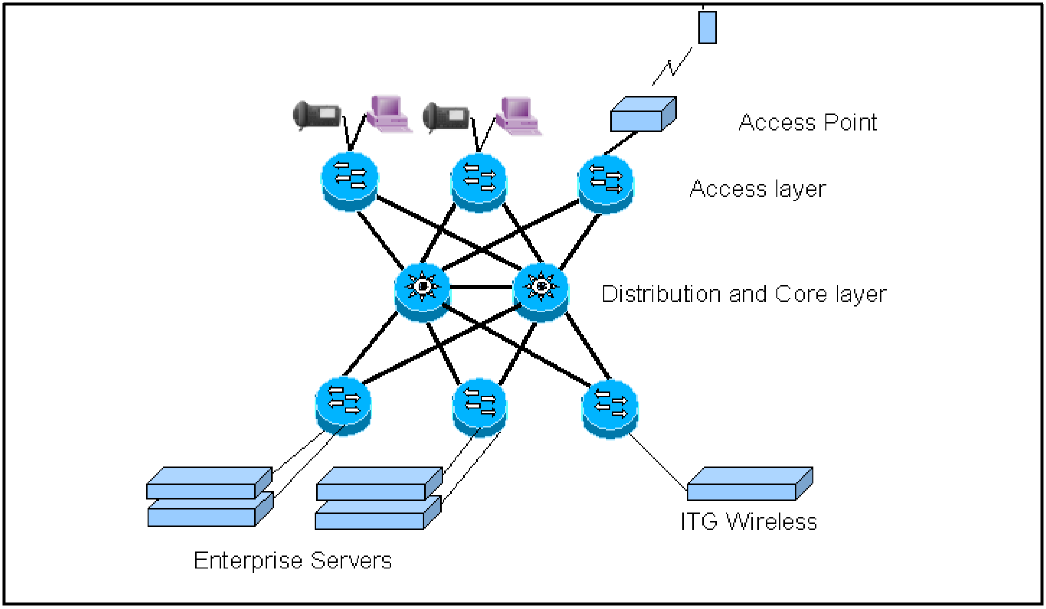
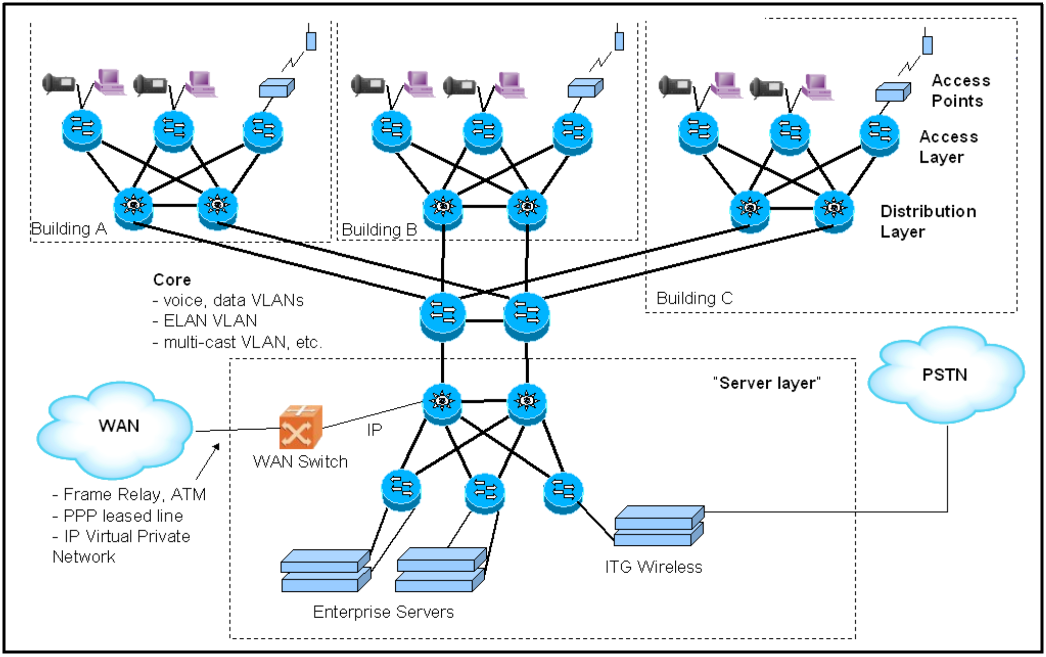


Figure 8 on page 49 is an example of a large campus network design.

Figure 8
Large campus network example



QoS problem locations

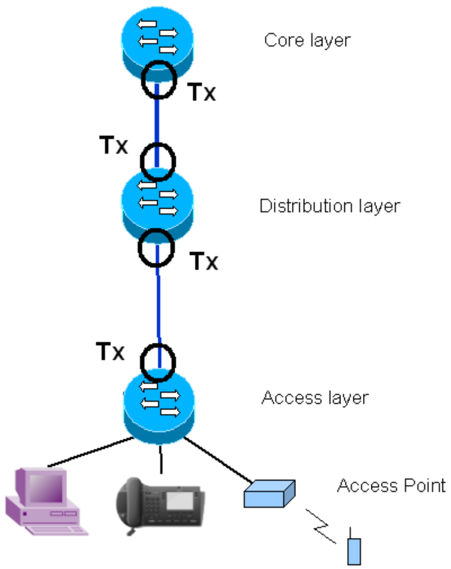
Figure 9 on page 50 identifies typical network congestion areas.

Voice traffic competes for the use of limited bandwidth on the uplinks. These uplinks are shown in Figure 9.

Congestion at these points causes the majority of all packet loss, delay, and jitter that is incurred. Using QoS mechanisms alleviates this congestion by using multiple queues with different priorities.

Figure 9
Campus network congestion points

- Voice traffic competes for the use of limited bandwidth on the "risers" (up-links).
- QoS mechanisms are meant to give voice traffic higher priority on these up-links.
- This applies to both layer two and layer three switches.



Roaming solutions

Wireless LAN technology inherently allows Wireless IP handsets to seamlessly roam from one Access Point to another within the same subnet. A basic subnet with 8 zero bits in the mask has up to 254 IP addresses. These IP addresses are shared among the Wireless IP handsets, the Wireless LAN Access Point, and any Wireless LAN NIC cards utilizing the network.

When additional roaming capability is required (either due to physical area or number of IP addresses), then the use of a Virtual LAN (VLAN) or DHCP is recommended.

VLAN configuration

Virtual LANs can be used to support Wireless VoIP roaming by extending the same sub-network to physically dispersed locations.

Campus wide VLAN network configurations make the network logically appear as a flat bridged network and can provide an ideal roaming solution for small to medium size networks.

Campus wide VLAN architectures do not necessarily scale well to large networks due to the following issues:

- All devices in a flat bridged network are within the same broadcast domain. This means that broadcast storms effect all devices in the VLAN.
- Managing and troubleshooting a flat bridged campus becomes increasingly difficult as the number of users increases.
- Scaling a flat bridged network can be difficult because broadcast traffic increases and STP convergence time increases. Switch administration and management can also become more difficult.
- VLANs can be implemented on layer two and layer three switches, providing adequate bandwidth on a flat VLAN campus network. Broadcast storms sometimes reduce the available bandwidth.
- Network security is limited within a flat bridged network. Any user logging onto the network can potentially disrupt any other user.
- VLANs can belong to either single or multiple spanning tree groups. This varies among vendors and switch models.
- Network redundancy is addressed with spanning tree protocol. Link failures cause the spanning tree to be recalculated. This results in network outages (of typically 40 to 50 seconds), while the spanning tree protocol calculates the new network topology.

Network Implementation

Wireless VoIP handsets can be allocated to a separate voice VLAN in order to avoid problems caused by broadcast storms elsewhere on the network

Campus wide VLANs require tagged trunks between all switches.

Every access point must be on the same VLAN in order to support roaming. This is configured by assigning the access point’s layer two switch port to a specific port based default VLAN. The access points’ layer two switch port is configured as untagged, the default (PVID, native, static) VLAN being the Wireless VoIP VLAN.

Wireless VoIP VLAN membership can be configured by associating the MAC address of a Wireless VoIP handset with the Wireless VoIP VLAN. This is known as MAC address based VLANs.

Some MAC addresses based VLANs are not scalable.

Some vendors implement a central VLAN management server in order to configure switch port VLAN memberships by asking a central database for the VLAN membership of a device based on the devices MAC address.

Configuration of VLANs varies between layer two switch vendors. Refer to the layer two switch user manual for VLAN configuration details.

Virtual routers must be configured for each VLAN if the ITG Wireless card is installed on another sub-net or VLAN.

Connecting the ITG Wireless card to the Wireless VLAN may increase overall network security if the Wireless VLAN / sub-network is made to be non-routable.

> ***Note:*** Do not assign a virtual router to the Wireless VoIP VLAN, thus allowing no users on the Wireless VLAN to gain access to the rest of the network.

Refer to the layer three switch/router user manual for detailed instructions on configuring virtual router interfaces.

DHCP

If available, Dynamic Host Configuration Protocol (DHCP) allows Wireless IP handsets to acquire an IP address within the subnet where they are located prior to registering with the ITG Wireless card. This is typically performed on a power cycle of the Wireless IP handset. The Wireless IP handset will maintain this new IP address for a time specified by the DHCP server.

The ITG Wireless card gatekeeper maintains a list of registered Wireless IP handsets and their associated IP addresses. The Wireless IP handset is removed from the list upon user logout or automatically after twice the registration renewal time. If a Wireless IP handset attempts to register with a new IP address while still on the list, then the registration will fail.

In a typical example, using DHCP to allow roaming between physically separate locations, the user of the Wireless IP handset:

- logs off and powers down the handset prior to leaving the first location
- powers up and logs on the handset when entering the new location.

For more details on DHCP, refer to Appendix E: "DHCP Supplementary Information" on page 211.

Wireless LAN Security

When implementing network security the following basic requirements must be addressed: authentication and availability, integrity and privacy. Authentication and availability must be addressed to ensure that data is only available to authorized parties. Integrity must be addressed to ensure that data appearing on the network in genuine. Privacy must be addressed to ensure that conversations cannot be overhead by unauthorized parties.

An improperly implemented wireless network can potentially allow unauthorized parties with Wireless network interfaces to obtain access to the rest of the data network.

Authentication on a Wireless LAN is addressed through the use of a standards-based authentication, MAC access control list, or unique Subscriber Service Identifier.

> ***Note 1:*** For information about the 802.11 Authentication scheme, refer to your Wireless LAN vendor.

> ***Note 2:*** Simple firewalls are usually implemented through access lists that identify traffic based on identifiers such as IP address, port number, or protocol. Simple firewalls often do not satisfy the three basic requirements, particularly authentication and availability. Solutions meeting all three requirements are often more desirable.

Integrity can be ensured through the use of encryption. Encryption techniques available include Wireless Equivalency Privacy ("WEP") algorithm, or DES encryption.

Privacy and confidentiality are also achieved through encryption. A network card in running a sniffer application can potentially capture open-air Wireless transmissions. Encrypted transmissions can be difficult, if not impossible to decode in any reasonable amount of time.

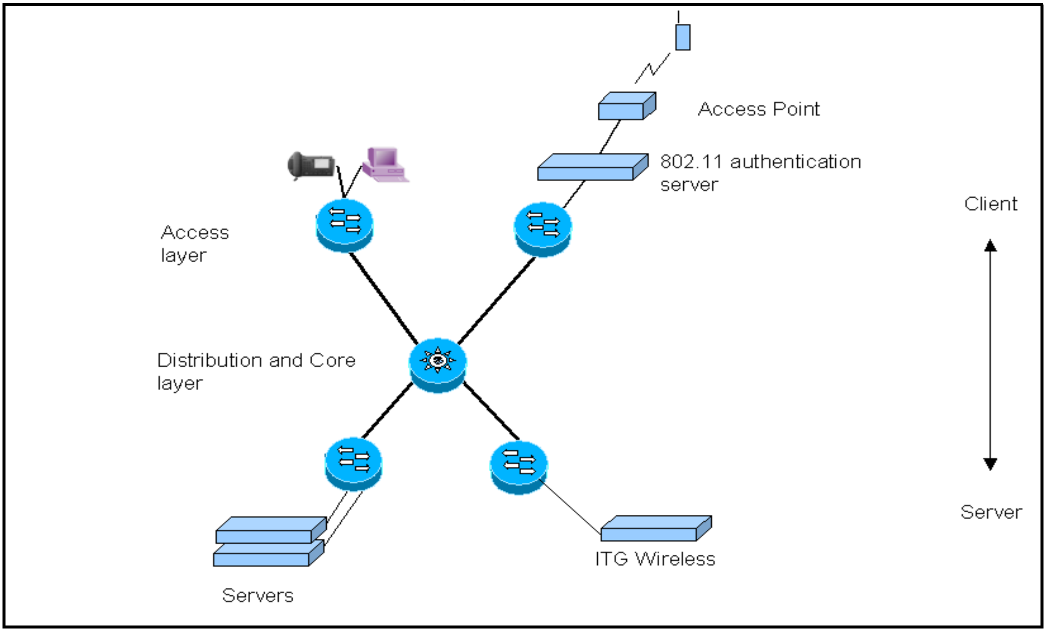
> ***Note:*** WEP is easily compromised. It has been demonstrated that it can be broken in close to real time.

802.11 Authentication Server

Suggested solutions for a securing a Wireless IP network are:

1. The authentication, integrity, and confidentiality of network data, can be achieved by deploying an authentication based gateway and firewall between the Wireless IP network and the rest of the network.

Figure 10
Authentication Server and firewall deployment

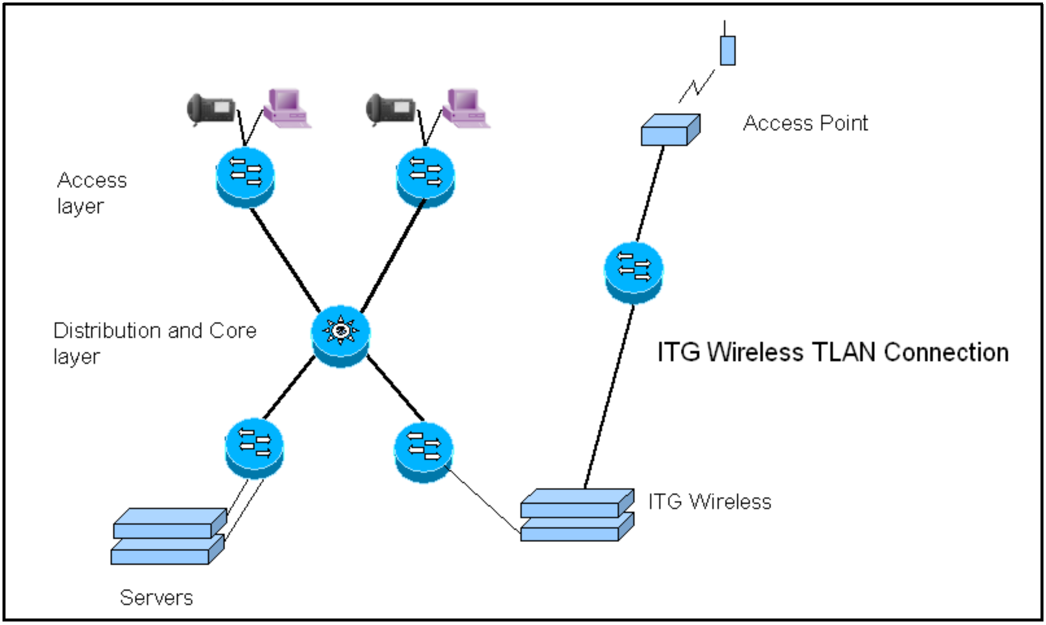


Once clients are authenticated they are allowed through the firewall.

2 Isolated Wireless IP network:

The Wireless IP gateway is directly connected to the Wireless IP network. The Wireless network is then isolated from the rest of the customer's network.

Figure 11
Isolated LAN deployment



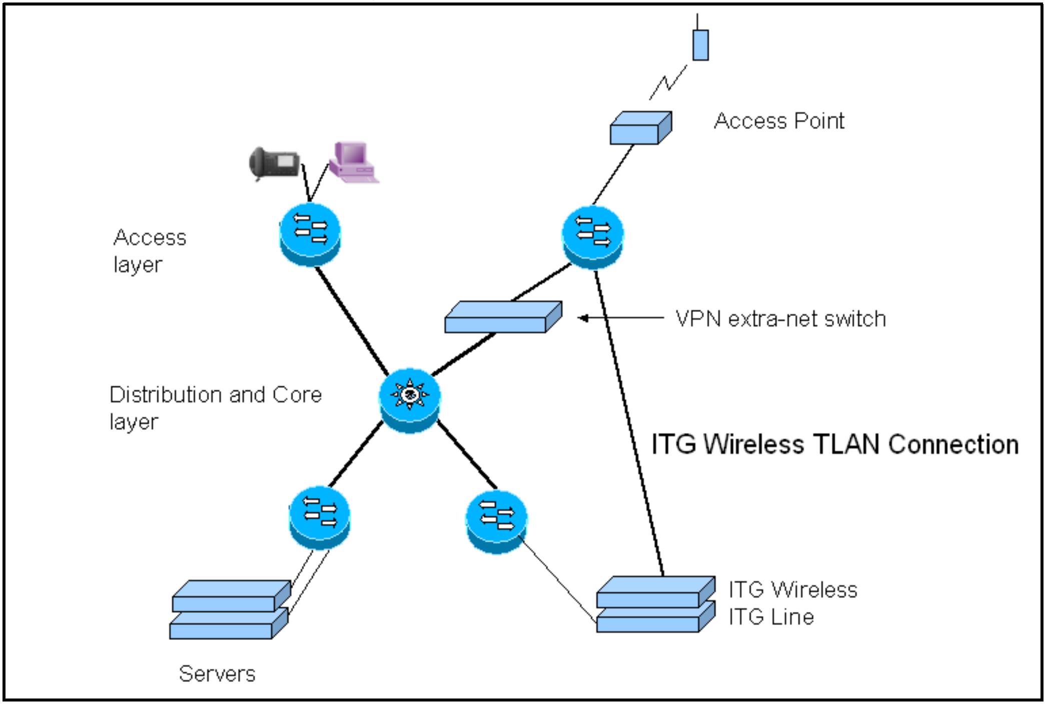
3 Virtual Private Network Tunneling:

Wireless IP sets would be deployed on an isolated Wireless IP network. The Wireless IP network would be connected to the rest of the network by a VPN capable extra-net firewall switch, such as Nortel Networks Contivity extra-net switch.

Access from authorized PCs can be achieved by tunneling a VPN through the Wireless network to the VPN firewall.

For example, Nortel Networks Contivity extra-net client can connect to a Contivity extra-net switch via a VPN connection. This provides authentication, data integrity, and privacy, therefore making any type of attack on the network much more difficult.

Figure 12
Isolated LAN with VPN tunnelling



Voice network analysis

Quality of Service (QoS)

Several QoS parameters can be measured and monitored to determine if desired service levels are provided and obtained. These parameters consist of the following:

- network availability
- bandwidth
- delay

- jitter
- loss

There are two QoS parameters that affect performance, but cannot be measured. They provide the traffic management mechanisms for network routers and switches. These parameters are as follows:

- emission priority
- discard priority

All of these QoS parameters affect the application's or end-user's level of service.

Evaluation process overview

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

In the process, it is assumed that the Ping program is available, or some network management tool which can collect delay and loss data that is accessed to the TLAN connecting to the Router going out to the Intranet:

1 Use *ping* or equivalent tool to collect round-trip delay (in ms) and loss (in%) data.

2 Divide the delay by 2 to approximate one-way delay, add the ITG processing and buffering time. (For more information refer to "Adjusting jitter buffer size" on page 66.)

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

4 If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

Set QoS

The users of corporate voice and data services expect these services to meet some perceived quality of service (QoS) which in turn influence network design. The goal is to design and allocate enough resources in the network to meet users' needs. QoS metrics or parameters are what quantifies the needs of the "user" of the "service".

In the context of a Meridian 1 and Succession CSE 1000 systems, there are two interfaces that the technician needs to consider.

- The Meridian 1 and Succession CSE 1000 (including the ITG nodes) interfaces with the end users; voice services offered by the need to meet user-oriented QoS objectives.
- The ITG nodes interface with the intranet; the service provided by the intranet is "best-effort delivery of IP packets", not "guarantee QoS for real-time voice transport." The ITG translates the QoS objectives set by the end-users into IP-oriented QoS objectives. The guidelines call these objectives intranet QoS objectives.

Network availability

Network availability has the most significant effect on QoS. If the network is unavailable, even for brief periods of time, the user or application can achieve unpredictable or undesirable performance levels.

Network availability is dependent on the availability of a redundant network. A redundant network should include the following elements:

- redundant devices such as

— interfaces

— processor cards

— power supplies in routers and switches

- resilient networking protocols
- multiple physical connections, such as copper or fiber
- backup power sources

Bandwidth

Bandwidth is also a significant parameter that affects QoS. There are two types of bandwidth:

1. Available Bandwidth
2. Guaranteed Bandwidth

Available bandwidth

Many network operators oversubscribe the bandwidth on their network to maximize the return on their network infrastructure or leased bandwidth. Oversubscribing bandwidth mans that the bandwidth a user subscribes to is not always available. All users compete for Available Bandwidth. The amount of bandwidth available to a user depends on the amount of traffic from other network users at any given time.

When using the Wireless IP network for data and voice, high data traffic (such as, ftp, RF set firmware updates) can interfere with the Wireless IP handset's ability to make and receive calls. A call in progress should not be affected since voice received priority at the AP. The RF update of set configuration requires less little traffic and is not expected to interfere with calls.

Guaranteed bandwidth

Some network operators offer a service that guarantees a minimum bandwidth and burst bandwidth in the Service Level Agreement (SLA). This service is more expensive than the Available Bandwidth service. The network operator must ensure that the Guaranteed Bandwidth subscribers get preferential treatment (QoS bandwidth guarantee) over the Available Bandwidth subscribers.

This can be accomplished in several ways. Sometimes, the network operator separates the subscribers by different physical or logical networks, such as Virtual Local Area Networks (VLANs) or Virtual Circuits. In other cases, the Guaranteed Bandwidth traffic shares the same infrastructure as the Available Bandwidth traffic. This is often seen where network connections are expensive, or the bandwidth is leased from other service providers. When both types of subscribers share the same infrastructure, the network must be able to prioritize the Guaranteed Bandwidth traffic over the Available Bandwidth traffic. This ensures that when network traffic is heavy, the Guaranteed Bandwidth subscriber’s SLA is met.

Burst Bandwidth

Burst bandwidth is defined as the amount and the duration of excess bandwidth use (burst) above the guaranteed minimum bandwidth. QoS mechanisms can be activated that discard traffic that is consistently above the Guaranteed Bandwidth agreed upon in the subscriber's SLA.

Delay

Delay is defined as the wait time from when an application's data is sent, to when it is received. Delay causes significant QoS issues with voice and video applications. Other applications, such as Fax transmissions and System Network Architecture (SNA), simply time-out and fail with excessive delay.

The delays inherent in IP telephony restrict the number of TDM to IP and IP to TDM transmissions in a call

Some applications can compensate for specified amounts of delay, but once that amount is exceeded, the QoS is compromised. One example of compensation is network equipment that imitates an SNA session on a network. The equipment sends local acknowledgements when the network delay would cause the SNA session to time-out. VoIP and gateways also provide delay compensation by using local buffering.

Delay can be fixed or variable. Some examples of fixed delay are as follows:

- application-based delay, such as:
  - voice Codec processing
  - IP packet creation time required by the TCP/IP software stack
- data transmission wait-time (queuing delay) at each network hop of the physical network
- propagation delay – the delay caused by the finite speed at which electronic signals can travel through a transmission medium.

Some examples of variable delay are as follows:

- queuing delay for traffic entering a network node
- contention (vying for access) with other traffic at each network node
- queuing delay for traffic exiting a network node

Variable delays are affected by the amount of network traffic.

Table 6 on page 61 describes the delays of various scenarios with different codecs.

Table 6
Known System Delay

One-way Call Scenarios	G711 codec delay (ms)	G729A codec delay (ms)
Wireless IP Handset to 2616	132	161
Wireless IP Handset to Wireless IP Handset	261	290
Wireless IP Handset to i2004	268	298
Wireless IP Handset to i9050	217	233
Wireless IP Handset to 2616 via IP Trunk	242	261
Wireless IP Handset to Wireless IP Handset via IP Trunk	374	395
Wireless IP Handset to i2004 via IP Trunk	336	360

Note: This measured value represents the sum of codec encoding, decoding and jitter values.

Jitter

Jitter is defined as how much the arrival time between consecutive packets varies, within a given traffic flow.

Jitter has a pronounced effect on real-time, delay-sensitive applications, such as video and voice. These applications need to receive packets at a fairly constant rate, with a fixed delay between consecutive packets. If the arrival rate varies, the jitter affects the application's performance. Minimal jitter might be acceptable, but if jitter increases, the application could become unusable.

Some applications, such as VoIP gateways and Wireless IP handsets, can compensate for a finite (specified) amount of jitter. Voice applications require the audio to play at a constant rate. If the next voice packet does not arrive within the playback time, the application replays the previous voice packet until the next voice packet arrives. If the next packet is delayed too long, it is discarded when it arrives. This results in a small amount of distorted audio.

All networks have some jitter. This is due to the differences in delay created by each network node, as packets are queued. If jitter is contained within Jitter Buffer size, QoS can be maintained.

Loss

Physical medium loss

Loss is defined as the drop in the level of signal strength between two points on a network. Loss can occur due to errors created by the physical medium used to transmit the data. Most landline connections have very low loss (measured in Bit Error Rate {BER}).

Wireless connections, such as satellite, mobile, or fixed Wireless networks, have a high BER. The BER can vary due to the following:

- radio frequency interference
- cell handoff during roaming calls
- weather conditions, such as fog and rain
- physical obstacles such as trees, buildings, and mountains

Wireless technology usually transmits redundant information, since packets are often dropped during transmission due to the physical medium.

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. In voice conversation, packet loss appears as gaps in the conversation. Sporadic loss of a few packets can be more tolerable than infrequent loss of a large number of packets clustered together.

> ***Note:*** For high quality voice transmission, the long-term average packet loss must be < 1%, and the short-term packet loss must not exceed 5% in any 10 second interval.

Measuring end-to-end packet loss

The PING program also reports whether the ICMP packet made its round trip successfully or not. Use the same PING host setup to measure end-to-end error, and, in making delay measurement, use the same packet size parameter.

Sampling error rate, however, requires taking multiple PING samples (at least 300 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).

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. A packet is late if its delay exceeds the voice playout maximum delay provisioned through OTM.

For example, assume:

- The average one-way delay is 50 ms.
- The jitter buffer is set to a nominal (or average) value of 60 ms
- Then the maximum value is 2 x 60 + 50 = 170 ms.

Therefore, any packet which exceeds the maximum delay is discarded and must be added to the total number of packets lost. A “site pair” is defined as the measurement between the host ITG and the remote subnet served by a server.

Problem Resolution

Reducing delays

The link delay is the time it takes for a voice packet to be queued on the transmission buffer of a link until it is received at the next hop router. Link delay can be reduced by:

- upgrading link capacity. This reduces the serialization delay of the packet, but also reduces the utilization of the link and the queueing delay. Before upgrading a link the technician must check both routers connected to the link to be upgraded and make sure 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 ITG traffic, which can be derived from the traceroute output for each site pair. Then, using the intranet link utilization report, note the highest utilized and/or the slowest links. Estimate the link delay of suspect links using the traceroute results.

Example: a 256kbps link from router1 to router 2 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 the example 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 ITG Wireless card must be connected to the intranet to minimize the number of router hops between the ITG Wireless card and the Wireless IP handset. This reduces the fixed and variable IP packet delay, and improve the Voice Over IP Quality of Service. It is recommended that no more than one card utilize a particular 10BaseT LAN collision domain.

> ***Note:*** 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 ITG Wireless card node and the TLAN router should be placed as close to the WAN backbone as possible in order to:

- minimize the number of router hops.
- segregate constant bit-rate VoIP traffic from sporadic LAN traffic.
- simplify the end-to-end QoS engineering for packet delay, jitter, and packet loss.

If an access router separates the ITG Wireless card node from the WAN router, there must be a high-speed link (for example, 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 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.

Adjusting jitter buffer size

The jitter buffer parameters directly affect the end-to-end delay. Lowering the *voice playout* settings decreases *one-way dela*y, but this comes at the expense of giving less waiting time for voice packets that arrive late.

You adjust the jitter buffer size when you configure the DSP Profiles in the ITG IP Telecommuter application. The jitter buffer is statically configured and is the same for all devices in the network. The jitter butter size range is 0-200 milliseconds. The default value is 50 milliseconds.

As each call is set up, the jitter buffer for each device is set to the next larger configurable value for the selected codec. If the jitter buffer depth is configured as zero, the depth of the jitter buffer is set to the smallest value the device can support. In practice, the optimum depth of the jitter queue is different for each call. For sets that are on a local LAN connection, a short jitter queue is desirable to minimize delay. For sets that are several router hops away, a longer jitter queue is required.

Lowering the jitter buffer size decreases the *one-way delay* of voice packets; however setting the jitter buffer size too small causes unnecessary packet discard.

If the technician decides to discard packets, to downsize the jitter buffer, they must do the following:

- **Check the delay variation statistics.** 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 (s) of one-way delay for that flow.** It is recommended that the jitter buffer size should not be set smaller than 2s.

Installation and configuration

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *Installation Planning* (553-3001-120)
- *Features and Services* (553-3001-306)
- *Administration Input/Output Guide* (553-3001-311)

Overview

This chapter explains how to complete the following tasks:

- install and configure new ITG Wireless nodes, cards and associated cables
- configure ITG Wireless data on Meridian 1 and Succession Communication Server for Enterprise 1000
- configure ITG Wireless data on OTM and transmit to ITG Wireless cards
- upgrade ITG Wireless card software and firmware.

The following assumptions must be in place before proceeding with the installation:

- LAN infrastructure (wired and Wireless) installed and tested.
- OTM PC installed and available
- OTM IP Telecommuter application is installed

  Note: The DN to TN configuration in OTM must be coordinated with the Overlay 11 configuration.

- Required ISM parameters installed on Meridian 1 and Succession CSE 1000
- Review the “Engineering Guidelines” on page 31.

Installation procedure summary

Summary of steps

The following summary of steps can be used as a reference guide to install and configure an ITG Wireless card node.

> *Note:* Complete all installation and configuration steps before data is transmitted to the ITG Wireless cards.

Table 7
Installation procedure summary of steps

Step	Page number
Create the ITG Wireless card Installation Summary Sheet	71
Install ITG Wireless cards in Meridian 1 and Succession CSE 1000	73
Configuring data in Meridian 1 and Succession CSE 1000	78
Configure ITG Wireless card in OTM	80
Configuring card properties for Wireless IP handsets	89
Activate SNMP traps for ITG Wireless cards	97
Configuring security for SNMP access	99
Transmit configuration data	101
Verify card software	105

Create the ITG Wireless card Installation Summary Sheet

It is recommended that an ITG Wireless card Installation Summary Sheet, seen in Table 8 on page 72, be filled in as the cards are unpacked, inventoried, and provisioned in the Meridian 1 and Succession CSE 1000 system. IP information is normally be supplied by the customer’s IS department. Use the Installation Summary Sheet to facilitate entry of configuration data on Meridian 1 and Succession CSE 1000.

The MAC address is the Motherboard Ethernet address shown on the ITG Wireless card faceplate. The ELAN Management IP address is the address of the management interface used to perform management through OTM. The TLAN Voice IP address is the IP address of the voice interface.

Table 8
ITG Wireless card Installation summary sheet

Site:		**System:**		**Customer:**
Management LAN (ELAN): **Gateway IP:** ______________________________ **Subnet mask:** _____________________________ **SNMP Manager List IP:** _____________________		**Voice LAN (TLAN):** **Gateway IP:** ______________________________ **Subnet mask:** ____________________________		
Management MAC	**Management IP address**	**Node/Voice IP Address**	**Node Number**	**Card TN**

Install ITG Wireless cards in Meridian 1 and Succession CSE 1000

Each ITG Wireless card requires two slots in the Meridian 1 and Succession CSE 1000 shelf. Only the left slot of the card connects to the Meridian 1 and Succession CSE 1000 Backplane and I/O panel.

Install up to a maximum of eight ITG Wireless cards in an IPE shelf in Option 51C/61C/81/81C. The ITG Wireless card occupies any two adjacent slots in an IPE shelf, with the left slot of the card plugging into slots 0 to 6 and 8 to 15. You cannot plug in the left slot of an ITG Line card in slot 7, because the XPEC card is situated in-between slots 7 and 8.

To allow a module to hold the maximum number of ITG Wireless cards, install each card with the left slot of the card inserted into an even-numbered slot

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

Procedure 1
ITG Wireless card installation

1 For each ITG Wireless card, identify the IPE card slot selected for the ITG Wireless card. Use the information from the Table 9 on page 74.

Note: Although the ITG Wireless card is a two-slot card, only the left slot is counted for the card slot number. Example: the slot number is 2 for an ITG Wireless card installed in slots 2 and 3.

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

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

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

Note 1: The red LED on the faceplate remains lit until the card is configured and enabled in software, at which point it turns off.

Note 2: The faceplate display window displays startup selftest results (T:xx) and status messages. A display "F:xx" indicates a failure of the self-test. It is normal for the card to display "F:10" during the start-up self test.

Refer to "Faceplate maintenance display codes for card reset" on page 146 for a listing of display codes

End of Procedure

Table 9
ITG Wireless card installation by module type

Meridian 1 Modules	ITG Wireless card Slots
NT8D37BA/EC IPE modules, NT8D11BC/ ED CE/PE modules	All available IPE card slots.
NT8D37AA/DC IPE modules	0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	0

ITG-specific I/O panel filter connector

Note: This NTCW84JA ITG-specific Filter Connector is not required on Option 11C, 11C-Mini, or Succession CSE 1000 systems

CAUTION
For Meridian 1 large systems manufactured during the period of 1998 - 1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon assembly with a non-removable Filter Connector. The NT8D81BA is compatible with 10BaseT TLAN, but if you require a 100BaseT TLAN connection, you need to order and install the NT8D81AA Backplane to I/O Panel ribbon cable assembly. Do NOT try to install the NTCW84JA Filter Connector onto the existing non-removable Filter Connector.

Remove existing I/O panel Filter Connector

The standard I/O Filter Connector is shielded metal with a black plastic insert connector. The NTCW84JA connector uses yellow warning labels to indicate EMC filtering modifications and which MDF connection points can support 100BaseT connections.

Procedure 2
Remove existing I/O panel Filter Connector

1 Before any of the following steps, remove the ITG pack, or any other IPE pack, from the IPE shelf card slot corresponding to the I/O Panel connector to be removed.

Note: Use the I/O panel connector which corresponds to the left slot number of the DCHP card.

2 Remove the NT8D81AA Backplane to I/O Panel ribbon cable assembly, which is connected to the Backplane side of the existing block, by releasing the latching pins on the filter block and pulling the NT8D81AA cable away.

3 Unscrew the existing Filter Connector from the I/O panel. There is one screw on the lower front of the connector and one screw on the upper back of the connector. Remove the connector.

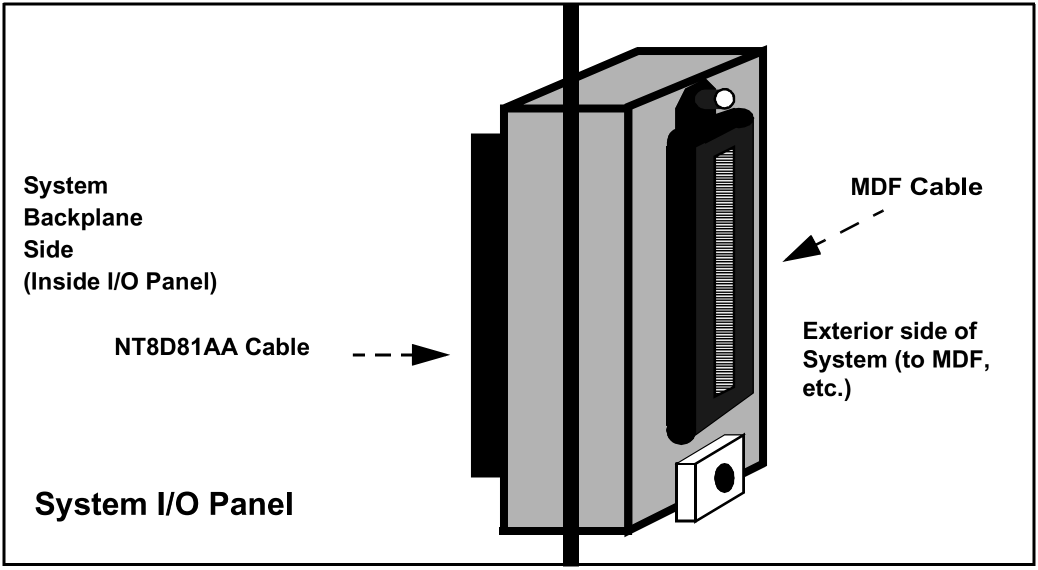
4 Re-position the new NTCW84JA Filter Connector in the now vacant I/O panel opening. (See Figure 13 on page 76.)

5 Attach the new NTCW84JA ITG-specific Filter Connector to the I/O panel by securely fastening the top back screw and the bottom front screw.

6 Reconnect the NT8D81AA cable and secure it in place by snapping shut the locking latches provided on the NTCW84JA connector.

End of Procedure

Figure 13
NTCW84JA 50-pin ITG-specific I/O Panel Filter Connector for Meridian 1 large systems



Install the NTMF94EA ELAN, TLAN, serial interface cable

The NTMF94EA cable provides the ELAN, TLAN and serial interface for the NTEZ04AA ITG Wireless card. Refer to “NTMF94EA I/O cable” on page 170 for pinouts and technical specifications on the NTMF94EA cable.

Procedure 3
Installing the NTMF94EA ELAN, TLAN, serial interface cable

1 On large systems, connect the NTMF94EA ELAN, TLAN, and RS232 Serial Maintenance I/O cable to the I/O panel connector for the left hand card slot.

If using an Option 11C, 11 C Mini, or Succession CSE 1000, connect the cable to the I/O connector in the cabinet that corresponds to the ITG Wireless card slot (see Figure 43 on page 172).

2 Connect a shielded Category 5 cable from the customer's TLAN hub or switch equipment to the port labeled "TLAN".

3 Connect a shielded Category 5 cable from the customer's ELAN hub or switching equipment to the port labeled "ELAN".

4 Install the NTAG81CA serial cable into the faceplate Maintenance port. If required, use the NTAG81BA maintenance extender cable

Note: Alternatively, for a permanent connection to the maintenance port, use the dB9 female connector on the NTMF94BA breakout cable to connect a modem (via a null modem) or directly to a local TTY terminal.

> **CAUTION**
> **Service Interruption**
>
> 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 results in incorrect and unpredictable operation of the ITG Wireless card.

End of Procedure

Refer to "I/O, maintenance and extender cable description" on page 169 in Appendix A for further information on cables.

Configuring data in Meridian 1 and Succession CSE 1000

ITG Wireless card configuration guidelines

Each port on an ITG Wireless card is configured as an M2616 unit. Configure each TN as a M2616 digital telephone set in LD 11. To distinguish the ITG Wireless card for administrative purposes, set the Designator (DES) prompt in LD 11 to “ITG”. 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 ITG Wireless card must have the same Customer Number, and same configuration. All ITG Wireless cards in the same group must also have the same Customer Number. Coordinate the DN configuration on each TN with the configuration of DNs to ITG Wireless card ports in OTM. Refer to *Features and Services* (553-3001-306) for further information.

LD 11 – Configure ITG Wireless cards

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 ITG Wireless card, u = 0-23 for the 24 configured TNs on each ITG Wireless card).
TN	C u	In Option 11C, 11C Mini and Succession CSE 1000, terminal Number (corresponding to ports on the ITG Wireless card, u = 0-23 for the 24 configured TNs on each ITG Wireless card).
DES	ITG	To identify the ITG Wireless card.
...	...	...
CUST	0-99	Customer Number (All sets corresponding to the same ITG Wireless 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).
	POA (POD)	Allow or deny Privacy Override
...	...	...
KEY	00 SCR xxxxxx 00 MCR xxxxxxxx	Single or 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	Leave blank; this is reserved for future development.
KEY	02 TRN	Transfer key.
KEY	03 AO6	6 party Conference key.
KEY	04 RGA	Ring Again key
KEY	05 PRK	Call Park key
KEY	06 MSB	Make Set Busy key
KEY	08 SSU yyyy	System Speed Call User key, where yyyy = SCL number
KEY	09 CFW yy..zz	Call Forward key

Configure Flexible Feature Codes

A Group Call Flexible Feature Code (GRPF) is required to activate Group Call. A pick Up Ringing Number Flexible Feature Code (PURN) is required to activate Call Pickup. A Call Park Access Code Flexible Feature Code (CPAC) is required to activate Call Park Retrieve.

Configure ITG Wireless card in OTM

The site name, Meridian 1 or Succession CSE 1000 system name, and customer number must exist in the OTM Navigator before a new ITG node can be added.

The following steps are required to configure ITG Wireless in OTM:

- Set card role to Leader.
- Manually add an ITG Node using OTM.
- Configure the node.
- Configure the ITG Wireless card to the node.
- Configure Wireless IP sets/users.

Procedure 4
Setting the card leader role

1 Ensure that the ITG Wireless cards are disabled in LD 32 before proceeding. Refer to *Administration Input/Output Guide* (553-3001-311) for further information.

2 Connect the OTM PC com port to the serial port on the ITG Wireless card faceplate or to the I/O serial maintenance port of the NTMF94EA cable.

3 Use the following port settings for the TTY terminal emulation on the PC:

- 9600 baud
- 8 bits
- no parity bit
- one stop bit
- Flow control set to Xon/Xoff (if using HyperTerminal to access the card)

When a new ITG Wireless card displays “T:22” on the 4-character display, (or “T:20” if the TTG Wireless card is not yet configured as an XDLC card), the ITG Wireless card begins sending bootp requests on the ELAN. A series of dots appears on the TTY.

4 Type **+++** and then press **Enter**. Enter the default “vxWorks login” and “password” of **itgadmin** to access the ITG shell command line prompt:

```
...+++
vxWorks login: itgadmin
password: itgadmin
ITG>
```

Note: Repeat this step as necessary, until the login prompt appears.

5 When the ITGL shell prompt appears, set the card role to Leader using the following command:

setLeader “xxx.xxx.xxx.xxx”,”yyy.yyy.yyy.yyy”,”zzz.zzz.zzz.zzz”

where,
xxx.xxx.xxx.xxx = IP address of management interface on card
yyy.yyy.yyy.yyy = IP address of management network gateway used by the card
zzz.zzz.zzz.zzz = Management subnet mask for the card

6 Reboot the Leader card using either the command line command “cardReset” (to perform a soft boot), or by pressing the reset button on the faceplate.

End of Procedure

Procedure 5
Add an ITG node manually

1 Launch OTM from the Start menu.

2 Double-click “IP Telecommuter” from the Services folder in the OTM Navigator window.

The **IP Telephony Gateway - IP Telecommuter** window appears. See Figure 15 on page 83.

3 Select Click **Configuration | Node | Add**

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

End of Procedure

Figure 14
OTM Navigator window

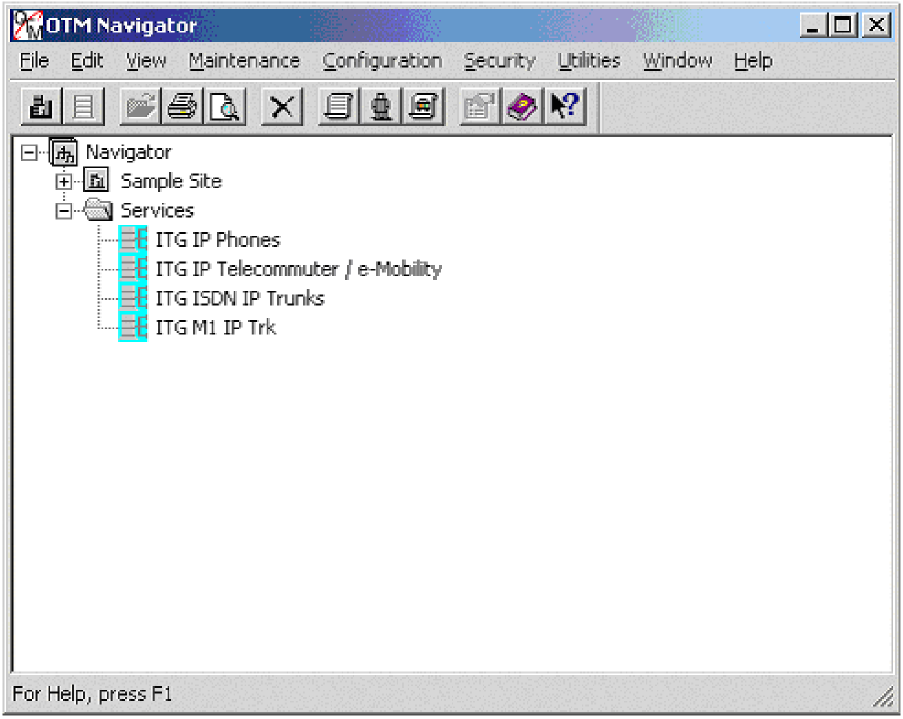
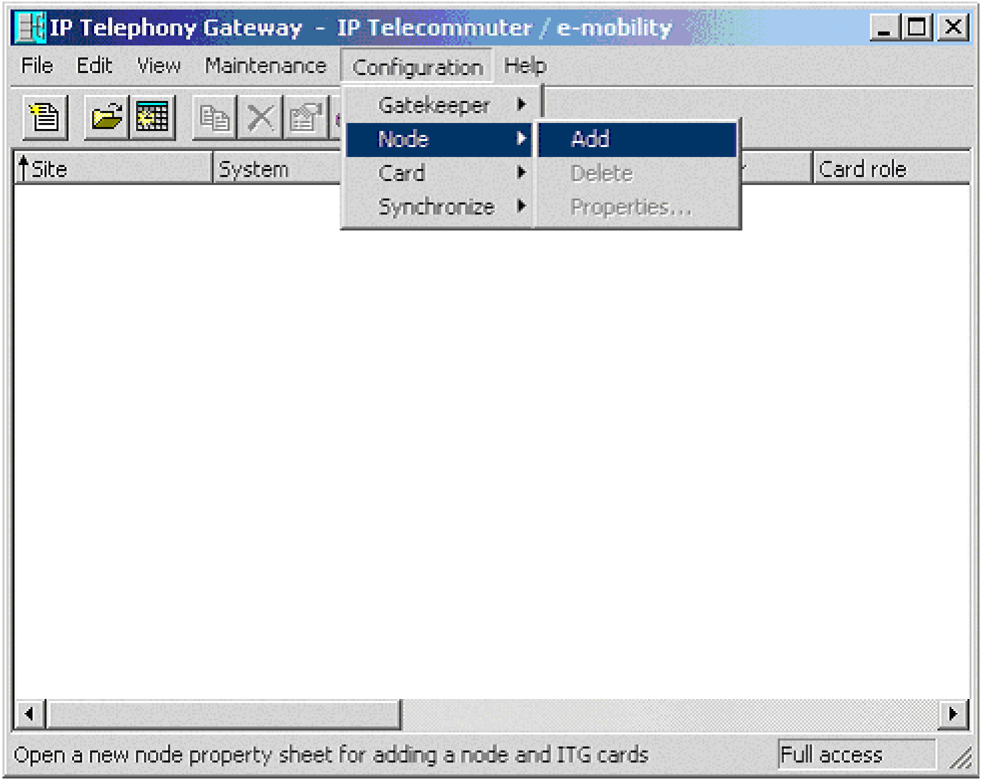
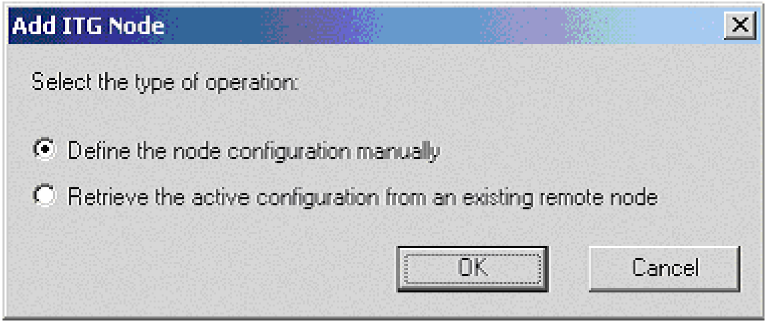

OTM Navigator
File Edit View Maintenance Configuration Security Utilities Window Help
Navigator
Sample Site
Services
ITG IP Phones
ITG IP Telecommuter / e-Mobility
ITG ISDN IP Trunks
ITG M1 IP Trk
For Help, press F1

Figure 15
IP Telephony Gateway – IP Telecommuter Configuration menu



Open a new node property sheet for adding a node and ITG cards

Figure 16
Add ITG Node dialog box



Select the type of operation:

● Define the node configuration manually

○ Retrieve the active configuration from an existing remote node

Configure ITG Wireless data in OTM

All IP addresses and subnet mask data must be in dotted decimal format. Convert subnet mask data from Classless Inter-Domain format (CIDR).

Refer to the Table 8 on page 72 for IP addresses and information required in this procedure.

Whenever node properties change, the ITG Wireless card must be reset in order for the changes to take effect.

Configure ITG Wireless IP addresses

CAUTION
System Failure
Nortel Networks only supports the separate ELAN and TLAN configuration.

Procedure 6
Configure ITG Wireless data on OTM

1 In the “ITG Node Properties” dialog box General tab, do the following: Select the OTM site, OTM system, Customer and Node number from the pull-down menus.

2 The site name, Meridian 1 or Succession CSE 1000 system name, and customer number must exist in the OTM Navigator before a new ITG node can be added.

3 Enter network connection data:

a. Select the checkbox beside **Use separate subnets for voice and management**.

b. Enter **Node IP address** (in dotted decimal format). This must be set to the TLAN Voice IP address.

c. Enter **Management LAN Gateway IP address** (in dotted decimal format).

d. Enter **Management LAN subnet mask address** (in dotted decimal format).

e. Enter the **Voice LAN Gateway IP address** (in dotted decimal format).

f. Enter the **Voice LAN subnet mask address** (in dotted decimal format).

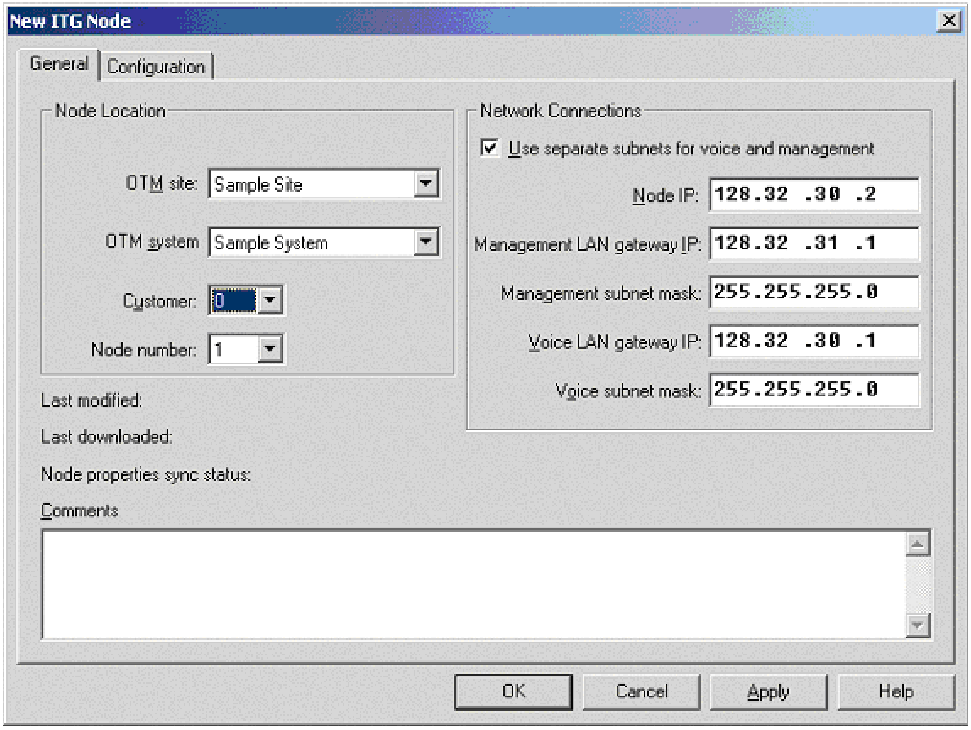
End of Procedure

Note 1: Gateway IP's and subnet masks depend on the customer's LAN configuration.

Note 2: See the network administrator for information on IP addresses. Refer to the ITG Wireless summary worksheet (see Table 8 on page 72) to assign IP addresses. Also, refer to the ITG Wireless card Installation Summary Sheet.

CAUTION
Service Interruption
Unlike other ITG Wireless cards, the Voice IP address on the Configuration tab **must** match the Node IP address on the General tab. Both the Voice IP address and the Node IP address **must** match the customer TLAN address. If the addresses do not match, the ITG Wireless card cannot work.

Figure 17
New ITG Node General Tab



Node Location

OTM site: Sample Site

OTM system: Sample System

Customer: 0

Node number: 1

Last modified:

Last downloaded:

Node properties sync status:

Comments

Network Connections

☑ Use separate subnets for voice and management

Node IP: 128.32 .30 .2

Management LAN gateway IP: 128.32 .31 .1

Management subnet mask: 255.255.255.0

Voice LAN gateway IP: 128.32 .30 .1

Voice subnet mask: 255.255.255.0

Configure ITG Wireless card properties

The "Configuration" tab is used to configure ITG Wireless cards within the node. When adding ITG Wireless cards, select the Card role "Leader 0."

> ***Note 1:*** If the IP Network administrator provides IP addresses and subnet masks in CIDR format, e.g. "10.1.1.10/24", the subnet mask must be converted to dotted decimal format. On the Configuration tab – Add, Change or Delete the ITG Wireless cards in the node one at a time.
>
> ***Note 2:*** The Leader card cannot be deleted in the Configuration tab. The node must be deleted in order to delete the Leader.

Procedure 7
Configure ITG Wireless card properties

1 From the ITG Node Properties window, click the **Configuration** tab. Refer to Figure 18 on page 89.

2 Enter the **Card Properties** data for each card:

a. **Define Card role:** Assign the Card role: Leader 0. Refer to Procedure 4 on page 80.

Note: The Card role is always “Leader 0” for ITG Wireless cards.

b. **Management IP:** This is the ELAN IP address for the card. OTM and Meridian 1 or Succession CSE 1000 use this address to communicate with the card.

c. **Management MAC:** This is the motherboard Ethernet address from the Table 8 on page 72.

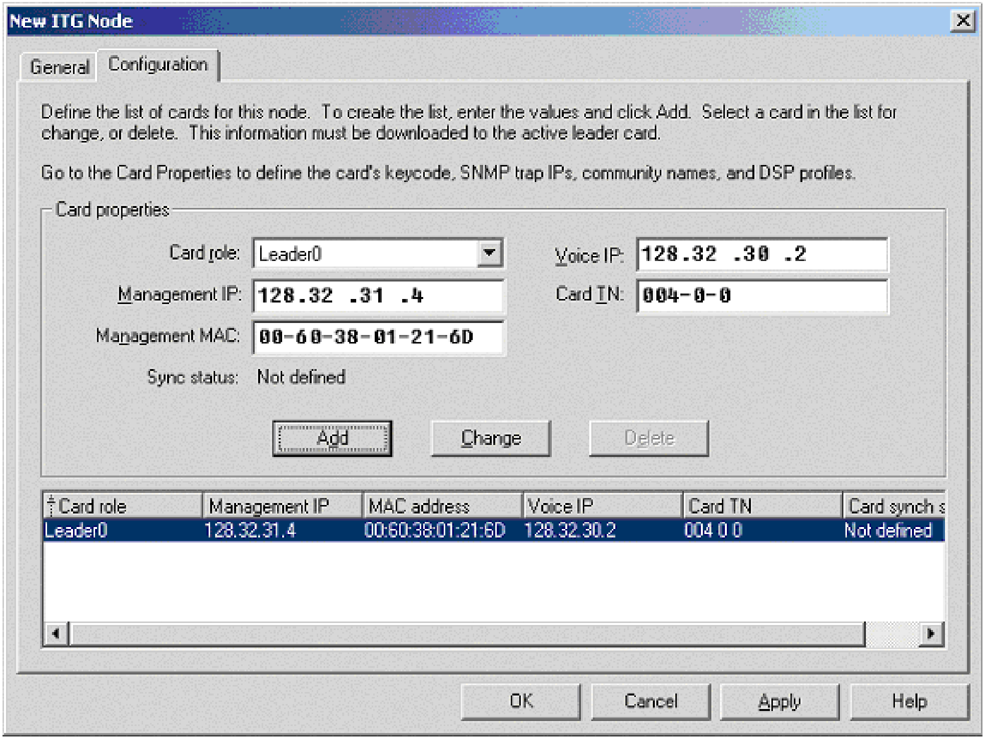
d. **Card TN:** For Large systems, enter Card TN (l s c). For small systems, enter only the card number (0 -49), as **xxx**, where the first **x** is always 0 (zero) and the next digits are the card number.

Example 1: Card 41 is entered as **041**
Example 2: Card 07 is entered as **007**

3 When all ITG Wireless cards have been configured, click **OK**. The “IP Telecommuter” window displays all configured ITG Wireless cards.

End of Procedure

Figure 18
ITG Node Properties – Configuration tab



Define the list of cards for this node. To create the list, enter the values and click Add. Select a card in the list for change, or delete. This information must be downloaded to the active leader card.

Go to the Card Properties to define the card's keycode, SNMP trap IPs, community names, and DSP profiles.

Card properties

Card role: Leader0

Voice IP: 128.32 .30 .2

Management IP: 128.32 .31 .4

Card TN: 004-0-0

Management MAC: 00-60-38-01-21-6D

Sync status: Not defined

Card role	Management IP	MAC address	Voice IP	Card TN	Card synch s
Leader0	128.32.31.4	00:60:38:01:21:6D	128.32.30.2	004 0 0	Not defined

Configuring card properties for Wireless IP handsets

The IP Clients tab is used to define the DN and password for each port on the ITG Wireless card.The list of ports is built by OTM when the ITG Wireless card is added using the node properties.

> ***Note:*** Initially, all 24 ports are set to “unused”.

Procedure 8
Configuring card properties for IP clients

Note: Cards do *not* need to be disabled to perform this procedure. All procedures using OTM are performed offline until "Synchronize" and "Transmit" commands are issued.

1 In the "IP Telecommuter" window, double-click the ITG Wireless card where the user's data and password are stored to display the "ITG Wireless card properties" window.

2 Click the "IP Clients" tab as shown in Figure 19 on page 91.Select the user's TN in the list.

3 Select "Make password same as DN" by clicking the checkbox.

Note: The password must be the same as the DN.

4 Enter the DN for the IP Client.

Note 1: The DN entered must match the DN entered for the port in Overlay 11. OTM does not check this condition.

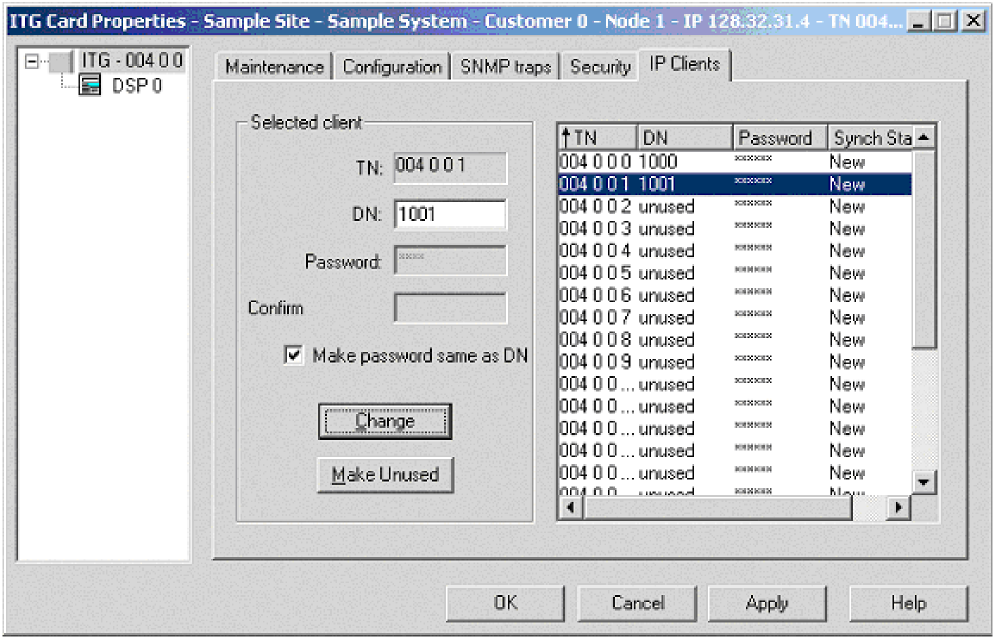
Note 2: The DN can be up to seven digits in length.

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

6 Click **OK**.

End of Procedure

Figure 19
ITG Wireless card properties – IP Clients tab



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...

Selected client

TN: 004 0 0 1

DN: 1001

Password: xxxx

Confirm

☑ Make password same as DN

TN	DN	Password	Synch Sta
004 0 0 0	1000	xxxxxx	New
004 0 0 1	1001	xxxxxx	New
004 0 0 2	unused	xxxxxx	New
004 0 0 3	unused	xxxxxx	New
004 0 0 4	unused	xxxxxx	New
004 0 0 5	unused	xxxxxx	New
004 0 0 6	unused	xxxxxx	New
004 0 0 7	unused	xxxxxx	New
004 0 0 8	unused	xxxxxx	New
004 0 0 9	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New

Gatekeeper properties

Every Wireless ITG Wireless card contains Gatekeeper functionality. There is one gateway property sheet for each ITG Wireless card. See Figure 20 on page 92. After configuring Gatekeeper properties, use the Open and Show commands, as shown in Procedure 10 on page 92 and Figure 21 on page 93, to retrieve and display the information in the ITG Wireless card files.

Procedure 9
Configure ITG Wireless card Gatekeeper properties

1 In the Configuration tab, choose “Use internal Gatekeeper” option.

2 Select a registration renewal time in the range of 10 – 60 minutes, by increments of 5 minutes.

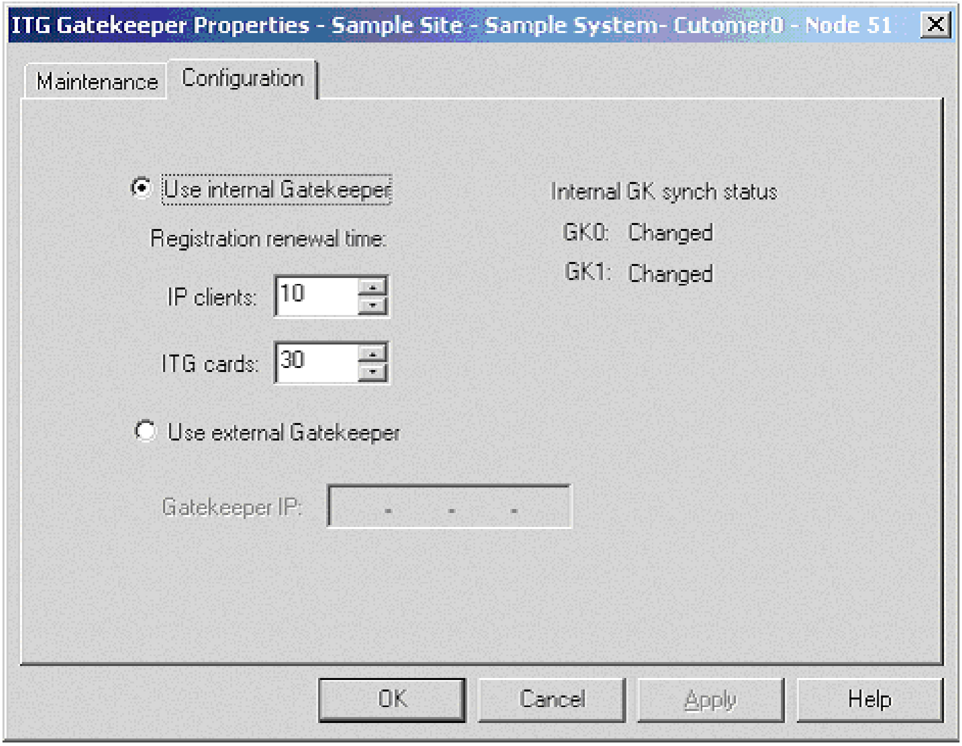
Note: Change the default value of 30000 to 10 for IP clients, 60 for ITG Wireless cards.

3 Click **Apply**.

4 Click **OK**.

End of Procedure

Figure 20
ITG Gatekeeper Properties – Configuration tab



ITG Gatekeeper Properties - Sample Site - Sample System- Cutomer0 - Node 51
Maintenance
Configuration
OK
Cancel
Apply
Help

● Use internal Gatekeeper

Registration renewal time:

IP clients: 10

ITG cards: 30

○ Use external Gatekeeper

Gatekeeper IP: . . .

Internal GK synch status

GK0: Changed

GK1: Changed

Procedure 10
Retrieve and display Gatekeeper properties

1 Click on the “Maintenance” tab in the ITG Gatekeeper Properties window.

2 To display all active calls, click on the “Show active calls” button. The file is retrieved from the active Gatekeeper (ITG Wireless card) and displayed as a text file in WordPad.

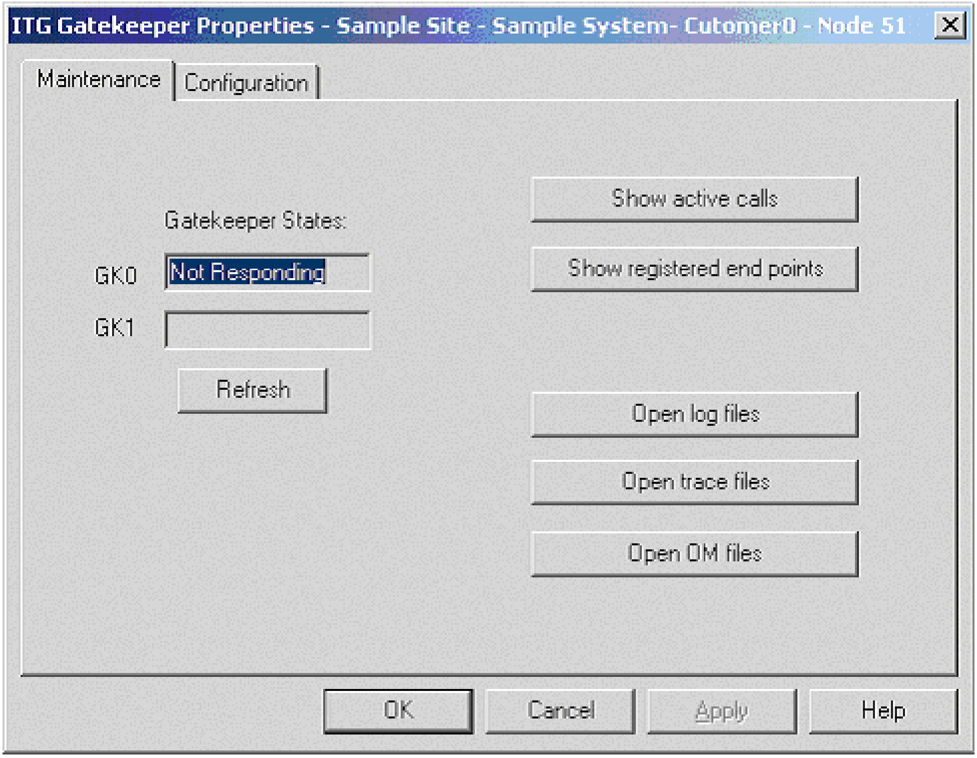
3 Select the “open” buttons to retrieve files from the active Gatekeeper (ITG Wireless card). Each active Gatekeeper opens its own copy of its files in WordPad.

End of Procedure

Note 1: If the external gatekeeper option is selected, the state of the Gatekeeper is “external’.

Note 2: The status of GK0 is the status of the active Gatekeeper (ITG Wireless card). The status of GK1 is always blank because there is only one Gatekeeper per card per node.

Figure 21
ITG Gatekeeper Properties – Maintenance tab



ITG Gatekeeper Properties - Sample Site - Sample System- Cutomer0 - Node 51

Gatekeeper States:

GK0: Not Responding

GK1:

DSP properties

Configure the DSP properties for the ITG Wireless card using the following procedure, and the default values for the DSP CODEC (see Procedure 11, step 6). See “Transmit and receive gain adjustment” on page 37.

> ***Note:*** Refer to *Read-Me-First (PO992423)* for settings of specific Wireless IP handsets.

Procedure 11
Configure DSP properties for ITG Wireless cards

1 Double-click “IP Telecommuter” from the Services folder in the OTM Navigator window.

2 In the “IP Telecommuter” window, select the ITG Wireless card that is having its properties modified.

3 Click the **right** mouse button on the card, and select **Card | Properties** from the popup menu.
The “ITG Wireless card properties” window appears. See Figure 22 on page 96.

4 Click the DSP0 icon underneath the ITG Wireless card.

5 Click the Configuration tab to configure the parameters as required.

6 Select either “G.729A”, “G.711Mu-Law” or “G.711 A-Law” from the “DSP coding algorithm” pull-down menu.

7 Set the Transmit Gain for the path from the PCM (TDM) they network to the packet data.

The range is –14 to +14 dB. Increase the Transmit Gain in increments of one to increase the volume level heard at the ear piece of the handset. The setting used depends on the loss characteristic of the specific Wireless IP handset (refer to *Read-Me-First* (PO992423)).

8 Set the Receive Gain for the path from the packet network into the PCM (TDM) network. The range is -14 to +14 dB. Increase the Receive Gain in increments of one to increase the level from the mouthpiece of the handset. The setting used depends on the loss characteristic of the specific Wireless IP handset (refer to *Read-Me-First* (PO992423)).

Note: The recommended gain range is -6 dB to +6 dB. Gains outside of this range can result in noticeable distortion.

9 Click **Apply,** then click **OK**.

10 Click the Advanced tab.

11 Set the Voice Payload Size. The setting used depends upon the capabilities of the specific Wireless IP handset. (Refer to *Read-Me-First* (PO992423) for further information.)

12 Set the Voice playout nominal delay. The setting used depends upon the capabilities of the specific Wireless IP handset. (Refer to *Read-Me-First* (PO992423) for further information.)

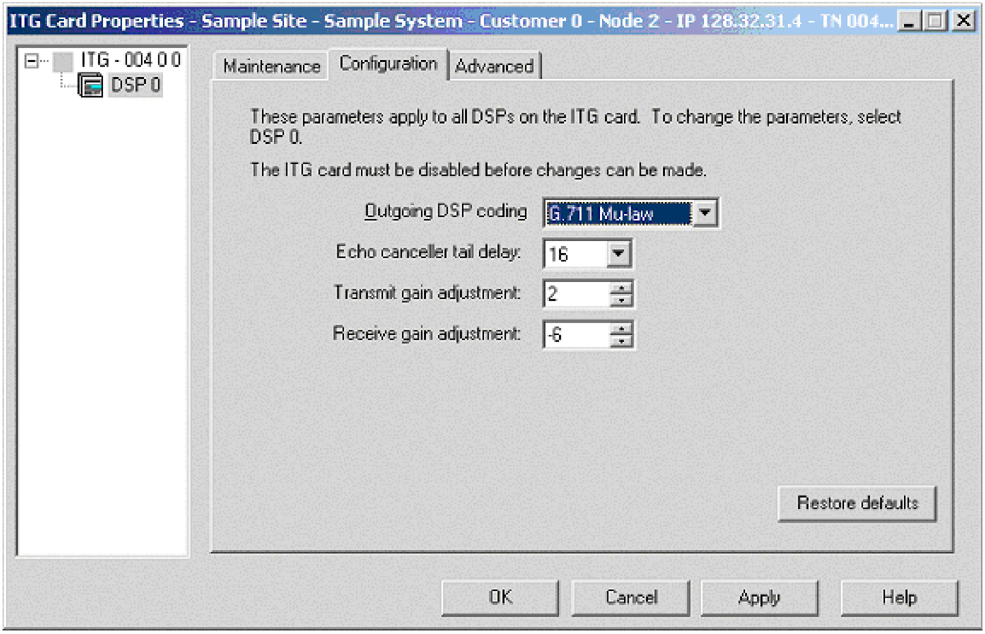
13 Set the Voice playout maximum delay. The setting used depends upon the capabilities of the specific Wireless IP handset. (Refer to *Read-Me-First* (PO992423) for further information.)

14 Click **Apply**.

15 Click **OK**.

End of Procedure

Figure 22
ITG Wireless card properties – Configuration tab.



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 2 - IP 128.32.31.4 - TN 004...

These parameters apply to all DSPs on the ITG card. To change the parameters, select DSP 0.

The ITG card must be disabled before changes can be made.

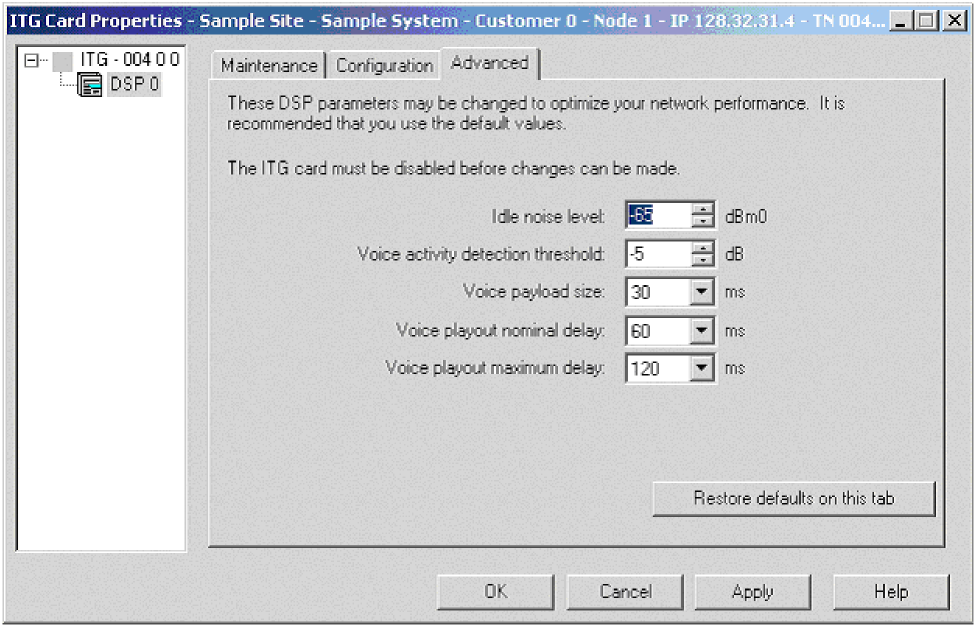
Outgoing DSP coding: G.711 Mu-law

Echo canceller tail delay: 16

Transmit gain adjustment: 2

Receive gain adjustment: -6

Figure 23
ITG Wireless card properties – Advanced tab


ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...
ITG - 004 0 0
DSP 0
Maintenance
Configuration
Advanced
Restore defaults on this tab
OK
Cancel
Apply
Help

These DSP parameters may be changed to optimize your network performance. It is recommended that you use the default values.

The ITG card must be disabled before changes can be made.

Idle noise level: -65 dBm0

Voice activity detection threshold: -5 dB

Voice payload size: 30 ms

Voice playout nominal delay: 60 ms

Voice playout maximum delay: 120 ms

Activate SNMP traps for ITG Wireless cards

Define and activate SNMP traps with Procedure 12.

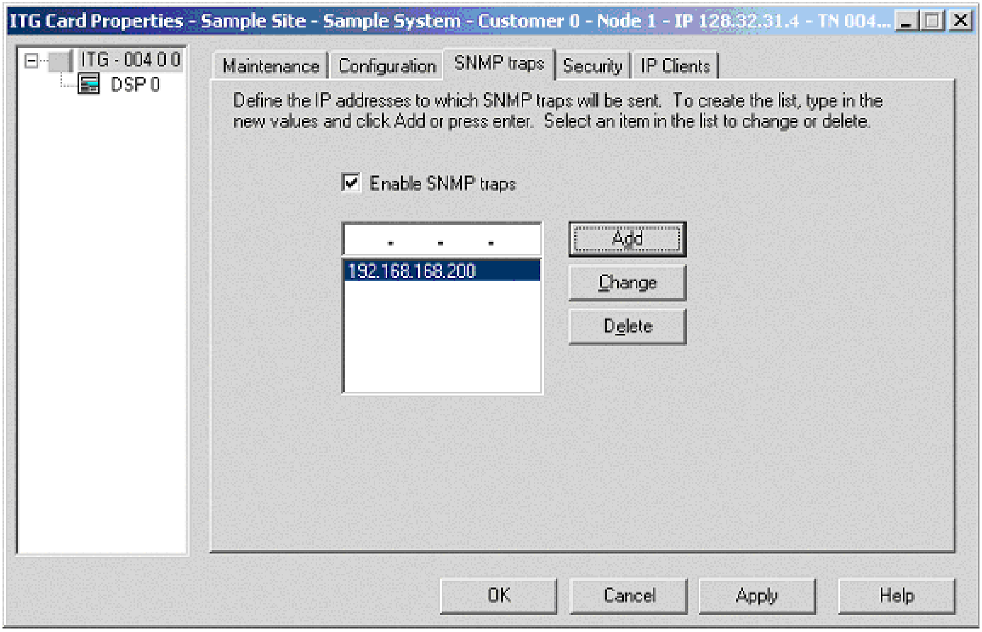
Procedure 12
Activating SNMP traps

1 Double-click “IP Telecommuter” from the Services folder in the OTM Navigator window. The IP Telecommuter window appears.

2 Double-click an ITG Wireless card to define the SNMP traps for that card.
The “ITG Wireless card properties” window appears.

3 Click the **SNMP traps** tab as shown in Figure 24 on page 98.

Figure 24
ITG Wireless card properties – SNMP Traps tab.



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...

Define the IP addresses to which SNMP traps will be sent. To create the list, type in the new values and click Add or press enter. Select an item in the list to change or delete.

☑ Enable SNMP traps

192.168.168.200

4 To add an SNMP Manager IP address, type the address in the entry field, and click **Add**.
Typically, each card has the same address.

Note: A maximum of eight SNMP Manager IP addresses can be added.

5 If the OTM PC is on a different subnet than the Wireless IP Gateway Management IP address, add the OTM PC IP address to the list of SNMP Manager IP addresses.

6 Click **OK**.

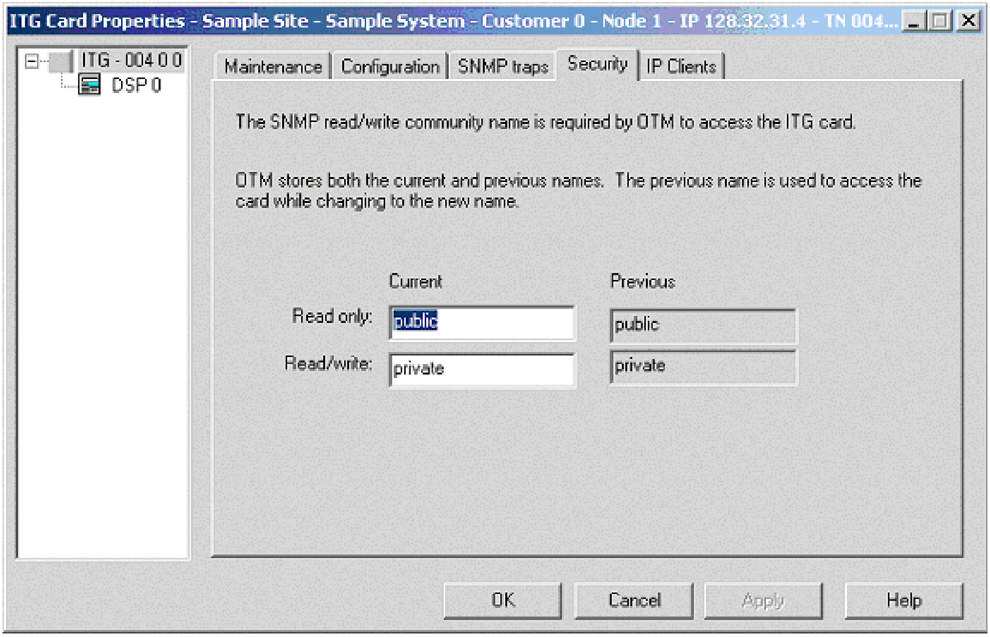
End of Procedure

Configuring security for SNMP access

Procedure 13 on page 100 explains how to change the SNMP Read/Write Community Names to provide better security for the ITG node. OTM uses the Read/Write Community Name to refresh the ITG Wireless card status, and to control the transmitting and retrieving of configuration data files for database synchronization.

> ***Note:*** To obtain community names, connect a TTY to the ITG Wireless card maintenance port. Restart the card. The card displays the Read/ Write Community Name on the TTY during startup.

Figure 25
ITG Wireless card properties – Security tab



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...

The SNMP read/write community name is required by OTM to access the ITG card.

OTM stores both the current and previous names. The previous name is used to access the card while changing to the new name.

	Current	Previous
Read only:	public	public
Read/write:	private	private

Procedure 13
Configuring security for SNMP access

1 Click the **Security** tab. See Figure 25 on page 99.

2 Change the default Read only and default Read/Write Community Names.

OTM uses the previous Read/Write Community Name to transmit the card properties. When data is transmitted for the first time after changing the Read/Write Community Name, the Previous Read/Write Community Name is used. For all following data transmissions, the changed password is used.

3 Click **Apply**.

Note 1: If a failed card has been replaced with a spare card, try the default community names. The default Read/Write Community Name is **public**. The default Read/Write Community Name is **private**. OTM ITG only uses the Read/Write Community Name.

Note 2: Both current and previous fields reflect the new Read/Write Community Names.
The Read/Write Community Names might be mismatched between the OTM ITG and the ITG Wireless cards due to the following:

- if OTM ITG cannot refresh the status
- if OTM ITG cannot transmit and retrieve configuration files to or from a particular ITG Wireless card, and
- if the card can be pinged from the OTM ITG PC

Call your Nortel Networks technical support representative for further assistance.

End of Procedure

Transmit configuration data

CAUTION
Loss of Data

Ensure that all ITG Wireless cards are **disabled** in the Meridian 1 and Succession CSE 1000 before transmitting card properties.

The Wireless ITG Wireless card data, first configured in OTM, is transmitted to the cards. The configuration data can also be "retrieved" from the cards.

For example, a Nortel Networks service representative can dial in and retrieve a customer's node for debugging purposes. This saves him from entering all the IP addresses, etc. Later, the customer can retrieve any changes made.

The configuration data is contained in text files and is transmitted, using File Transfer Protocol (FTP), between the cards and OTM. The text files are as follows:

- Node properties – bootp.1 (on every card)

  Note: Card must be rebooted when node properties are changed.

- Gatekeeper properties – gktable.1 (on every card)
- Card properties – config1.ini (on every card)

  Note: Disable the card when card properties are changed.

Procedure 14
Transmitting configuration data between the cards and OTM

1 In the "IP Telecommuter" window, select a card. Refer to Figure 26 on page 103.

2 Click **Configuration** | **Synchronize** | **Transmit.**

3 In the ITG – Transmit Options window, select the "**Transmit to selected nodes**" option.

4 Select the check boxes beside:

- **Node Properties to activate leader**
- **GK properties to both leaders**
- **Card properties**

5 Click the **Start Transmit** button.

The transmission status is displayed in the “Transmit control” box. Refer to Figure 27 on page 104. Confirm that card properties are transmitted successfully.

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

7 In the “IP Telephony Gateway” main window, select **View | Refresh**.

8 In the “IP Telephony Gateway” main window, use the cardReset command to reboot the card.

Note: A reboot of the ITG Wireless card typically takes four minutes.

9 Use the LD 32 ENLC command to re-enable the ITG Wireless cards.

10 In the “IP Telephony Gateway” main window, select **View | Refresh**.

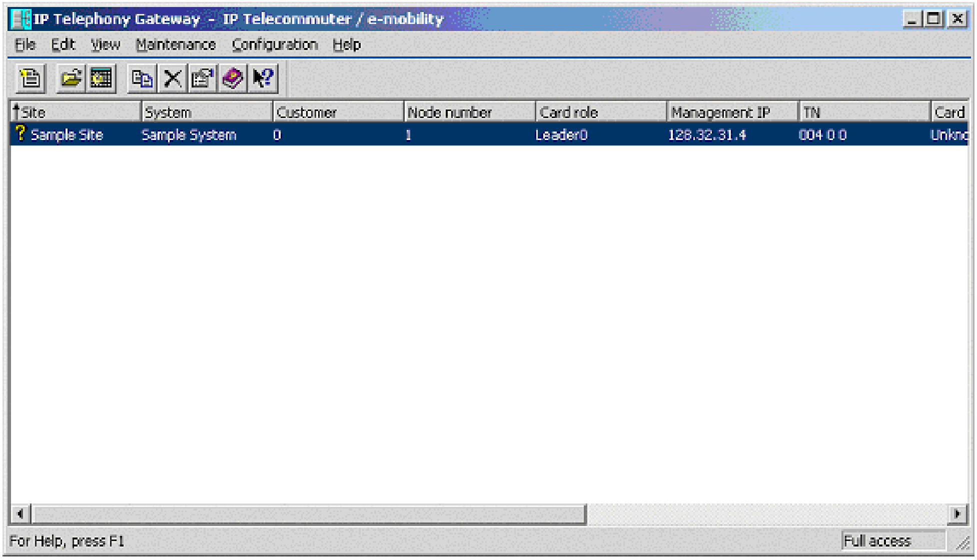
11 After the card reboots, the card status should now show “Enabled.”

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

End of Procedure

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 and Succession CSE 1000 configuration is performed and the Wireless IP handsets have been configured.

Figure 26
IP Telephony Gateway – IP Telecommuter window

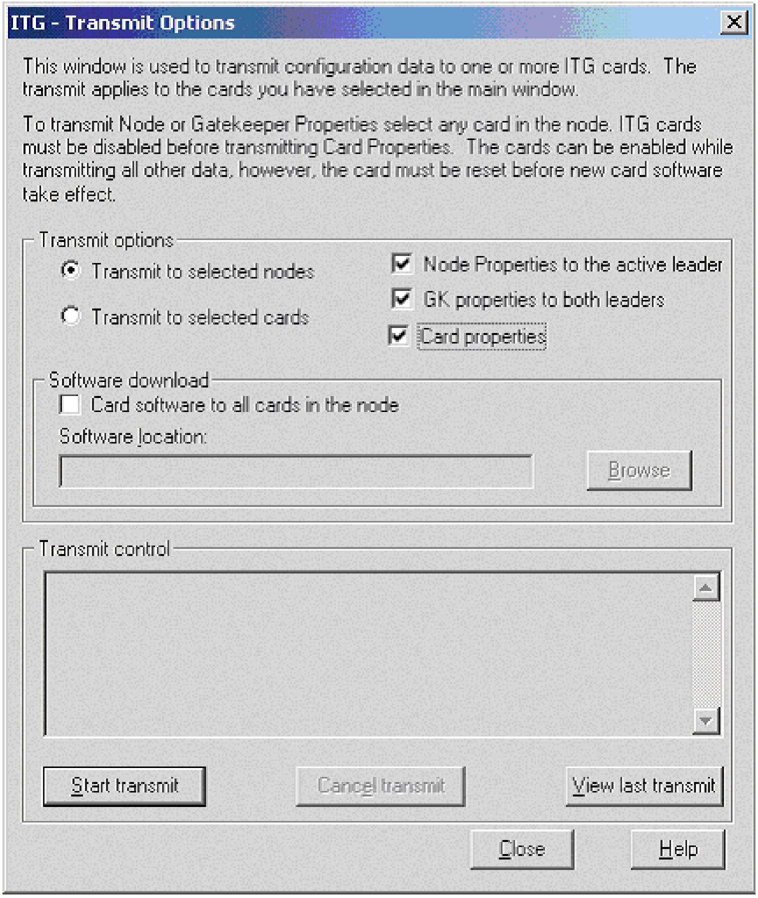


Site	System	Customer	Node number	Card role	Management IP	TN	Card
? Sample Site	Sample System	0	1	Leader0	128.32.31.4	004 0 0	Unkno

For Help, press F1

Full access

Figure 27
The “ITG - Transmit Options” window



ITG - Transmit Options

This window is used to transmit configuration data to one or more ITG cards. The transmit applies to the cards you have selected in the main window.

To transmit Node or Gatekeeper Properties select any card in the node. ITG cards must be disabled before transmitting Card Properties. The cards can be enabled while transmitting all other data, however, the card must be reset before new card software take effect.

Transmit options

● Transmit to selected nodes

○ Transmit to selected cards

☑ Node Properties to the active leader

☑ GK properties to both leaders

☑ Card properties

Software download

□ Card software to all cards in the node

Software location:

Verify card software

Procedure 15
Verifying ITG Wireless card software

1 In the IP Telephony Gateway window, double-click each ITG Wireless card to open the ITG Wireless card properties window.

2 Leave the default selection of the ITG Wireless card in the Card Properties window, and click the “Configuration” tab.

The software release is displayed on this tab.

3 Verify the software release of each ITG Wireless card is the latest recommended software release for the card.

Contact your Nortel Networks representative for the URL of the website to check the latest recommended ITG Wireless card software release.

If any of the cards require a software upgrade, refer to Procedure 16 on page 105.

——————— ***End of Procedure*** ———————

Upgrade ITG Wireless card software (if required)

Procedure 16
Upgrading ITG Wireless card software

1 Download the Wireless IP Gateway ITG software from the World Wide Web to the OTM PC hard drive.

Contact your Nortel Networks representative for information on how to access the website.

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

3 Open OTM, and launch the “IP Telecommuter Gateway” application, if not already opened.

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

5 Select the cards from the main card list view that are to be upgraded. Upgrade all the cards in the node together, unless a spare card that has older software is being installed.

6 Disable all ITG Wireless cards to be upgraded.

Use the LD 32 DISI command from OTM Maintenance Windows, the OTM System Passthru terminal, or a Meridian 1 and Succession CSE 1000 system management terminal directly connected to a TTY port on the Meridian 1 and Succession CSE 1000.

7 In the OTM “IP Telephony Gateway” main window, select **View | Refresh** and verify that the card status is showing “Disabled.”

8 Select **Configuration | Synchronize | Transmit**.

An “ITG – Transmit Options” dialog box is displayed as shown in Figure 28.

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

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

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

12 Click on the **Start Transmit** button to begin the ITG Wireless card software upgrade process.

The software is transmitted and burned into the flash ROM on the ITG Wireless card.

13 Monitor progress in the “Transmit Control” window. Confirm that the card software is transmitted successfully to the card. Note any error messages, investigate and correct any problems, and repeat card software transmission until it is completed successfully on the ITG Wireless card. The card continues to run the old software until it is rebooted.

14 Reboot the ITG Wireless card that received transmitted software, so that the new software can take effect.

Reboot the card by the pressing the reset button on the faceplate of the card, or by re-seating the card.

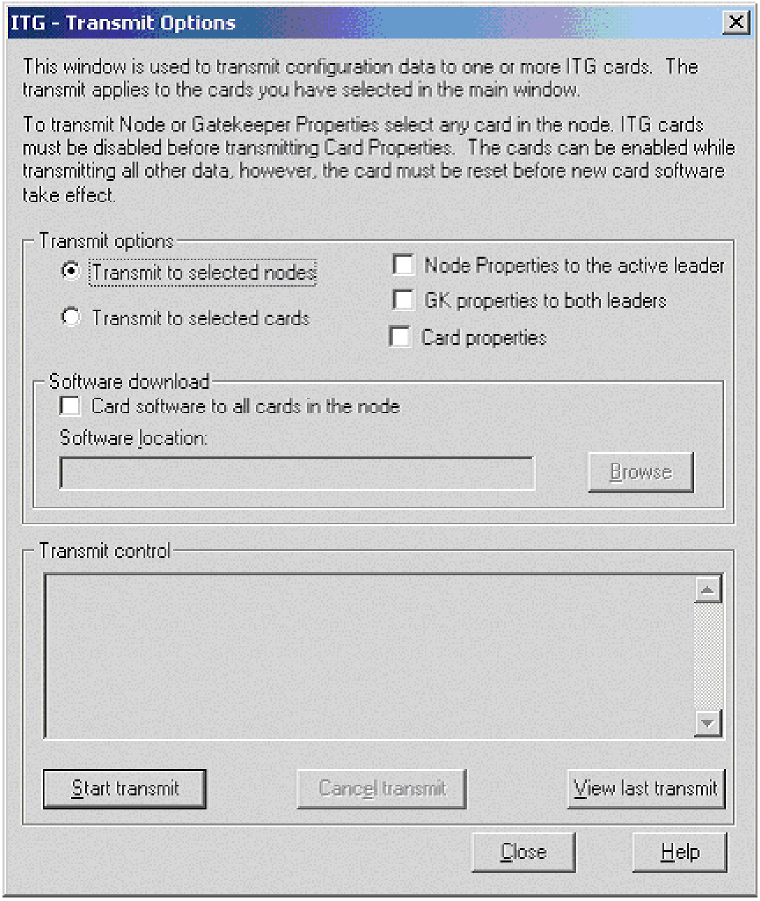
Ensure that the ITG Wireless card has been reset, successfully rebooted, and is responding again. Use the OTM ITG status refresh. The status is either disabled: active; disabled: backup; or disabled.

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

16 Use the LD 32 ENLC command to re-enable the ITG Wireless card.

End of Procedure

Figure 28
ITG – transmit options window



ITG - Transmit Options

This window is used to transmit configuration data to one or more ITG cards. The transmit applies to the cards you have selected in the main window.

To transmit Node or Gatekeeper Properties select any card in the node. ITG cards must be disabled before transmitting Card Properties. The cards can be enabled while transmitting all other data, however, the card must be reset before new card software take effect.

Transmit options

● Transmit to selected nodes

○ Transmit to selected cards

□ Node Properties to the active leader

□ GK properties to both leaders

□ Card properties

Software download

□ Card software to all cards in the node

Software location:

Features

Contents

This section contains information on the following topics:

Reference list

The following are the references in this section:

- *Features and Services* (553-3001-306)

Overview

This chapter describes the Meridian 1 and Succession CSE 1000 features available to Wireless IP handsets in the Wireless IP Gateway. It also briefly describes how these features work in the Wireless IP environment. For more detailed information on these features, including feature interaction and implementation, refer to *Features and Services* (553-3001-306).

Feature summary

On the Meridian 1 and Succession CSE 1000 systems, features are implemented as though the Wireless IP handsets are Aries 2616 digital sets. The ITG Wireless card provides the translation necessary to support the display messages on the Wireless IP handsets, and to refresh the terminal sets' display and status as required. The Wireless IP handsets simply display the information that is sent to them by the Gateway.

The following list summarizes the Meridian 1 features available to Wireless IP handsets in the Wireless IP Gateway:

- Calling Line IP (CLID)
- Called/Calling Party Name Display (CPND)
- Conference
- Call Transfer
- Call Park
- Message Waiting Indication
- Call Forward (All Calls)
- Make Set Busy
- Dialed Access to Group Call
- System Speed Call User
- Ring Again
- Call Pickup
- Overhead Paging
- Multiple Appearance DN

Calling Line ID

The Calling Line Identification (CLID) feature allows the number of the caller and called party to be displayed on each other's set at the same time.

CLID is a display message displayed on the Wireless IP handsets. Class of service, Call Number Information Allowed /(Denied) determines whether or not the number is displayed. If allowed, the CLID display lasts for the duration of the call.

CLID occurs during a call as well as when in the idle state. For example, in a Call Transfer, the display updates to indicate the number of the transferred party when the originator of the transfer terminates the call.

Called/Calling Party Name Display

The Called/Calling Party Name Display (CPND) feature allows the name of the caller and called party to be displayed on each other's sets at the same time.

Class of service, Call Party Name Display Allowed /(Denied) determines whether or not the name is displayed.

CPND occurs during a call as well as when in the idle state. For example, in a Call Transfer, the display updates to indicate the name of the transferred party when the originator of the transfer terminates the call.

Conference

The Conference feature adds additional parties to an already established call. A maximum number of 3 or 6 calls per conference is allowed, depending on the conference feature assigned to the conference call originator.

The conference feature can be accessed only when on an established call.

Call Transfer

The Call Transfer feature allows a caller on a two-party call to hold the existing call and originate another call to a third party. The call originator and third party may talk privately or transfer the call on hold to the third party.

Call Park

The Call Park feature places a call in a parked state similar to call hold, where an attendant or another Wireless IP handset can retrieve it. A parked call must have a system ID, also known as the Park DN. Simply parking the call on any telephone DN in the system provides this ID. A parked call does not occupy a DN and there is no visual indication that the call is parked.

The Call Park feature is intended to be used with Call Paging. The person paged is able to pick up the call directly by dialling the Park DN. It also allows the Wireless terminal that originally received and parked the call, to make or answer other calls.

Parked calls must be retrieved within a specified time. The length of time to retrieve the parked call is configured in LD 50. The length of time can be between 30 seconds and 4 minutes.

Message Waiting Indication

The Message Waiting Indication (MWI) feature notifies the user when a new voicemail message arrives within the mail system.

Call Forward (all Calls)

The Call Forward All Calls (CFW) feature automatically forwards incoming calls to another destination within or outside the Meridian 1 system. Only calls to the prime DN or any single-appearance DN, are call forwarded. Outgoing calls can be made from a telephone with this feature active.

Make Set Busy

The Make Set Busy feature allows the Wireless terminal to appear busy to all incoming calls. Outgoing calls can still be made from the Wireless terminal. If a voicemail system is installed, incoming calls are routed straight to the voice mailbox configured for that terminal.

Dialed Access to Group Call

The Group Call feature allows a single caller to simultaneously call as many as 20 DNs in large systems, 6 DNs in small systems. Activation of this feature originates a call to all the assigned members of that group. When the first member answers, ring back tone is removed and a speech path is established with the originator of the call. As each group member answers, they are added to the call. The lamp associated with the Group Call feature flashes until all group members have answered.

System Speed Call User

The Speed Call feature allows the user to place calls by dialling a code. Speed Call applies to both internal and external calls. The call lists are set up on the switch as System Speed Call lists.

Ring Again

The Ring Again feature provides the opportunity, after encountering a busy DN, to ring the DN again when it becomes free. Pressing the Ring Again key (or its equivalent), asks the system to monitor the busy DN. When it becomes available, the system notifies the originating caller. Pressing the Ring Again key (or its equivalent) a second time causes the call to be automatically dialled again.

Call Pickup

The Call Pickup feature allows a group of terminals to be arranged in groups consisting of any combination of terminals. Wireless IP handset configured with Class of Service, Call Pickup Allowed (CPA), can answer calls made to any terminal within the Call Pickup group. For example, if a Wireless terminal is ringing, another user can pickup the call for that terminal by pressing a key (or its equivalent).

Overhead Paging

The Overhead Paging feature provides access to the customer’s speaker or radio paging equipment.

Multiple Appearance Directory Number with optional Privacy Override

A Multiple Appearance, Multiple Call Arrangement is available between the Wireless IP handset and other Meridian 1 or Succession CSE 1000 proprietary telephones. It allows as many calls to be in progress as there are appearances of the Directory Number. Privacy is inherent in this arrangement.

A Multiple Appearance, Single Call Arrangement is available between the Wireless IP handset and other Meridian 1 or Succession CSE 1000 telephones. This arrangement allows a single call to be active on a Directory Number irrespective of its number of appearances. A Wireless IP handset with Privacy Override Allowed (POA) class of service can enter an established call which is active on another telephone sharing that Directory Number.

Administration

Contents

This section contains information on the following topics:

Overview

This chapter explains how to administer the ITG Wireless card using one of three administration interfaces:

- Optivity Telephony Management (OTM).
  - Provides a graphical interface to the ITG Wireless card. Use OTM to Telnet to the card, install and upgrade software, configure alarm event reporting, view and update card properties and configuration data, schedule reports and other related tasks.
- Command Line Interface (CLI)
  - Use the CLI to display card/node status, check software version and other card information. The CLI can be accessed through a direct serial connection to the I/O panel serial port, the faceplate maintenance port, or through a Telnet session.
  - ITG shell commands are described in Table 29 on page 219.
  - Use the following parameters on the TTY: 9600 baud, 8 bits, no parity bit, one stop bit.
- Overlays
  - Use the same commands and messages for the ITG Wireless card as used for the digital line (XDLC) card.
  - Meridian 1 system commands as described in “Meridian 1 system commands” on page 141.

OTM administration interface

OTM provides a graphical interface for administering commands to the ITG Wireless card.

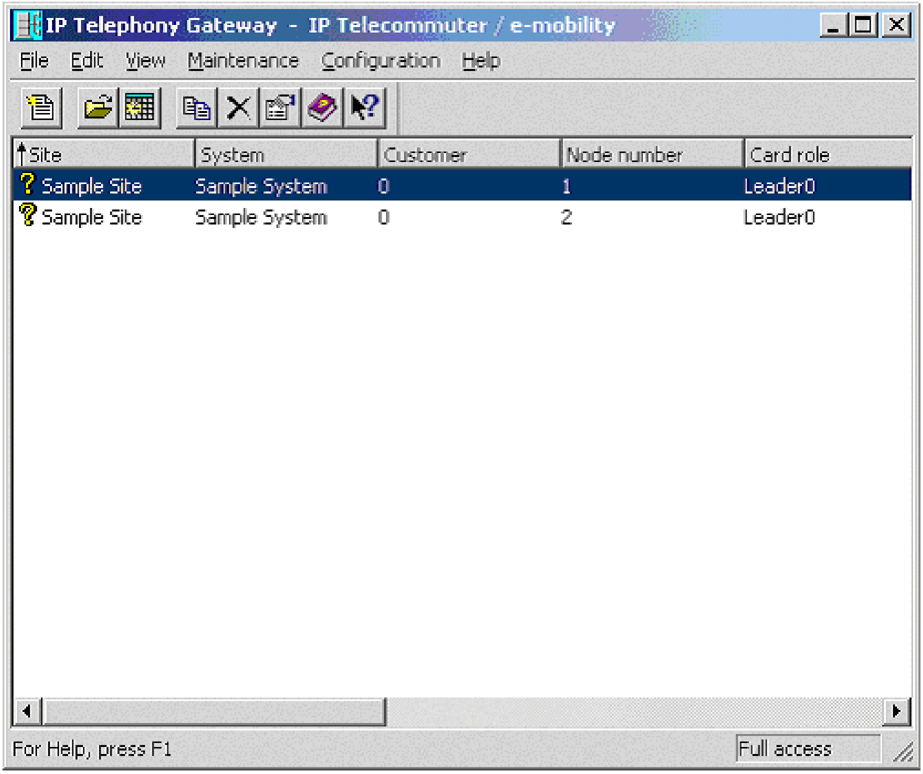
Note: This document discusses only ITG Wireless nodes. For information regarding IP Telecommuter nodes, refer to *Meridian 1 Integrated Telephony Gateway Line Card 1.0/IP Telecommuter: Description, Installation, and Operation* (553-3001-119)

IP Telecommuter window

The “IP Telephony Gateway – IP Telecommuter” window contains a list of all defined ITG Wireless IP Gateways, nodes and cards.

When the “ITG IP Telecommuter” icon is clicked from the “Services” folder in the “Navigator” window, the first window to open is the “IP Telephony Gateway - IP Telecommuter” window. Refer to Figure 29 on page 117.

Figure 29
IP Telephony Gateway – IP Telecommuter window



Site	System	Customer	Node number	Card role
Sample Site	Sample System	0	1	Leader0
Sample Site	Sample System	0	2	Leader0

OA&M tasks

The ITG application provides most of the ITG administration commands.

The following procedures are described in this chapter:

- “Report scheduling and generation” on page 118.
- “View ITG Wireless card information and error log” on page 124.
- “Backup and restore ITG Wireless card data” on page 125.
- “Deleting an ITG Wireless card” on page 125
- “Changing an IP address” on page 126
- “Updating ITG Wireless card properties” on page 127.
- “Update ITG Wireless card DSP properties” on page 131.
- “Telnet to an ITG Wireless card” on page 137.
- “Using the Retrieve command” on page 135.

Report scheduling and generation

Operational Measurement (OM) reports provide important statistical and traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file applies only to the calls routed over the IP network by the ITG Wireless card. OM reports also provide a quantitative view of system performance also including:

- Incoming voice calls attempted
- Incoming voice calls completed
- Out-going voice calls attempted
- Out-going voice calls completed
- Total voice time

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

Generate reports as necessary or on a pre-selected schedule. Each time a report is generated, the application retrieves the latest OM data from each ITG Wireless card that is defined.

A new file is created for each month of the year for which data is collected. The files are named as "itgLine_dd_mm_yyyy_hh_min_ss_fileN.csv," where "dd" = the day, "mm" = the month, "yyyy" = the year, "hh" = the hour, "min" = the minute, "ss" = the second, "N" = the file number. The file number default value is 1. When a file gets 64000 records a new file is generated, and the file number gets incremented.

The default data directory is:
<drive>:\Nortel\Common Data\ITGLineSide Data

> ***Note 1:*** Replace <drive> with the OTM installation directory.

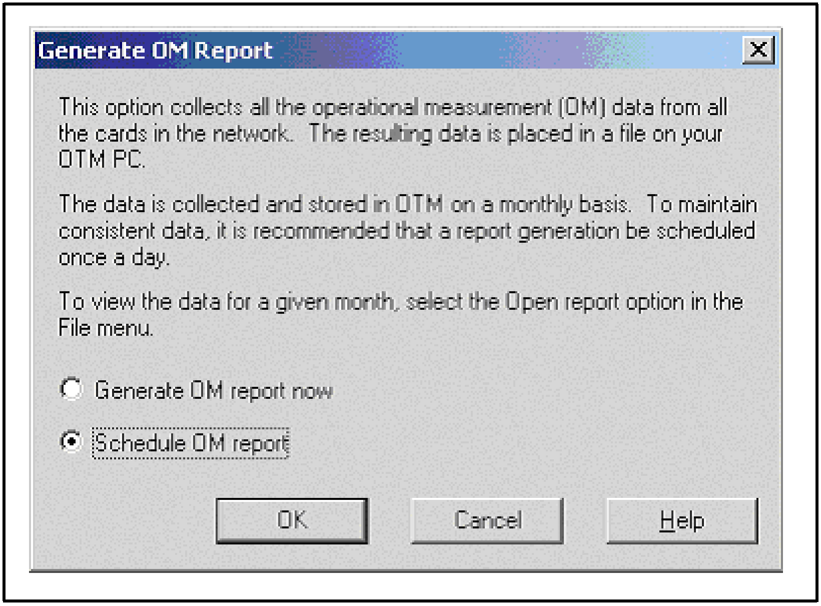
> ***Note 2:*** It is recommended that report generation be scheduled for once a day.

Procedure 17
Report scheduling

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. See Figure 30 on page 120.

Figure 30
ITG _Generate OM Report window



Generate OM Report

This option collects all the operational measurement (OM) data from all the cards in the network. The resulting data is placed in a file on your OTM PC.

The data is collected and stored in OTM on a monthly basis. To maintain consistent data, it is recommended that a report generation be scheduled once a day.

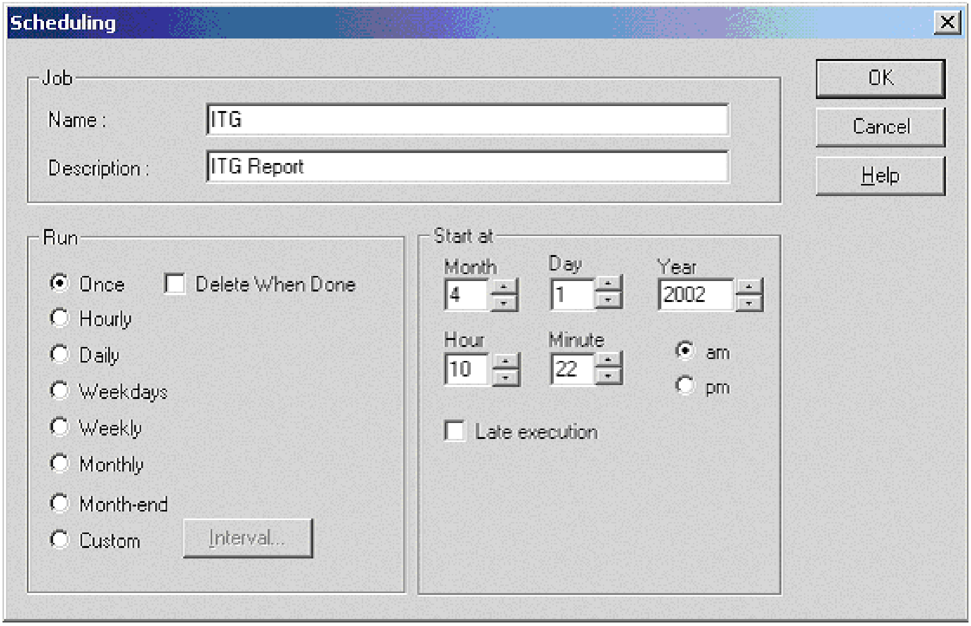
To view the data for a given month, select the Open report option in the File menu.

○ Generate OM report now

● Schedule OM report

The Scheduling window appears, as shown in Figure 31 on page 121.

Figure 31
Scheduling window



Job

Name : ITG

Description : ITG Report

Run

● Once □ Delete When Done
○ Hourly
○ Daily
○ Weekdays
○ Weekly
○ Monthly
○ Month-end
○ Custom

Start at

Month 4 Day 1 Year 2002

Hour 10 Minute 22 ● am ○ pm

□ Late execution

3 In the “Job” text box, enter the name and description of the schedule.

4 In the “Run” box, click the radio button that indicates the frequency of report generation.

Note: Nortel recommends scheduling reports once a day.

5 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.

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

End of Procedure

Procedure 18
Report generating

1. In the “IP Telephony Gateway – IP Telecommuter” window, click the **File** menu and select **Report**, then **Generate**.
2. In the “ITG - Generate Report” window, select the **Generate report now** radio button. Refer to Figure 30 on page 120.
3. Click **OK**.

   Note: The report created and displayed is called the “ITG IP Telecommuter - Operational Measurement Report”. The default display is Microsoft Excel.™

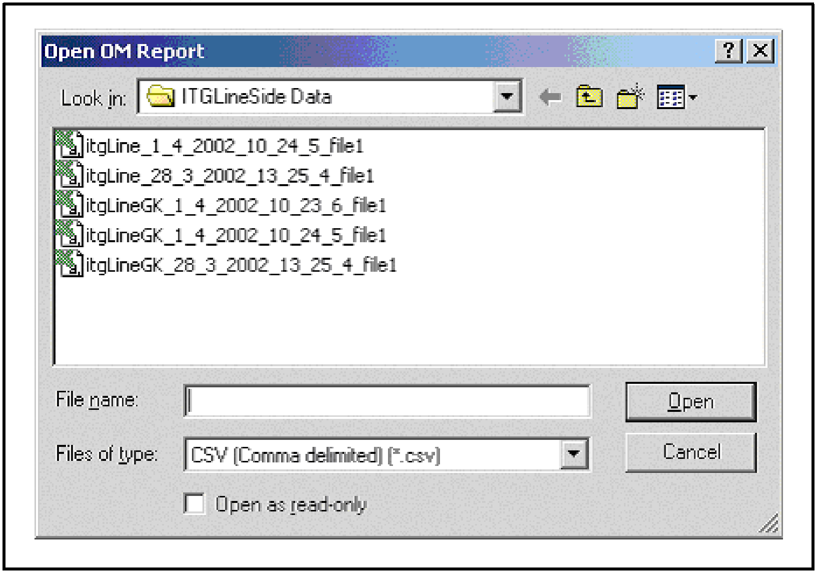
End of Procedure

Procedure 19
Viewing reports

1. In the “Navigator” window, select the **ITG IP Telecommuter** icon from the “Services” folder.
2. In the “IP Telephony Gateway - IP Telecommuter” window, click the on the File pull-down menu.
3. Select **Reports** and **Open**. The “Open OM Report” dialog box appears as shown in Figure 32.
4. From the list of files, select the desired file and click “Open”. The file opens in MS Excel, formatted for easy viewing. Refer to Figure 33 on page 124 for an example of an OM Report.
   Open OM Report dialog box.

End of Procedure

Figure 32
OM Report dialog box



Look in: ITGLineSide Data

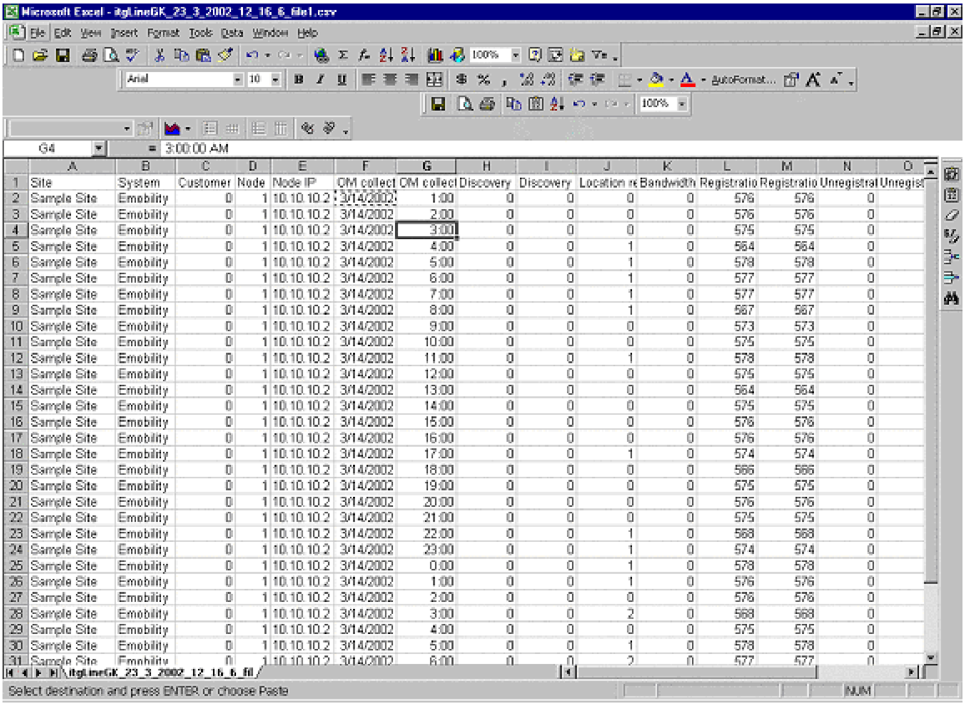
itgLine_1_4_2002_10_24_5_file1
itgLine_28_3_2002_13_25_4_file1
itgLineGK_1_4_2002_10_23_6_file1
itgLineGK_1_4_2002_10_24_5_file1
itgLineGK_28_3_2002_13_25_4_file1

File name:

Files of type: CSV (Comma delimited) (*.csv)

☐ Open as read-only

Figure 33
OM Report example



Microsoft Excel - itgLineGK_23_3_2002_12_16_6_file1.csv
File Edit View Insert Format Tools Data Window Help
100%
Arial
10
AutoFormat...
100%

G4 = 3:00:00 AM

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Site	System	Customer	Node	Node IP	OM collect	OM collect	Discovery	Discovery	Location re	Bandwidth	Registratio	Registratio	Unregistrat	Unregist
2	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	1:00	0	0	0	0	576	576	0	
3	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	2:00	0	0	0	0	576	576	0	
4	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	3:00	0	0	0	0	575	575	0	
5	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	4:00	0	0	1	0	564	564	0	
6	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	5:00	0	0	1	0	578	578	0	
7	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	6:00	0	0	1	0	577	577	0	
8	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	7:00	0	0	1	0	577	577	0	
9	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	8:00	0	0	1	0	567	567	0	
10	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	9:00	0	0	0	0	573	573	0	
11	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	10:00	0	0	0	0	575	575	0	
12	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	11:00	0	0	1	0	578	578	0	
13	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	12:00	0	0	0	0	575	575	0	
14	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	13:00	0	0	0	0	564	564	0	
15	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	14:00	0	0	0	0	575	575	0	
16	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	15:00	0	0	0	0	576	576	0	
17	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	16:00	0	0	0	0	576	576	0	
18	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	17:00	0	0	1	0	574	574	0	
19	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	18:00	0	0	0	0	566	566	0	
20	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	19:00	0	0	0	0	575	575	0	
21	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	20:00	0	0	0	0	576	576	0	
22	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	21:00	0	0	0	0	575	575	0	
23	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	22:00	0	0	1	0	568	568	0	
24	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	23:00	0	0	1	0	574	574	0	
25	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	0:00	0	0	1	0	578	578	0	
26	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	1:00	0	0	1	0	576	576	0	
27	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	2:00	0	0	0	0	576	576	0	
28	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	3:00	0	0	2	0	568	568	0	
29	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	4:00	0	0	0	0	575	575	0	
30	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	5:00	0	0	1	0	578	578	0	
31	Sample Site	Emobility	0	1	10.10.10.2	3/14/2002	6:00	0	0	2	0	577	577	0	

itgLineGK_23_3_2002_12_16_6_fil

Select destination and press ENTER or choose Paste

View ITG Wireless card information and error log

OTM uses FTP to transfer the error log file from the ITG Wireless card to the PC and open it in the WordPad application. The ITG Error log file displays error information, including error date/time, the originating module (ITG node), and specific error data.

Procedure 20
Viewing ITG Wireless information and error log

1 In the “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 log file opens for viewing.

——————— ***End of Procedure*** ———————

Backup and restore ITG Wireless card data

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

Deleting an ITG Wireless card

Procedure 21
Deleting an ITG Wireless card

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

2 Telnet to the card.

3 Enter the **clearLeader** command from the ITG shell.

4 In the “IP Telephony Gateway - IP Telecommuter” window, select **Node | Properties** from the popup menu. The ITG Node Properties window is displayed.

5 Click the “Configuration” tab.

6 Select the ITG Wireless card to be deleted from the list.

7 Click the **Delete** button.

8 Click **Apply,** then **OK**.

9 On Meridian 1 and Succession CSE 1000, using LD 11, remove the M2616 sets for the ITG Wireless cards using the System Passthru terminal, or by a management terminal directly connected to a TTY port.

End of Procedure

Changing an IP address

Procedure 22
Changing an IP address

1 From the “IP Telephony Gateway - IP Telecommuter” window, click **Configuration|Node|Properties**. Update the ITG Wireless 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.

If not saving the changes, click **Cancel**.

3 Transmit the node properties to the Leader 0 card.

4 Select the Leader 0 ITG Wireless card in the IP Telephony Gateway – IP Telecommuter window.

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

6 Click the “Transmit to selected nodes” radio button.

7 Click the “Node Properties” check box.

8 Click the **Start Download** button.

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

10 Click **Close**.

11 Reset the cards for the changes to take effect.

End of Procedure

Updating ITG Wireless card properties

Procedure 23
Updating the ITG Wireless card properties

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

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

3 Click the right mouse button to select **Cards | Properties** from the pop-up menu. The “ITG Wireless card properties” window appears.

4 Select one of the option tabs, “Maintenance”, “Configuration”, “SNMP traps”, “Security”, or “IP Clients”. Refer to the following sections for detailed information on how to update these properties.

5 When the changes are complete, click **Apply** then **OK**.

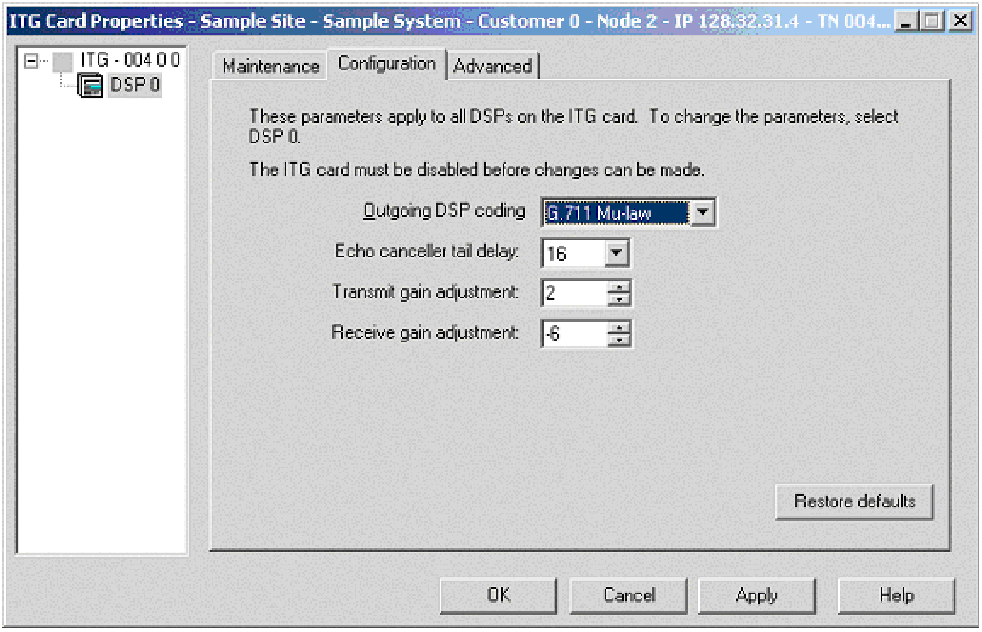
——— ***End of Procedure*** ———

Card properties options

Configuration tab

The Configuration tab displays ITG Wireless card information as shown in Figure 34 on page 128.

Figure 34
ITG Wireless card properties – Configuration tab


ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 2 - IP 128.32.31.4 - TN 004...
ITG - 004 0 0
DSP 0
Maintenance
Configuration
Advanced
Restore defaults
OK
Cancel
Apply
Help

These parameters apply to all DSPs on the ITG card. To change the parameters, select DSP 0.

The ITG card must be disabled before changes can be made.

Outgoing DSP coding: G.711 Mu-law

Echo canceller tail delay: 16

Transmit gain adjustment: 2

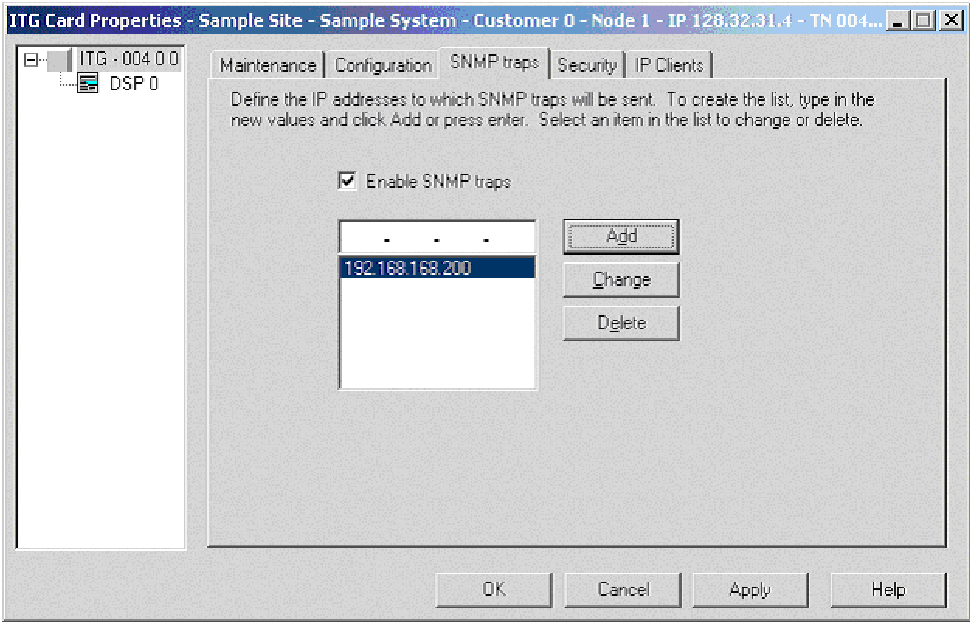
Receive gain adjustment: -6

SNMP traps tab

The SNMP traps tab is used to define the IP addresses to which SNMP traps are sent. Refer to Figure 35 on page 129. This tab is also used to:

- Send SNMP traps to receive alarms (error messages) to the hosts specified by the IP addresses in the list:
  Check the "Enable SNMP traps" box.
- Add an IP address to receive SNMP traps:
  Type the address in the entry field, and click "Add."
- Delete an IP address:
  Select the address from the list, and click "Delete."
- Change an IP address:
  Select the address from the list. Type the new address in the entry field, then click "Change."

Figure 35
ITG Wireless card properties – SNMP traps tab



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...

Define the IP addresses to which SNMP traps will be sent. To create the list, type in the new values and click Add or press enter. Select an item in the list to change or delete.

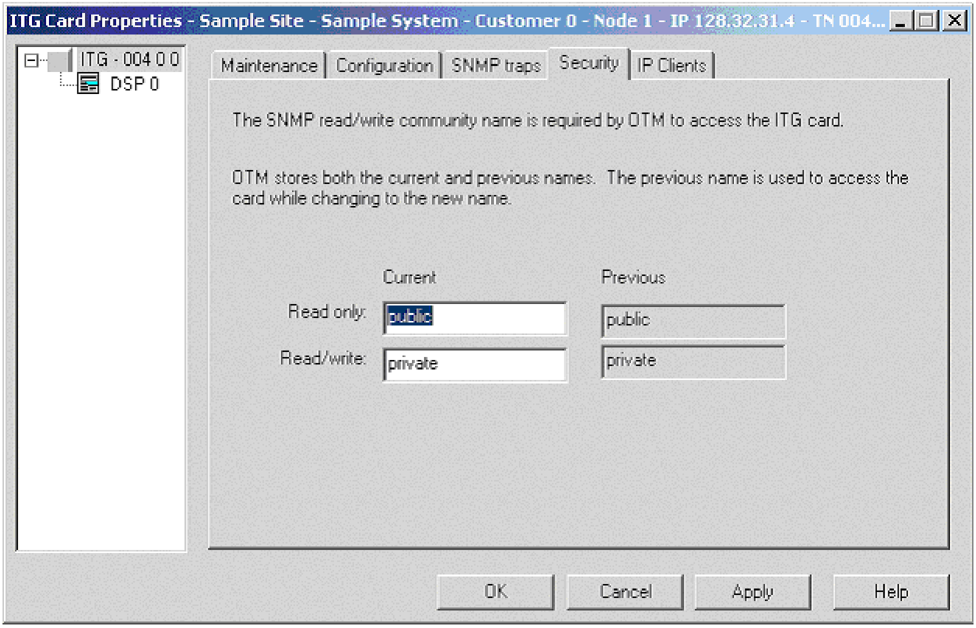
☑ Enable SNMP traps

192.168.168.200

Security tab

The Security tab allows the user to change the SNMP community names of the ITG Wireless card. Refer to Figure 36 on page 130.

Figure 36
ITG Wireless card properties – Security tab



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...
ITG - 004 0 0
DSP 0
Maintenance
Configuration
SNMP traps
Security
IP Clients
OK
Cancel
Apply
Help

The SNMP read/write community name is required by OTM to access the ITG card.

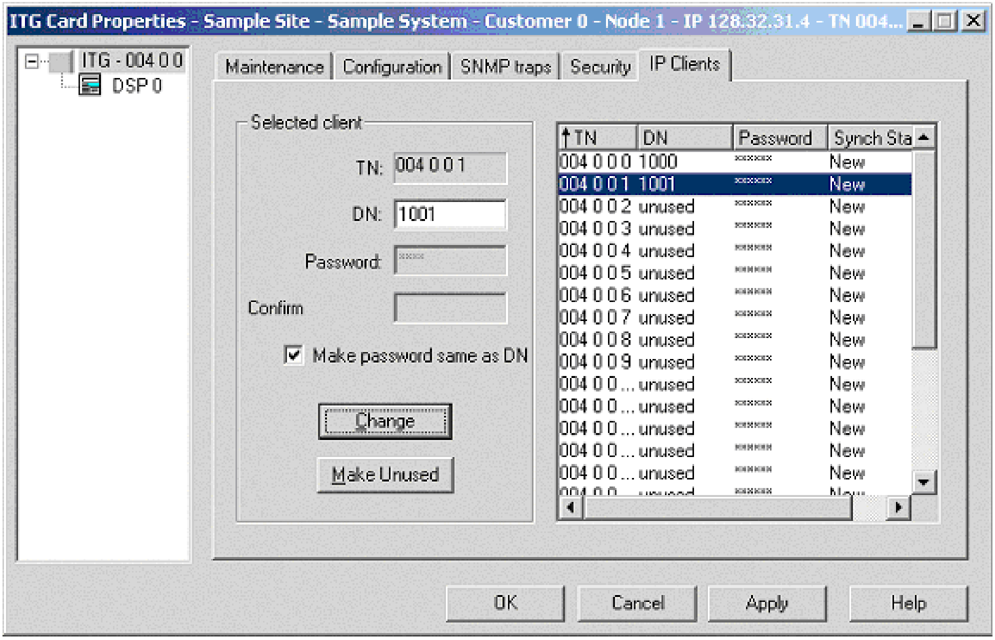
OTM stores both the current and previous names. The previous name is used to access the card while changing to the new name.

	Current	Previous
Read only:	public	public
Read/write:	private	private

Changing IP Clients

Use Procedure 15 on page 83 to configure the items in the IP Client tab. See Figure 37 on page 131.

Figure 37
ITG Wireless card properties – IP Clients tab



Selected client

TN: 004 0 0 1

DN: 1001

Password: xxxx

Confirm

☑ Make password same as DN

TN	DN	Password	Synch Sta
004 0 0 0	1000	xxxxxx	New
004 0 0 1	1001	xxxxxx	New
004 0 0 2	unused	xxxxxx	New
004 0 0 3	unused	xxxxxx	New
004 0 0 4	unused	xxxxxx	New
004 0 0 5	unused	xxxxxx	New
004 0 0 6	unused	xxxxxx	New
004 0 0 7	unused	xxxxxx	New
004 0 0 8	unused	xxxxxx	New
004 0 0 9	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New
004 0 0 ...	unused	xxxxxx	New

Update ITG Wireless card DSP properties

Note: The properties of all DSPs on an ITG Wireless card are modified by configuring the properties for “DSP 0” on an ITG Wireless card.

Procedure 24
Updating ITG Wireless card DSP properties

1. In the “Navigator” window select the **ITG IP Telecommuter** icon from the “Services” folder.
2. In the “IP Telephony Gateway – IP Telecommuter” window select the ITG Wireless card that is having its DSP properties modified.
3. Click the right mouse button on the card and select **Card | Properties** from the popup menu. The “ITG Wireless card properties” window appears.

4 Click the **Configuration** tab and configure the parameters as required. Refer to Figure 38 on page 133.

5 Click the **Advanced** tab. Refer to Figure 39 on page 134.

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

Transmit the card properties to the updated ITG Wireless card.

7 Select the updated ITG Wireless card in the IP Telephony Gateway – IP Telecommuter window.

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

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

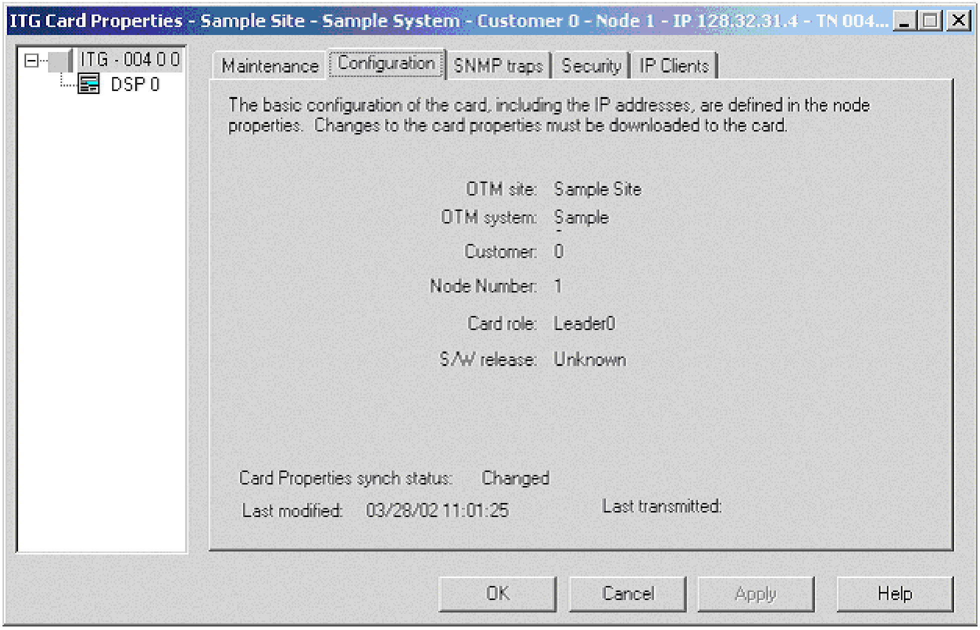
10 Click the **Start Download** button.

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

11 Click **Close**.

End of Procedure

Figure 38
ITG Wireless card properties – Configuration tab



ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...
ITG - 004 0 0
DSP 0
Maintenance
Configuration
SNMP traps
Security
IP Clients
OK
Cancel
Apply
Help

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.

OTM site: Sample Site
OTM system: Sample
Customer: 0
Node Number: 1
Card role: Leader0
S/W release: Unknown

Card Properties synch status: Changed
Last modified: 03/28/02 11:01:25
Last transmitted:

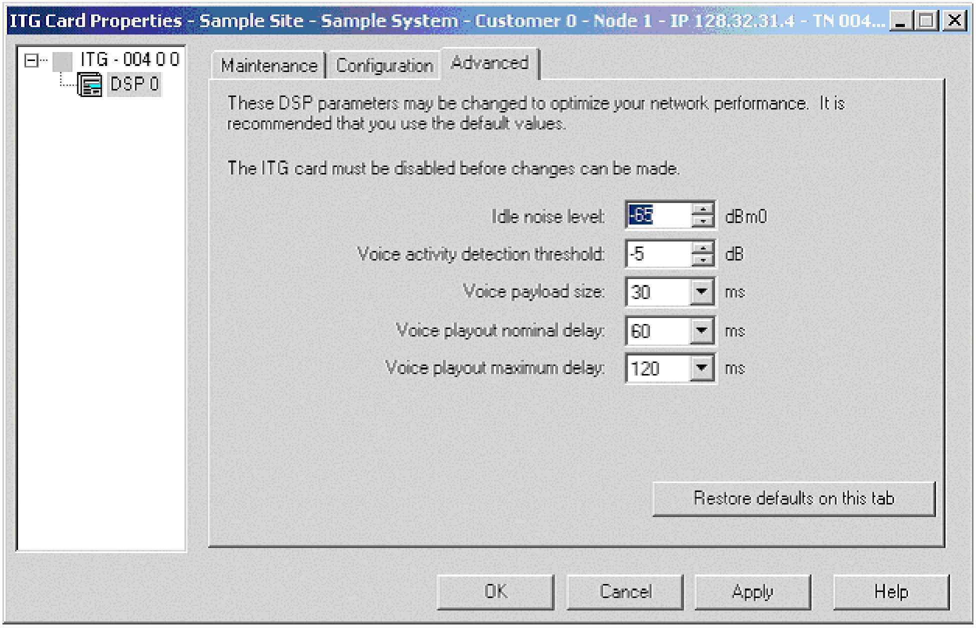
Configuration tab parameters

> ***Note:*** Do not use the default settings. For more information, refer to "Engineering Guidelines" on page 31.

The following are the Configuration tab parameter descriptions.

- Select the "G.711" codec from the "DSP coding algorithm" pull-down menu.
- The "Echo canceller tail delay" parameter range is: 8 – 16ms. The default is 16 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 +6 dB. The default is –4 dB.

Figure 39
ITG Wireless card properties – Advanced tab


ITG Card Properties - Sample Site - Sample System - Customer 0 - Node 1 - IP 128.32.31.4 - TN 004...
ITG - 004 0 0
DSP 0
Maintenance
Configuration
Advanced
Restore defaults on this tab
OK
Cancel
Apply
Help

These DSP parameters may be changed to optimize your network performance. It is recommended that you use the default values.

The ITG card must be disabled before changes can be made.

Idle noise level: -65 dBm0
Voice activity detection threshold: -5 dB
Voice payload size: 30 ms
Voice playout nominal delay: 60 ms
Voice playout maximum delay: 120 ms

Advanced tab parameters

> ***Note:*** Do not use the default settings. For more information, refer to "Engineering Guidelines" on page 31.

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

- 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 +10 dB. 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.

Using the Retrieve command

The Retrieve command sends information from the ITG Wireless cards to the ITG node. The Retrieve command can be used in the following situations:

- when a remote user downloads 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 information, and
- for downloading information to a “dummy” node, that has been created for this purpose, in order to view the configuration of the ITG Wireless cards and node.

Procedure 25
Using 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.

End of Procedure

The Command Line Interface

The Command Line Interface (CLI) displays the status of the card/node, check the software version, and provide other card information. To access the CLI, connect the OTM PC com port to the RS-232 serial maintenance port of the ITG Wireless card through an NTAG81CA Faceplate Maintenance cable.

Alternatively, use the OTM PC to access the ITG shell through a Telnet session. Refer to “Telnet to an ITG Wireless card” on page 137.

The following lists the administration procedures and commands available through the CLI:

- “Telnet to an ITG Wireless card” on page 137.
- “Changing the ITG Telnet password” on page 137
- “Downloading the OM file” on page 138
- “Reset the operational measurements” on page 138.
- “Display the number of DSPs” on page 139.
- “Display ITG Node Properties” on page 139.
- “Transfer files” on page 140.
- “ITG Wireless card shell commands” on page 219.
- “Download the ITG Wireless card error log” on page 140.
- “Display the Gatekeeper properties” on page 141.

Telnet to an ITG Wireless card

Procedure 26
Accessing the ITG shell command line

1 From the OTM PC, in the “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 ITG Wireless card to be accessed. Select **Card | Telnet to ITG Wireless card** from the popup menu.

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

Note: The default user name and password are **itgadmin**.

End of Procedure

Changing the Telnet password

A good security policy requires changing user names and passwords periodically. The ITG user name and password protects FTP and Telnet access to the ITG Wireless card over the LAN.

Procedure 27
Changing the ITG Telnet password

1 From the ITG shell use the command **shellPasswordSet** to change the default user name and password for Telnet to ITG shell, and FTP to the ITG Wireless card file system. The default user name is **itgadmin** and the default password is **itgadmin**.

2 A prompt appears 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
```

3 If the entire sequence of commands is successfully entered, the system responds with 'value = 0 = 0x0'. The new user name and password are now stored in the non-volatile RAM on the ITG Wireless card, and are retained even if the card is reset, powered-off, or on.

End of Procedure

Download the ITG Wireless card operational measurements

The ITG Wireless Card collects operational measurements from the Wireless IP handset sets and DSP channels and saves the information to a log file every 60 minutes.

Use the following procedure to download this file from the ITG Wireless card to the OTM PC.

Procedure 28
Downloading the OM file

1 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.

2 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.

End of Procedure

Reset the operational measurements

This command resets all operational measurement (OM) parameters that have been collected since the last log dump.

At the ITG shell prompt, type: **resetOM**.

Display the number of DSPs

At the ITG shell, enter the following command to display the number of DSPs on the ITG Wireless 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 is displayed on the TTY:

- IP addresses for the management and voice subnets
- default router for the management and voice subnets
- subnet mask for the management and voice subnets
- SNMP manager

Enter the following command to display information about an ITG Wireless card:

```
itgCardShow
```

The following commands give additional information about an ITG Wireless card:

- ldrResTableShow
- ifShow
- firmwareVersionShow
- swVersionShow
- emodelSim

Transfer files

To transfer a file from the ITG Wireless card to the OTM PC or from the OTM PC to the ITG Wireless card, use one of the commands listed in "ITG Wireless card shell commands" on page 219.

> ***Note 1:*** These commands are from the perspective of the ITG Wireless card; that is, commands containing "Get" as part of the command, refer to file transfer from the OTM PC to the ITG Wireless card. Commands containing "Put" as part of the command, refer to file transfer from the ITG Wireless card to the OTM PC:
>
> ***Note 2:*** These commands are case-sensitive. The parameters following the command must each be enclosed in quotes. There must be a comma and no spaces between the parameters.
>
> ***Note 3:*** Refer to "Maintenance" on page 145 for a complete description of the various ITG shell file transfer commands.
>
> ***Note 4:*** *Hostname* refers to one of the following:
>
> - the IP address of the FTP host
> - the ITG Wireless card itself
> - another ITG Wireless card, when a PC card in the A: drive or C: drive of the ITG Wireless card contains the software binary file. (The swDownload command must only use the A: drive.)

Download the ITG Wireless card 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

The following Meridian 1 system commands are used to administer the ITG Wireless card from Overlay 32:

- "Disable the specified ITG Wireless card" on page 143.

  Note 1: The ITG Wireless card must be disabled before card properties can be transmitted from the OTM ITG application to the card.

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

  Note 3: The gatekeeper functions are not disabled when the ITG Wireless card in LD 32 are disabled. Wireless IP handsets are still able to register with the ITG Wireless card but are not to make or receive calls.

- "Disable the specified ITG Wireless card when idle" on page 143.
  This temporarily prevents the ITG node from seizing the port from incoming calls.
- "Disable a specified ITG Wireless card port" on page 143.
- "Enable a specified ITG Wireless card" on page 143.
- "Enable a specified ITG Wireless card port" on page 143.
- "Display ITG Wireless card ID information" on page 144.

  Note: This command displays the PEC (Product Engineering Code) for the card. The ITG PEC is NTEZ04AA.

- "Display ITG Wireless card status" on page 144.
- "Display ITG Wireless card port status" on page 144.

A summary list of ITG Meridian 1 system administration commands is shown in Table 10 on page 142.

Table 10
LD 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 IGT Wireless card when idle, where: l = loop, s = shelf, c = card Note: Use the DISI command to disable the ITG Wireless card instead of the DISC command. The disablement of the ITG Wireless card is indicated by the NPR011 message.
DISU l s c u	Disable the specified unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the specified card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, where: l = loop, s = shelf, c = card
STAT l s c	Print the Meridian 1 software status of the specified card. where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 software status of the specified unit, where: l = loop, s = shelf, c = card, u = unit

Disable the specified ITG Wireless card

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

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

Disable the specified ITG Wireless card when idle

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

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

Disable a specified ITG Wireless card port

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

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

Enable a specified ITG Wireless card

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

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

Enable a specified ITG Wireless card port

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

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

Display ITG Wireless card ID information

To display the ITG Wireless card ID in LD 32, use the following command:

IDC l s c	Display the card ID for the ITG Wireless card, where: l = loop, s = shelf, c = card

Display ITG Wireless card status

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

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

Display ITG Wireless card port status

To display the status of a port on the ITG Wireless 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

Contents

This section contains information on the following topics:

Introduction

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

- “Faceplate maintenance display codes for card reset” on page 146.
- “System error messages (alarms)” are described on page 149.
- “Replacing an ITG Wireless card” on page 153.
- “Add an ITG Wireless card on OTM by retrieving an existing ITG Wireless card” on page 157.

- “ITG Wireless card self-tests” on page 162.
- “Troubleshooting a software load failure” on page 164.
- “Warm rebooting the ITG Wireless card” on page 166.
- “Working with alarm and log files” on page 167.

Faceplate maintenance display codes for card reset

The ITG Wireless card faceplate four character display provides feedback to the technician on the following:

- the diagnostic status of the card during power-up
- the card’s operational state when in service.

Table 11 gives a list of display messages.

Table 11
ITG faceplate maintenance display code messages (Sheet 1 of 3)

Hex display code	Fault Code	Message
T:00	F:00	Initialization.
T:01	F:01	Testing Internal RAM.
T:02	F:02	Testing ALU.
T:03	F:03	Testing address modes.
T:04	F:04	Testing Boot ROM.
T:05	F:05	Testing timers.
T:06	F:06	Testing watchdog.
T:07	F:07	Testing external RAM.
T:08	F:08	Testing Host DPRAM.
T:09	F:09	Testing DS30 DPRAM.
T:10	F:10	Testing Security Device.

Table 11
ITG faceplate maintenance display code messages (Sheet 2 of 3)

Hex display code	Fault Code	Message
T:11	F:11	Testing flash memory.
T:12	F:12	Programming PCI FPGA.
T:13	F:13	Programming DS30 FPGA.
T:14	F:14	Programming CEMUX FPGA.
T:15	F:15	Programming DSP FPGA.
T:16	F:16	Testing CEMUX interface.
T:17	F:17	Testing EEPROM.
T:18	F:18	Booting processor, waiting for response with selftest information.
T:19	F:19	Waiting for application start-up message from processor.
T:20	F:20	CardLAN enabled, transmitting bootp requests. If this display persists, then the ITG Wireless card is running in BIOS ROM mode due to ITG Wireless card software failure.

Table 11
ITG faceplate maintenance display code messages (Sheet 3 of 3)

Hex display code	Fault Code	Message
T:21	F: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	F:22	The ITG Wireless card is attempting to start the ITG Wireless application.
Lxxx		Card is running active leader tasks, where xxx is the number of internet telephones registered on the card.
Fxxx		Card has detected the active leader, and is running Follower tasks, where xxx is the number of internet telephones registered on the card.
LDR		Card is running active leader tasks.
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.

Note: FLR is only displayed if the card is not properly displayed

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

If any of the other tests fail (up to and including the EEPROM test), a message is displayed to indicate this for three seconds. If more than one test fails, the message displayed indicates the first failure. If verbose mode has been selected (by the test input pin on the backplane), the three-second failure message is not 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 OTM or any SNMP manager that is configured in the SNMP Manager’s list in the ITG Wireless card properties.

SNMP also puts the system error message into the error log file containing error messages, which is available through the OTM ITG Wireless card properties by clicking on the “Open Log File” button on the “Maintenance” tab of the ITG Wireless card properties.

The log file can also be viewed in any text browser after uploading it to an FTP host using the **currLogFilePut** or **prevLogFilePut**. Events of the type **ITG4XX** and **ITG3XX** are written to the ITG face plate maintenance display, in the form “**Ixxx**”, 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) (Sheet 1 of 2)

Alarm Clearance - No intervention required	
ITG0100	Successful bootup. All alarms cleared.
ITG0101	Out of fallback.
ITG0105	Exit from card fallback. Leader card restored.
Minor Alarms - No intervention required	
ITG0203	Out of fallback.
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 TLAN.
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.
ITG0308	Address Translation failure. Call is released.
ITG0309	Unexpected DSP channel closed. Channel is unusable.
ITG0311	Unable to get response from Follower card.
ITG0312	Unable to push BOOTP tab file to backup leader.
ITG0313	Keycode validation failed.
ITG0320	Card at specified TN contains out of date boot information.
Major Alarms - Immediate Intervention Required	

Table 12
ITG system error messages (alarms) (Sheet 2 of 2)

ITG0402	Ethernet voice 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.
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	Leader does not exist.
ITG0416	Failed to start QoS Timer.
ITG0417	Failed to send fallback update to followers.
ITG0418	H.323 stack initialization failure.
ITGXXX	Insert entry error.
ITG0XXX	Unable to read bootp file, backup corrupted.
ITGIs0XXX	Unable to read password table file, backup corrupted.

Table 13 lists the Critical error messages.

Table 13
Critical ITG Error Messages

Maintenance Display	Corresponding Critical Error Message	Description
I300	ITG0300	Out of memory
I303	ITG0303	DSP failure
I304	ITG304	Unable to write to file
I309	ITG0309	Unexpected channel closed
I311	ITG311	Unable to get response from the card at specified TN
I320	ITG320	The card at specified TN contains out of date boot info
I402	ITG0402	Voice ethernet port disconnected
I404	ITG0404	Unable to read address translation table file or dialling plan table file
I406	ITG406	Unable to initialize memory buffer pool
I409	ITG0409	Bootp file corrupted
I411	ITG411	Unable to start UDP server for inter-card messaging
I412	ITG412	Unable to start UDP client for inter-card messaging
I413	ITG413	Failed to register with Leader card
I415	ITG0415	Leader does not exist
I416	ITG416	Failed to start QOS Timer
I418	ITG418	H.323 stack init failure

Replacing an ITG Wireless card

Replace an ITG Wireless card when the following conditions occur:

- If, following a reboot, the ITG Wireless card displays a code of the form "F:xx" on the faceplate LED display. This indicates an unrecoverable hardware failure and the card does not register with the Meridian 1. The exception is the "F:10" code, which occurs normally during start-up.
- If the management Ethernet interface or the voice Ethernet interface on the ITG Wireless card has failed. This can 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 TLAN cable are good.
- If a voice channel on the ITG Wireless 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.

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, replace the card.

Use the following procedure to replace a faulty ITG Wireless Card:

Procedure 29
Replace a faulty ITG Wireless card

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

2 Disable the faulty ITG Wireless card in LD 32 with the **DISI** command. The Meridian outputs "NPR011" when the card has been completely disabled by the DISI command.

3 Disconnect the TLAN Ethernet cable from the faceplate of the faulty ITG Wireless card in the Succession CSE 1000, Meridian large system IPE module, or the Option 11C cabinet. Label the cable to identify the LAN connection so that it can later be attached to the replacement ITG Wireless card.

> **CAUTION**
> **Damage to Equipment**
>
> In the Option 11C cabinet or Succession CSE 1000, the TLAN cable is hidden behind the faceplate of the ITG Wireless card. The card or cable can be damaged if an attempt to remove the cable is done without using the correct procedure.

Note: Refer to Appendix A for detailing instructions on connecting the TLAN cable to the ITG Wireless card in the Option 11C cabinet or Succession CSE 1000.

4 Remove the faulty ITG Wireless card from the Meridian 1 and Succession CSE 1000.

5 Install the replacement ITG Wireless card into the card slots in the Succession CSE 1000, Meridian 1 IPE module, or option 11 cabinet:

Note: Refer to Appendix A for detailing instructions on connecting the TLAN cable to the ITG Wireless card in the Succession CSE 1000 or Option 11C cabinet.

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

Note 1: When ITG Wireless 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. Refer to "Prior to communication with the Meridian 1, the 8051XA controller downloads FPGA data files and perform tests to ensure correct programming of the FPGA." on page 164 for a listing of display codes.

6 In the Meridian 1 large system IPE module, attach the TLAN Ethernet cable to the faceplate of the replacement ITG Wireless card.

Note 1: Refer to Appendix A for detailing instructions on connecting the TLAN cable to the ITG Wireless card in the Succession CSE 1000 or Option 11C cabinet.

Note 2: When connecting the ITG Wireless card to the TLAN, the link status LED on the ITG faceplate associated with the voice interface lights green when the connection is made, and the link status LED on the hub port also lights green when connected to the ITG Wireless card.

7 Use Procedure 4 on page 80 to set the card as the leader.

8 Select the ITG Wireless card in the OTM.

9 Click **Configuration | Node | Properties** in the "IP Telephony Gateway" window.

10 Click the **Configuration** tab in the "ITG Node Properties" window.

11 Change the "Management MAC" to the MAC address of the replacement ITG Wireless card. The MAC address is labeled on the faceplate of the replacement ITG Wireless card.

12 Click **Change**.

13 Click **OK** or **Apply**.

14 Use the **Configuration | Synchonize | Transmit** command to transmit the Node Properties from OTM to the new ITG Wireless card. Leave the default radio button selection “Transmit to Selected Nodes”. Check the **Node Properties**, **Card Properties** and **GK Properties** boxes, and then click **Start Transmit**. This updates the node properties on the replacement ITG Wireless card.

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

16 Reboot the ITG Wireless card.

17 Use the LD 32 ENLC command to re-enable the ITG Wireless card.

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

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

20 Verify the TN, management interface MAC address, and IP address for the ITG Wireless card. Compare the displayed values with those on the ITG Wireless Installation Summary sheet.

21 Make test calls on the new card to verify performance

End of Procedure

Procedure 30
Verifying ITG Wireless card software

1 In the “IP Telephony Gateway” window, double-click the replacement ITG Wireless card to open the “Card Properties”. Click the “Configuration” tab.

2 Verify that the “S/W release” shows the latest recommended ITG Wireless card software version.

Go to “http://www.nortelnetworks.com/support to check the latest recommended ITG software release.

End of Procedure

If the replacement card requires a software upgrade, refer to Procedure 16 on page 105.

Resolving problems with card replacement

Make test calls on the new card to verify good DSP channel performance.

Add an ITG Wireless card on OTM by retrieving an existing ITG Wireless card

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

- To add an existing ITG Wireless card to a particular OTM ITG PC in order to manage the ITG network from a single point of view.
- To restore the ITG configuration database to a OTM ITG PC whose hard drive had crashed. This is an alternative to restoring the OTM ITG Wireless cards from the OTM Disaster Recovery Backup.

> ***Note:*** In this section, the term “ITG Node” refers to the “ITG Wireless card”.

Once the ITG Wireless card has been installed and configured manually, that ITG Wireless card may be added to another OTM ITG PC by retrieving the configuration data from the existing ITG Wireless card.

The site name, Meridian 1 or Succession CSE 1000 system name, and Meridian 1 or Succession CSE 1000 customer number must exist in the OTM Navigator before a new ITG Wireless card can be added.

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

Configuring the ITG Wireless card

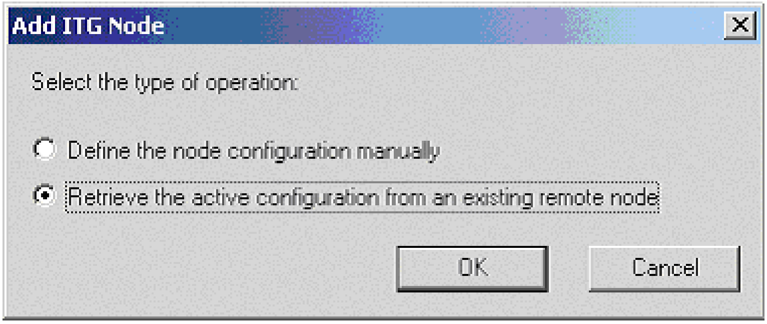
Procedure 31
Configure the ITG Wireless card

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

2 In the “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**. See Figure 40 on page 158.

Figure 40
Add ITG Node window.



Add ITG Node

Select the type of operation:

○ Define the node configuration manually

● Retrieve the active configuration from an existing remote node

4 In the “Retrieve ITG Node” window, select the OTM Site, OTM System, Customer and Node. See Figure 41 on page 159

Note: The site name, Meridian 1 or Succession CSE 1000 system name, and customer number must exist in OTM before a new ITG Wireless card can be added.

5 Enter the management IP address field for the ITG Wireless card on the existing ITG Wireless card.

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

7 Click the **Start Retrieve** button.

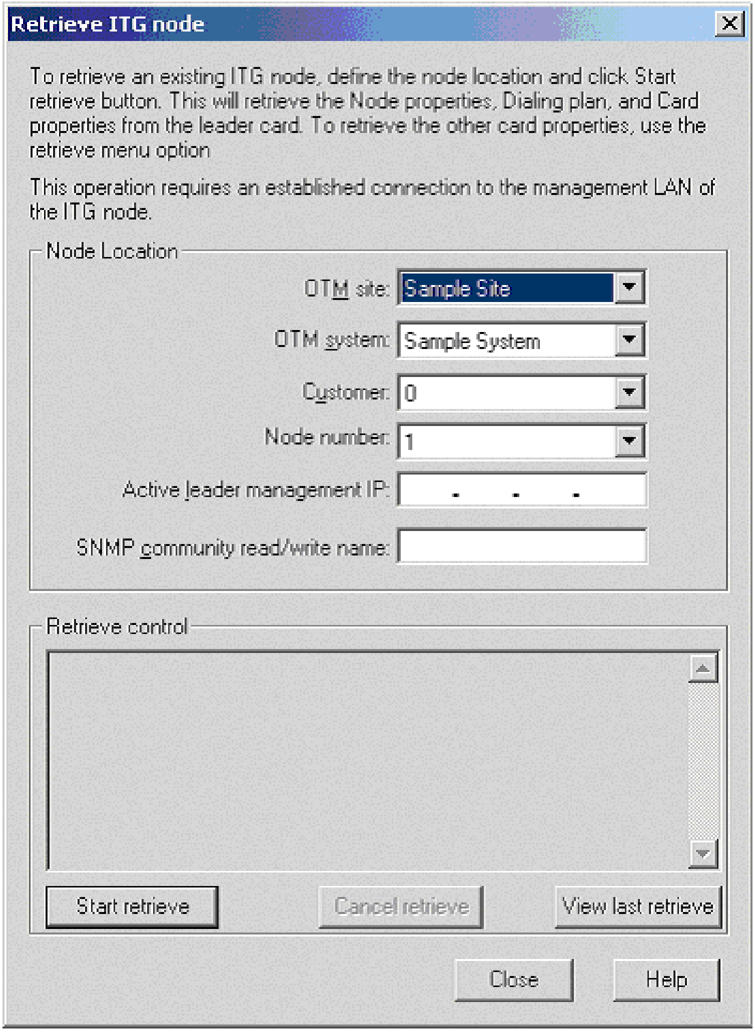
The results of the retrieval are shown in the “Retrieve control” dialog box. The ITG Wireless card properties are retrieved from the ITG Wireless card. The card properties are retrieved from the IP card.

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 ITG Wireless card are responding.

End of Procedure

Figure 41
Retrieve ITG node window



Retrieve ITG node

To retrieve an existing ITG node, define the node location and click Start retrieve button. This will retrieve the Node properties, Dialing plan, and Card properties from the leader card. To retrieve the other card properties, use the retrieve menu option

This operation requires an established connection to the management LAN of the ITG node.

Node Location

OTM site: Sample Site

OTM system: Sample System

Customer: 0

Node number: 1

Active leader management IP: . . .

SNMP community read/write name:

Retrieve control

Add a “dummy” ITG Wireless card to retrieve and view ITG Wireless card configuration

Use this procedure to create a “dummy” ITG Wireless card for retrieving and viewing the actual ITG Wireless card configuration, without over-writing the existing ITG configuration data for an existing ITG Wireless card in the OTM ITG database. Retrieving the actual ITG Wireless card configuration to the “dummy” ITG Wireless card is useful in the following cases:

- Isolating ITG Wireless card configuration faults
- Determining which copy of the database is correct, in order to determine the desired direction of database synchronization:
  - transmit OTM ITG to ITG Wireless card, or
  - retrieve ITG Wireless card to OTM ITG Wireless card.

The dummy ITG Wireless card can be added manually or by retrieving the ITG Wireless card configuration data from an existing ITG Wireless card.

The site name, Meridian 1 or Succession CSE 1000 system name, and customer number must exist in the OTM Navigator before a new ITG Wireless card can be added.

The following procedure is the recommended method to create the “dummy” ITG Wireless card.

Procedure 32
Create a dummy ITG Wireless card

1 In OTM Navigator add a site named “Retrieve ITG data.”

2 Add system named “Dummy,” of type “Meridian 1,” under the site named “Retrieve ITG data.”

3 Add Customer Number “99” on the “dummy” Meridian 1 system.

——————— ***End of Procedure*** ———————

To view the actual data on an existing ITG Wireless card, the technician selects the "dummy" ITG Wireless card and change the management IP address in the ITG Wireless card properties to access the desired ITG Wireless card. Use the **Configuration|Synchronize|Retrieve** function to retrieve data from that ITG Wireless card. This requires confirmation, allowing the system to over-write the OTM ITG data for the "dummy" ITG Wireless card.

Retrieve configuration information from the ITG Wireless card

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

- When adding an ITG Wireless card on OTM by retrieving an existing ITG Wireless card
- When it is suspected that the ITG Wireless card configuration on the ITG Wireless card differs from the OTM ITG database, for example, during maintenance and fault isolation procedures.
- When there are multiple OTM ITG PCs with multiple instances of the database (administration).

Procedure 33
Retrieving ITG configuration information from the ITG Wireless card

1 Launch the Meridian Administration Tools application on the OTM PC and double-click on ITG IP Telecommuter icon. The "IP Telecommuter" window opens.

2 In the "IP Telephony Gateway – IP Telecommuter" window, select Leader 0 or any card from the ITG Wireless card.

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:

5 Leave the default "Retrieve to selected nodes" when the OTM ITG data is out of date and all OTM ITG Wireless card data are synchronized with the data from the ITG Wireless card, or if adding an ITG Wireless card on OTM by retrieving from an existing ITG Wireless card.

6 Select "Retrieve from selected card" when attempting to isolate a problem with ITG configuration on a particular card.

7 Check the boxes for the ITG configuration data to be retrieved, depending upon the situation:

   a. Select “Node Properties,” “GK Properties” and “Card Properties,” if the OTM ITG data is out of date and all OTM ITG node data are synchronized with the data from the ITG Wireless cards on the node.

   b. Select “Card Properties” if adding a node on OTM by retrieving from an existing node that consists of more than one card.

   c. Select any combination of check boxes as indicated by problem symptoms, attempting to isolate a problem on a particular card. Use the “dummy” node for this purpose.

8 Click the **Start retrieve** button.

9 Monitor the progress of the retrieval in the “Retrieve control” box. The retrieved “Node Properties,” “GK Properties” and “Card Properties,” over-writes the existing OTM ITG configuration data for the respective node or card.

End of Procedure

ITG Wireless card commands

The ITG commands are accessed by connecting a TTY to the maintenance port on the ITG Wireless card faceplate. Commands are described in Appendix F: “ITG Wireless commands” on page 219.

ITG Wireless card self-tests

During power-up, the ITG Wireless card performs diagnostic tests to ensure correct operation. The faceplate maintenance port on the ITG Wireless 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, are echoed on this port.

Additionally, the ITG Wireless card has a hex LED display on the faceplate for the purpose of providing status information during maintenance operations. At power-up and during diagnostic tests, this display provides a visual indication of the progress of the selftest, and an indication of the first failure detected.

At power-up, the 8051XA controller on the ITG Wireless card takes control of the system and ensures that the processor is initially held in a reset state. The 8051XA controller takes control of one of the faceplate maintenance ports and uses 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 then attempts to bring up the processor by clearing the reset, and entering a timing loop in anticipation of receiving a message from the processor. If this loop times out, it sends an error to the faceplate maintenance port. It attempts to bring up the processor two more times before indicating an unrecoverable card failure.

Similarly, if a message is received from the processor, but the message indicates a failure of one or more of the circuit elements connected to the processor, up to two more resets are 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 faceplate maintenance port, however, to provide information to the maintenance technician that there might be a problem with the card.

Once the processor responds correctly, the 8051XA controller swatches its serial port to provide Card LAN communication and connect the processor with the external RS-232 port.

Card LAN

The ITG Wireless card supports the backplane Card LAN interface to communicate selftest errors and allow maintenance access such as resetting the card remotely.

BIOS selftest

The ITG Wireless card contains its own VxWorks based BIOS. At power-up, the BIOS performs its own initial test of the hardware. These tests cover the processor, PCI chipset, cache (if installed) and DRAM memory. The results of the BIOS self test are displayed on the faceplate maintenance port.

Base Code selftest

The ITG Wireless card base code performs the following tests:

- flash integrity test
- PGA read/write test
- PCMCIA controller test (also tests the PCI bus)
- Timer and DMA tests
- DSP test

FPGA testing

Prior to communication with the Meridian 1, the 8051XA controller downloads FPGA data files and perform tests to ensure correct programming of the FPGA.

Troubleshooting a software load failure

Symptoms

OTM cannot establish connection with the ITG Wireless card. The faceplate LCD display reads “BIOS.”

Type “JKL” to boot to the BIOS.

Problem

The ITG Wireless card has booted the BIOS load.

Diagnosis

In the event of a failure to load and run the ITG software, the ITG Wireless card defaults 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 faceplate maintenance 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 ITG Wireless card locating and loading the ITG software from flash memory:

```
Cookie array value:     0x11111100


Checksum Validation at Bank Address: 0xF9800000
Checksum in ROM =       98E899DF
Length of bank  =       001641A8
Calculated Checksum =   98E899DF


Checksum array value:   0x11111100


Loading code from address: F9800010


Cookie Address : 0xF9800010
Cookie Value   : 0x90909090


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:

```
Jumping to romStart at 0x00E00300
Booting from BIOS ROM
```

Case 3:

The boot sequence indicates that the “JKL” 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 OTM host. Use the following commands:

```
upgradeErase
upgrade "hostname","hostAccount","hostPassword",
     "hostDirectoryPath","hostSWFilename"
```

After the software loads to flash, reboot the card:

```
sysReboot
```

If the failure to load the ITG software into RAM persists, then the flash device is faulty. Replace the ITG Wireless card.

Case 3:

The escape sequence “JKL” is rarely transmitted. Reboot the card.

Warm rebooting the ITG Wireless card

The following ITG shell command performs a warm reboot of an out-of-service ITG Wireless card:

cardReset

Working with alarm and log files

Alarm and log file output is turned on through 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

Contents

This section contains information on the following topics:

Overview

This appendix describes the NTMF94EA, NTAG81CA and NTAG81BA cables required to cable the ITG Wireless card assembly.

NTMF94EA I/O cable

The NTMF94EA cable provides the signals to the ELAN and TLAN ports that provide the interface from the ITG Wireless 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 42 on page 171. Table 42 describes the NTMF94EA cable pins.

DANGER OF ELECTRIC SHOCK
Use the mounting screw provided on the top of the 25- pair amphenol connector to secure the NTMF94EA cable to the Meridian 1 and Succession Communication Server for Enterprise 1000. The screw ties the LAN cable shield to the Meridian 1 and Succession CSE 1000 frame ground for EMC compliance.

The NTMF94EA cable provides a factory installed, shielded RJ45-to-RJ45 coupler at the end of both its ELAN and TLAN ports. Both of the RJ45 ends of the cables are clearly labelled as to which is the TLAN and which is the ELAN. These provide the connection point to the customer's ELAN and TLAN equipment. Shielded Cat. 5 cable must be used for connection from this point to the customer's hub or router.

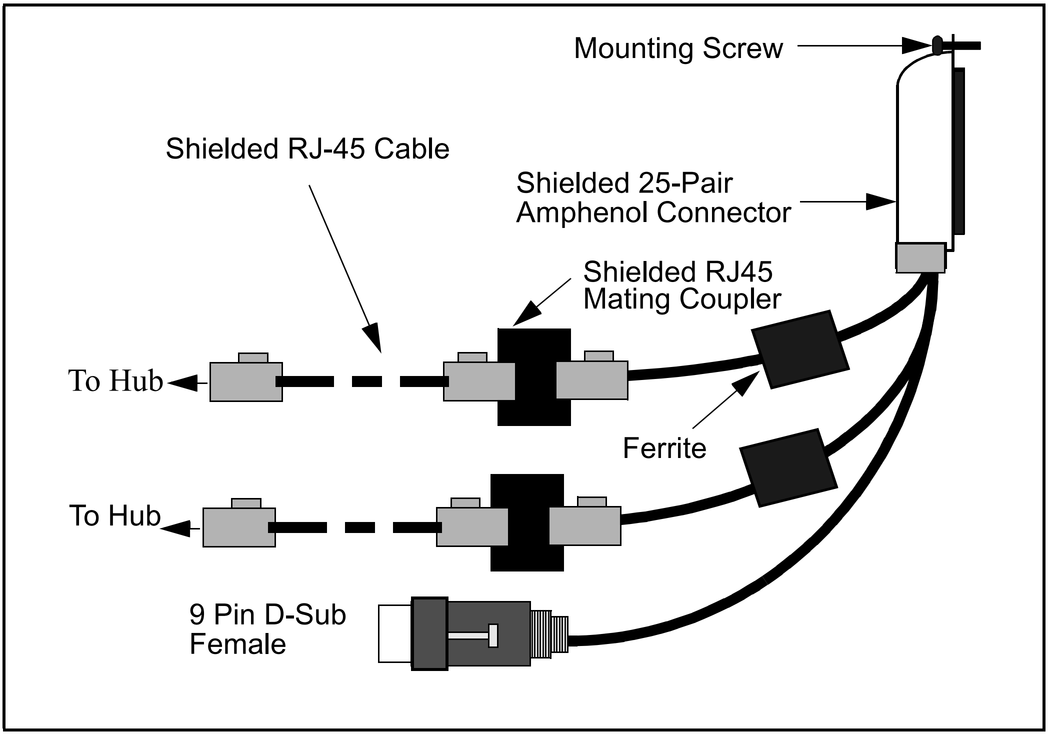
> ***Note:*** Use standard cable ties to bundle all LAN cables together as they route out of the system.

Shielded Category 5 cable for external ITG Wireless card LAN connections

Only Shielded Cat 5 cable is to be used to connect from the Meridian 1 I/O backplane (Small Systems) or I/O panel (Meridian 1 large systems) to the customer's hub or router. Ground the cable shields at one end only – either at the I/O panel connector or at the hub, but not at both ends.

Use the appropriate grounded or non-grounded RJ45 coupler provided with the I/O cable assembly to ground the shield, or isolate the shield at the I/O panel.

Figure 42
NTMF94EA management port, voice port and serial I/O cable (Meridian 1 large system)

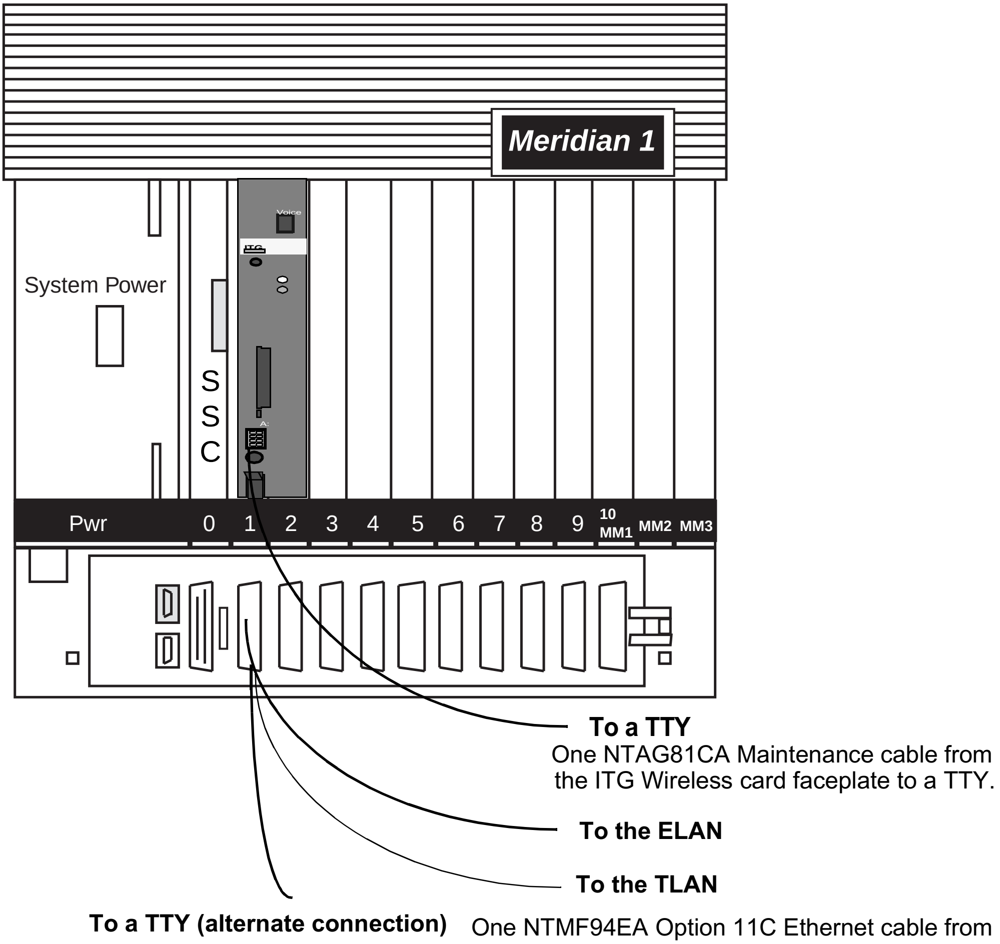


Refer to “Preventing ground loops on connection to external customer LAN equipment” on page 185 for information on how to conduct a test for ground loops.

Connector pin assignments

Table 14 on page 173 shows the I/O Connector pin designations for the ITG Wireless card.

Figure 43
I/O cabling for NTEZ04AA ITG Wireless card – in Meridian 1 Option 11C



To a TTY
One NTAG81CA Maintenance cable from the ITG Wireless card faceplate to a TTY.

To the ELAN

To the TLAN

To a TTY (alternate connection)

One NTMF94EA Option 11C Ethernet cable from the I/O backplane to the ELAN and TLAN.

Table 14
ITG Wireless card I/O Panel Pinout (Sheet 1 of 2)

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
2	R1	Not Used	26	T0	Not Used
3	R2	Not Used	27	T1	Not Used
4	R3	Not Used	28	T2	Not Used
5	R4	Not Used	29	T3	Not Used
6	R5	AGND	30	T4	AGND
7	R6	Not Used	31	T5	Not Used
8	R7	Not Used	32	T6	Not Used
9	R8	Not Used	33	T7	Not Used
10	R9	AGND	34	T8	AGND
11	R10	PGT0	35	T9	PGT1
12	R11	PGT2	36	T10	PGT3
13	R12	PGT4	37	T11	PGT5
14	R13	PGT6	38	T12	PGT7
15	R14	PGT8	39	T13	PGT9
16	R15	PGT10	40	T14	PGT11

Table 14
ITG Wireless card I/O Panel Pinout (Sheet 2 of 2)

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
17	R16	SGNDA	41	T15	BDCCDA-
18	R17	BSINA-	42	T16	BSOUTA-
19	R18	BDTRA-	43	T17	SGND
20	R19	BDSRA-	44	T18	BRTSA-
21	R20	BCTSA-	45	T19	BSINB-
22	R21	BSOUTB-	46	T20	BDC dB-
23	R22	BDTRB-	47	T21	BDSRB-
24	R23	DI+	48	T22	DI-
25	R24	DO+	29	T23	DO-
2	R1	no connect	50	no connect	no connect

Table 15
NTMF94EA cable pin description

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	BDC dB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RX dB+	P4-3	GRN/WHT
P1-19	TX dB+	P4-1	ORG/WHT
P1-43	RX dB-	P4-6	WHT/GRN
P1-44	TX dB-	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

NTAG81CA Maintenance Cable

This cable is required to connect a PC or terminal to the ITG Wireless card through the maintenance port connector on the faceplate for administration. This cable can be connected directly to the 9-pin D-type RS232 input on a standard PC.

Figure 44
NTAG81CA Maintenance cable

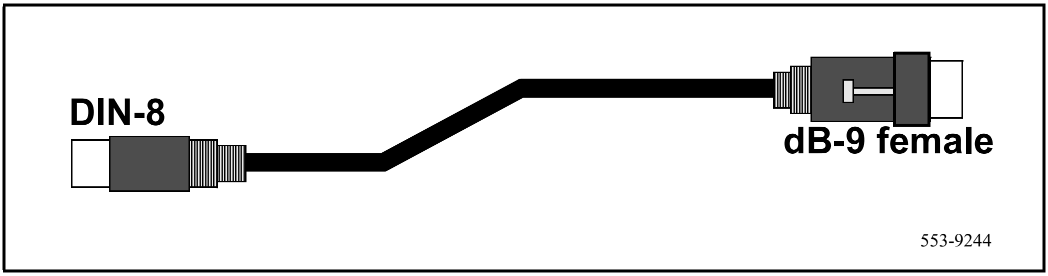


Table 16
Maintenance cable connections

Signals (MIX Side)	8-pin Mini-DIN (MIX Side) Male	9-pin D-Sub (PC Side) Female	Signals (PC Side)
DTRB-	1	6	DSR-
SOUTB-	2	2	SIN-
SINB-	3	3	SOUT-
GND	4	5	GND
SINA-	5	nc	nc
CTSA-	6	nc	nc
SOUTA-	7	nc	nc
DTRA-	8	nc	nc

NTAG81BA Maintenance Extender cable

This three-meter cable connects the NTAG81CA cable to a PC or terminal. It has a nine-pin D-type connector at both ends, one male, one female. It can also be used to extend the serial port presented by the NTMF94BA I/O panel cable.

Figure 45
NTAG81BA Maintenance Extender cable

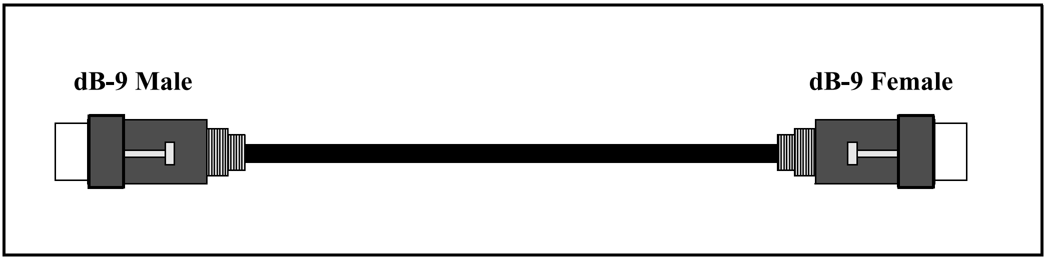
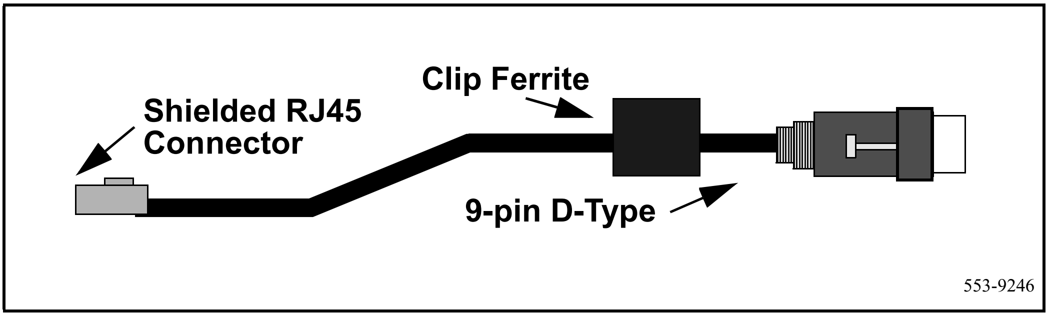


Table 17
Maintenance cable connections

9-pin D-Sub (Male)	9-pin D-Sub (Female)
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

Figure 46
NTCW84GA Shielded Faceplate Ethernet cable



9-pin D-Sub (Male)	10-pin RJ-45
1	1
2	2
3	3
6	6

Route the NTCW84GA cable

1 Attach the 9 pin D-Sub end of the cable to the 9 pin D-Sub socket on the faceplate of the ITG Wireless card (socket labelled NWK - “Network”), securing the cable fast with the available screw heads provided on the cable.

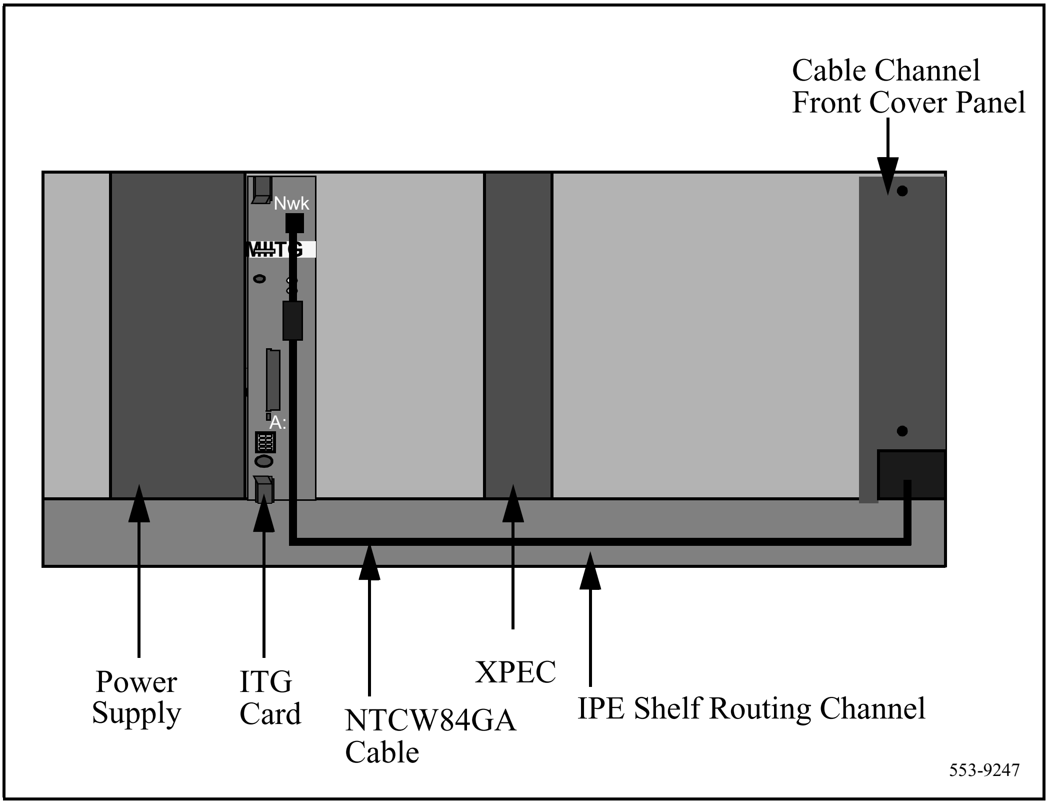
2 Allow the cable to drop from the connector vertically down along the faceplate to the front routing channel so that it does not impede removal or insertion of adjacent IPE cards

3 Route the cable along the front cabling channel to the right hand side of the IPE Shelf.

Note: The cable must be routed around to the back of the shelf so that it can mate with the shielded RJ-45 coupler in the I/O panel bracket. As the shelf power supply is positioned on the left hand side of the IPE shelf, routing the NTCW84GA cable around to the back of the system on the front left hand side is not recommended.

4 Route the cable around to the back of the IPE Shelf through the routing channel available on the side of the IPE Shelf. If routing is difficult, it is possible to unscrew the cable routing channel cover bracket which covers the gap between the last right-most IPE card and the side of the shelf itself. Ensure that this bracket is replaced once the cable has been successfully routed. See Figure 47 on page 179.

Figure 47
Routing path for ITG Wireless card Faceplate cable – Meridian 1 large system IPE shelf



Once the cable has been routed around to the back of the IPE shelf, the RJ45 end of the cable should be inserted into one of the two available shielded RJ45 coupler on the I/O Mounting Bracket as indicated in Figure 48 on page 183.

Choosing the I/O Panel location for the I/O Mounting Bracket

Some variances must be accounted for when choosing the I/O panel opening into which the I/O Mounting Bracket is being installed.

IPE Shelf System Variances

Currently Meridian 1 and Succession CSE 1000 shelves have 2 wiring setups between the backplane and the I/O panel:

1. NT8D37BA or later IPE modules have 24-pair Tip and Ring wiring where all 16 MDF I/O Panel openings are pre-wired for MDF connection (no free I/O panel locations immediately available):

   In this IPE I/O panel wiring setup, the position of the RJ45 Mounting Bracket is dependent on the card slots where the ITG Wireless cards are installed. As each ITG Wireless card takes up two slots, one MDF I/O Panel location corresponding to the right hand card slot of the ITG Wireless card slot assembly is always free. Only the left hand card slot of the ITG Wireless card uses Tip and Ring connections from the backplane to the I/O panel.

   The existing backplane to I/O panel cable assembly (NT8D81AA) should be removed from the I/O panel for the unused location corresponding to the right hand card slot and the I/O Panel Mounting Bracket should be installed in the now vacant slot.

   The left hand card slot of the ITG Wireless card has the NTMF94BA cable connected to the corresponding I/O panel location which are discussed in later sections. Note that this cable requires 24 pair Tip and Ring I/O wiring. This cable has a large ferrite pre-positioned approximately 2-3 inches below the 50 pin
   I/O connector.

CAUTION
Damage to Equipment
Care should be taken in the positioning of this cable and ferrite combination with respect to the positioning of the RJ45 I/O panel mounting bracket so as to avoid any possible straining on the shielded TLAN Ethernet cables plugged into the outside of the RJ45 mounting bracket.

It is essential to choose a card slot and corresponding I/O panel locations for the RJ45 I/O panel mounting bracket which is not up against the ferrite on the NTMF94BA.

2 NT8D37AA IPE modules have 24-pair Tip and Ring wiring for card slots 0,4,8 and 12 only:

In this case there are four I/O Panel connector locations - D, H, N and U, which is not pre-wired from the backplane to the I/O panel and the unused locations are shielded with metal knock-outs. Note that if this is the IPE module type then the ITG Wireless card itself can only be installed in card slots 0 and 1,4 and 5,8 and 9 and 12 and 13 where the left hand ITG Wireless card slot is the even-numbered card slot.

Note: To add 24-pair I/O Tip and Ring wiring for slots in this module, order the NT8D81AA backplane to I/O panel cable assembly.

To install the RJ45 I/O panel mounting bracket, choose one of the unused I/O panel locations, and push out the protective metal knock-out and install the RJ45 mounting bracket in the open location.

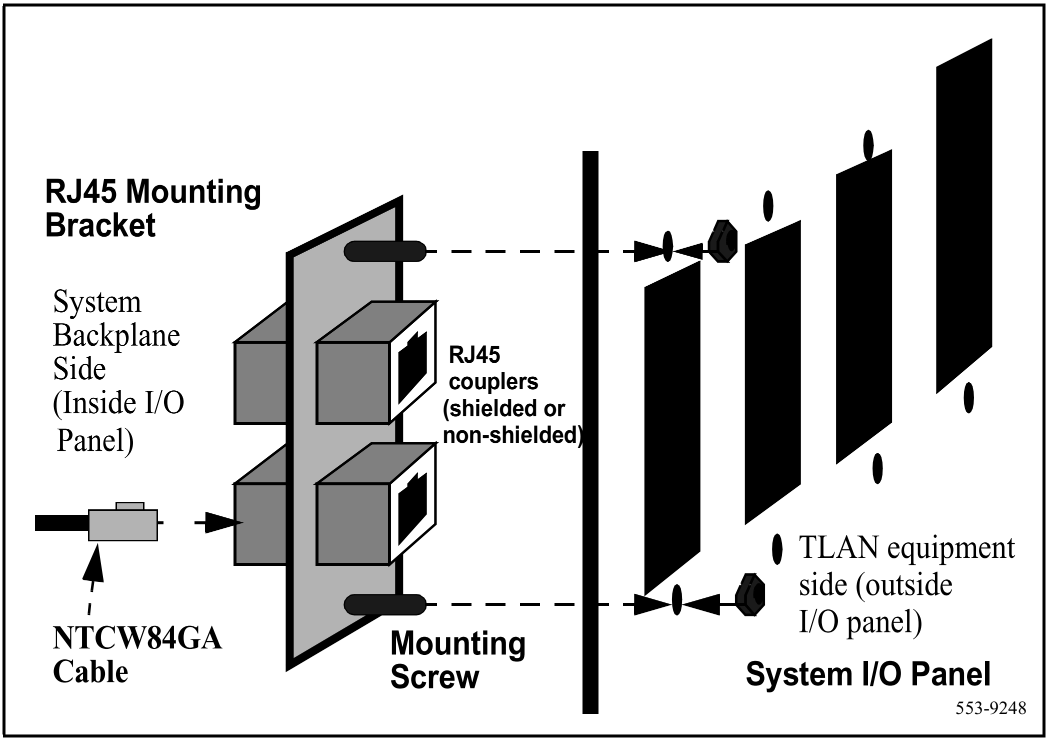
See Caution on page 181. Care must be taken in the relative positioning of the RJ45 I/O panel mounting bracket and the ferrites on the NTMF94EA ELAN and serial port cables. Required placement for this IPE module type in order to provide the required 24-pair Tip and Ring I/O wiring is provided in Table 18.

Table 18
ITG Wireless card slots and corresponding RJ45 mounting bracket locations

ITG Wireless card slots	RJ45 mounting bracket locations
0/1	H or B
4/5	D
8/9	U or L
12/13	N

Note: For all LAN cables originating from the ITG Wireless card, standard cable ties should be adopted to bundle these cables together as they route out of the system.

Figure 48
Installation view for I/O mounting bracket


RJ45 Mounting Bracket
System Backplane Side (Inside I/O Panel)
RJ45 couplers (shielded or non-shielded)
NTCW84GA Cable
Mounting Screw
TLAN equipment side (outside I/O panel)
System I/O Panel
553-9248

Installing the I/O Mounting Bracket

Figure 48 on page 183 shows the installation methodology for the RJ45 bracket. Each bracket supports two NTCW84GA cables and the TLAN interfaces for two ITG Wireless cards.

1 The I/O bracket fits into the standard 50 pin MDF cable openings provided on the I/O panel of the IPE Shelf. The bracket is pushed out through the opening from inside the I/O panel as indicated in the diagram and is secured via the screw and nut set provided.

2 The external TLAN network connections are then inserted into the opposing side of the shielded coupler into which the NTCW84GA cable has been installed. Shielded RJ45 cable is required for routing to the customer’s equipment. Routing of the RJ45 cable out of the system should follow the standard routing path as for MDF cables.

NTCW84FA Option 11C Shielded Drop-Down TLAN Ethernet cable

NTCW84FA takes advantage of the fact that the ITG daughterboard takes up the complete second slot of the ITG assembly but does not interface with the lower card guide rails. An internal daughterboard RJ-45 connector provides a second access point on the ITG assembly to the Voice Ethernet port (TLAN) in parallel with the faceplate connection point. NTCW84FA connects to this as shown. The cable is three meters long and provides a shielded male to male RJ45 coupler at the end point.

This is the connection point for the customer’s LAN cable to the Hub or Router supporting the TLAN.

External LAN cabling for EMC compliance

The ITG Wireless card or other ITG products require that the connection from the I/O panel to the customer’s hub or router must use Shielded Category 5 cable only.

Preventing ground loops on connection to external customer LAN equipment

The shielded (or unshielded, see step 3 below) RJ45 coupler is the connection point for the customer's shielded Category 5 LAN cable to the hub, switch, or router supporting the TLAN.

> ***Note:*** Shielded Category 5 RJ45 cable must be used when connecting to the customer's TLAN 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. It must measure open to ground before plugging it into the shielded RJ45 coupler on the end of the NTCW84FA

3 If it does not measure open to ground, an unshielded RJ45 coupler must be substituted on the end of the NTCW84FA in order to prevent ground loops to external LAN equipment.

Installing the NTCW84FA Cable in the Option 11C

The next figure shows a side view of the ITG Wireless card as it would be inserted into the Option 11C.

To connect the NTCW84FA cable in the RJ45 coupler for drop down insertion, the following steps are required:

1 Insert the ITG partially into the Option 11C card slot for which it is configured.

2 Push the NTCW84FA drop-down cable up through the front-most opening in the Option 11C cabinet lower grill of the right hand card slot of the ITG Wireless card.

3 Bring the cable up through the front opening in the ITG stiffening-frame positioned near the very front of the card assembly.

4 Insert the RJ45 plug into the shielded and filtered RJ45 connector on the ITG Wireless card daughterboard.

5 Push the ITG Wireless card fully into the Option 11C card slot and release any kinks in the drop down cable.

Figure 49
NTCW84FA Voice Ethernet cable for Option 11C

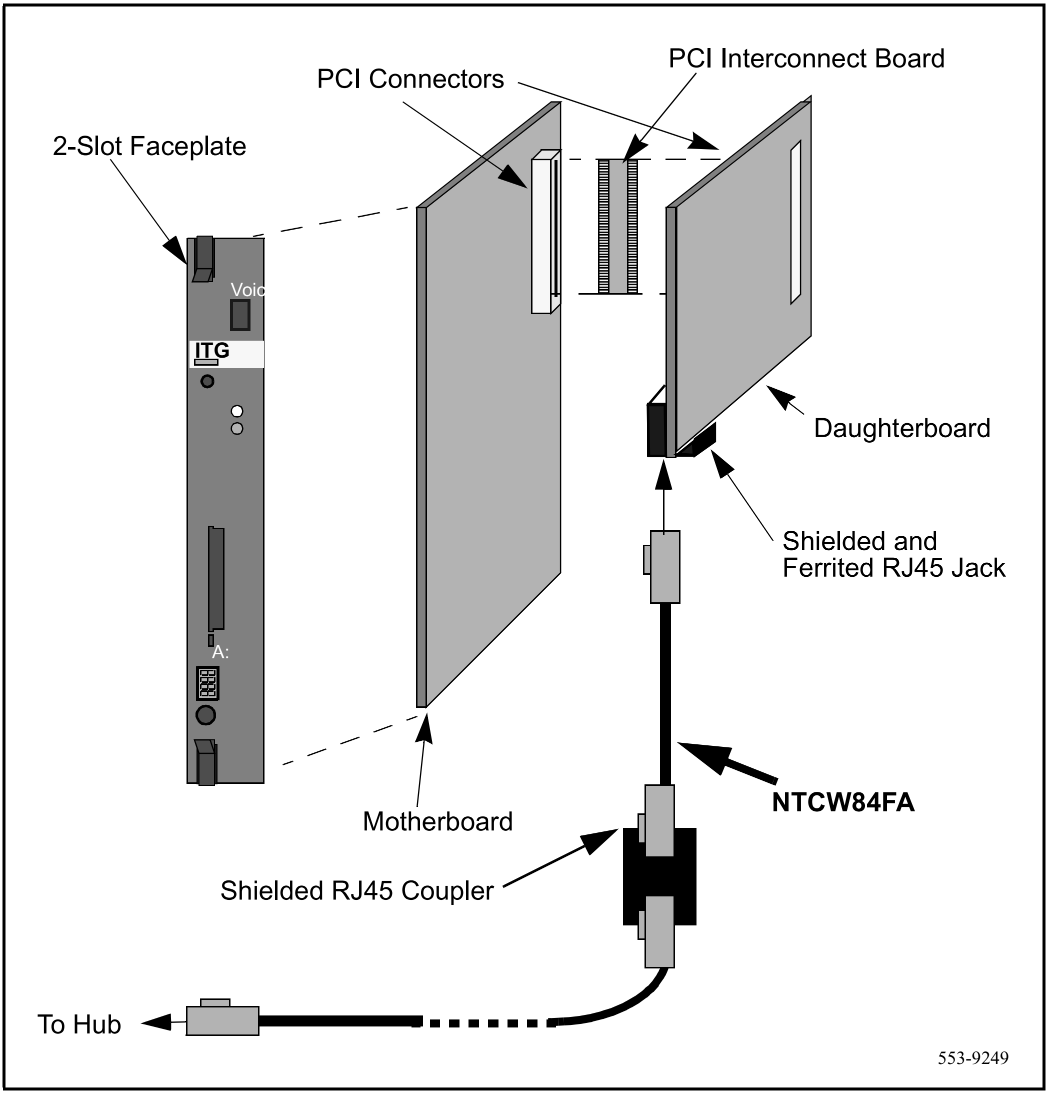
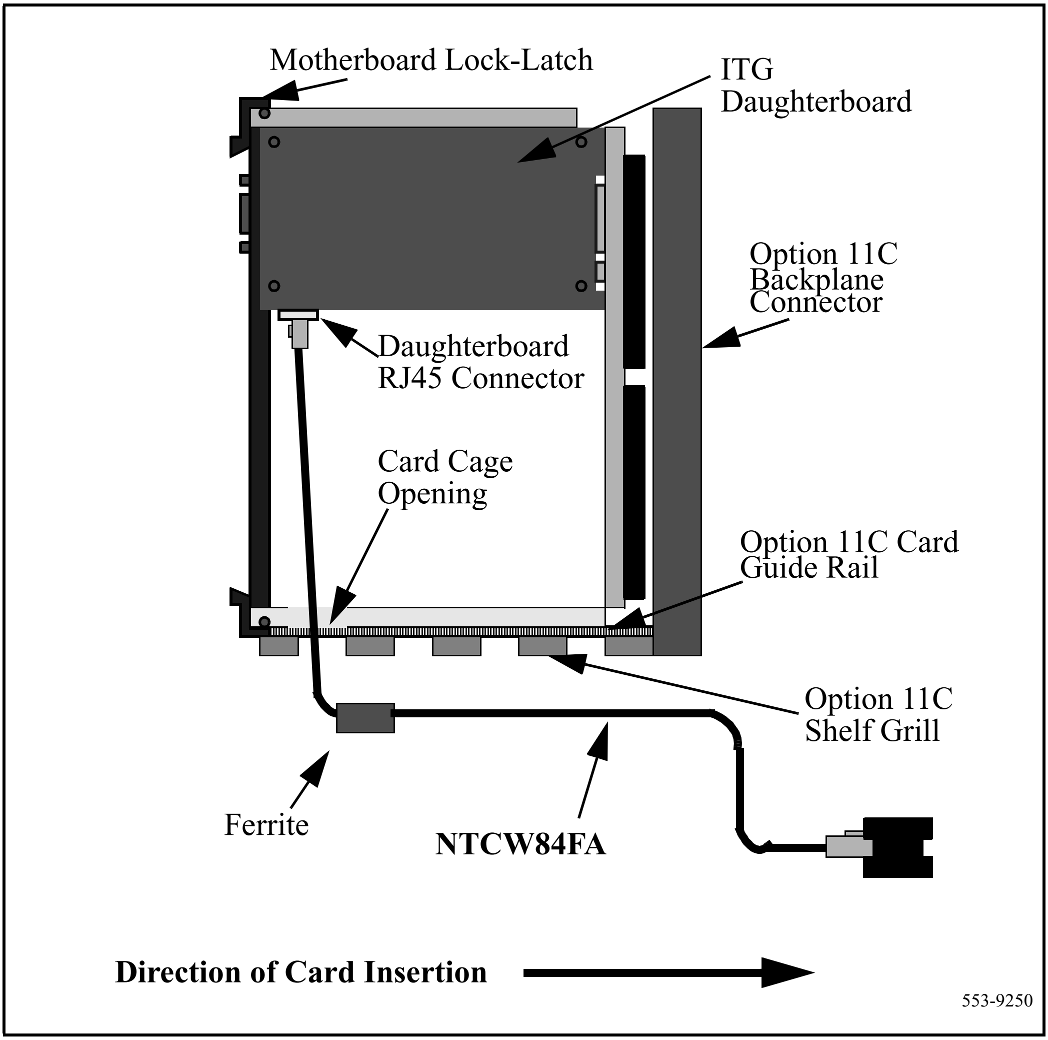


Figure 50
NTCW84FA cable routing in the Option 11C cabinet


Motherboard Lock-Latch
ITG Daughterboard
Option 11C Backplane Connector
Daughterboard RJ45 Connector
Card Cage Opening
Option 11C Card Guide Rail
Option 11C Shelf Grill
Ferrite
NTCW84FA
Direction of Card Insertion
553-9250

6 The left hand card slot of the ITG Wireless card has the NTMF94BA ELAN and serial port cable inserted into its corresponding 50-pin I/O panel connector.

Route the NTCW84FA TLAN cable out of the Small System cabinet through the same cable opening that is being used by the NTMF94BA ELAN and serial port cable. The TLAN cable should be routed under the Option 11C I/O connector cable retention bar as indicated in Figure 51 on page 189. The example assumes the ITG Wireless is in card slot 0).

7 The NTCW84FA cable provides a shielded RJ45 coupler for connection to the customer's TLAN equipment.

External LAN cabling for EMC compliance

The ITG Wireless card or other ITG products require that the connection from the I/O panel to the customer's hub or router must use Shielded Category 5 cable only.

Preventing ground loops on connection to external customer LAN equipment

The shielded (or unshielded, see step 3 below) RJ45 coupler is the connection point for the customer's shielded Category 5 LAN cable to the hub, switch, or router supporting the TLAN.

> ***Note:*** Shielded Category 5 RJ45 cable must be used when connecting to the customer's TLAN equipment.

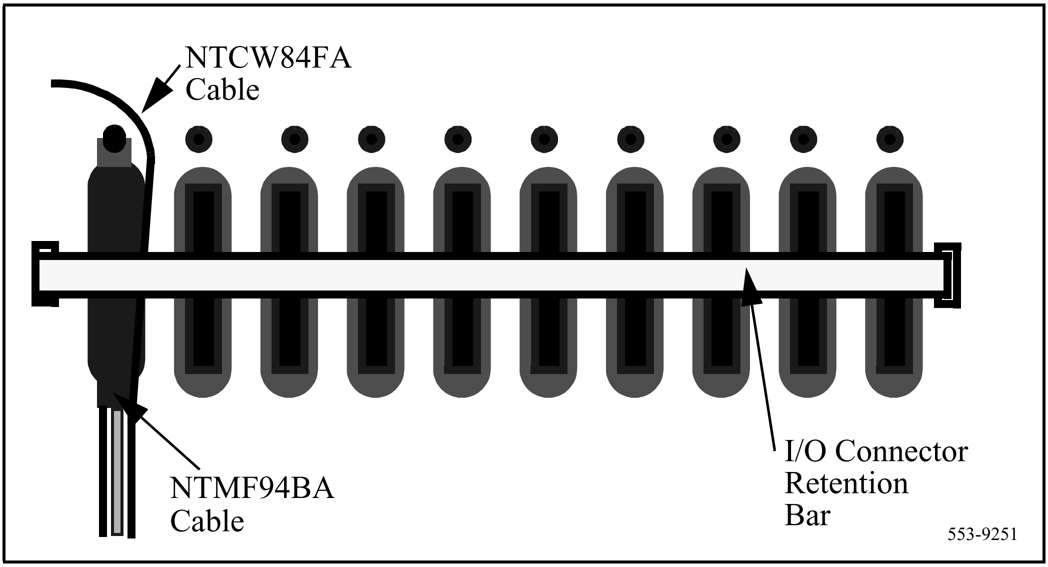
1 Connect the customer-provided shielded Category 5 LAN cable to the external LAN equipment. Ensure that the external LAN equipment is powered-up.

2 Use an ohmmeter to measure resistance to ground between the free end of the shielded RJ45 cable and building ground. It must measure open to ground before plugging it into the shielded RJ45 coupler on the end of the NTCW84FA

3 If it does not measure open, an unshielded RJ45 coupler must be substituted on the end of the NTCW84FA in order to prevent ground loops to external LAN equipment

Note: Use standard cable ties to bundle together all LAN cables originating from the ITG Wireless card.

Figure 51
NTCW84FA cable routing at Small System I/O panel



Removing the NTCW84FA cable (and the NTCW80AA assembly on Option 11C)

To remove the NTCW84FA cable from the ITG Wireless card to allow the ITG to be removed from the cabinet, perform the following:

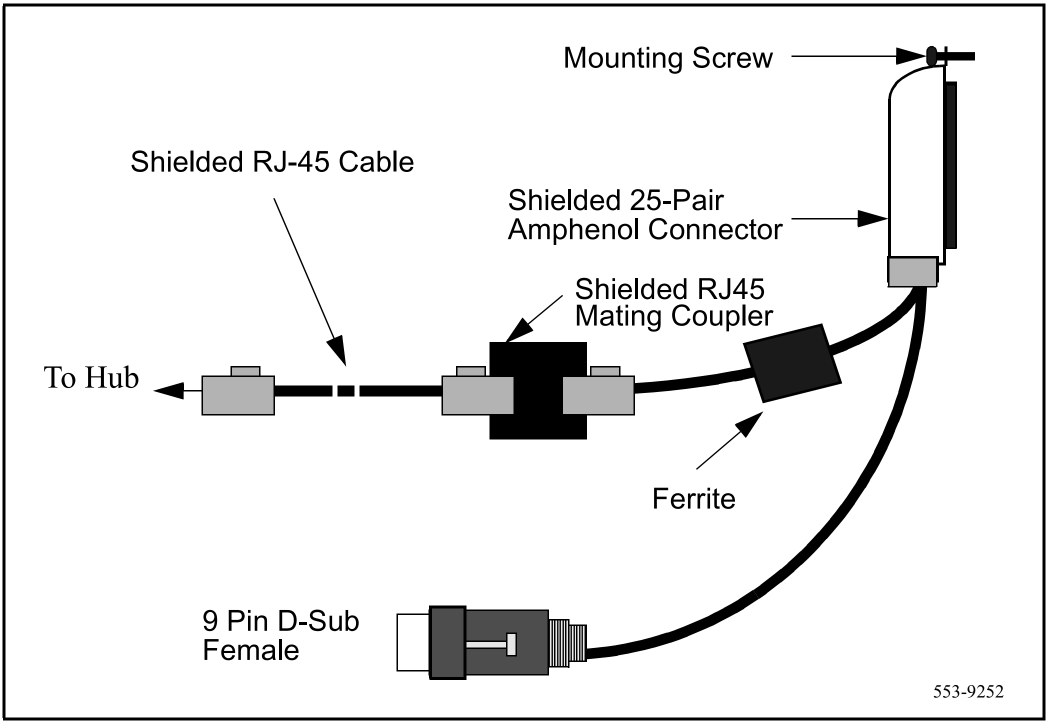
1. Unseat the ITG Wireless card from the Option 11C backplane and slide out the first third of the card so that the NTCW84FA cable is exposed.
2. Remove the shielded RJ45 connector from the jack on the lower edge of the daughterboard and drop the cable down through the ITG stiffening-frame and through the Option 11C cabinet lower grill.
3. Remove the ITG Wireless card completely.

NTMF94BA ELAN & serial port cable

The NTMF94BA cable breaks out the signals from the I/O connector on a small system cabinet, or the I/O panel on the IPE module of the Meridian 1 large systems, to the ethernet management port (ELAN connection) plus one RS232 maintenance port brought out on a dB-9 female connection.

On Meridian 1 large system IPE modules, the NT8D81AA cable is used to bring all
24-pair tip and ring cables from the left hand card slot from the backplane to the I/O panel and mates with the NTMF94BA cable. In the small system the NTMF94BA cable connects directly to the I/O connector at the bottom of the cabinet.

Figure 52
NTMF94BA ELAN and serial port cable



It is very important that the 50-pin connector of the NTMF94BA cable be secured to the I/O connector using the mounting screw provided on the top of the 50-pin connector, as well fasteners on the bottom, in order to tie the shield of the LAN cable to the Meridian 1 and Succession CSE 1000 frame ground for EMC compliance.

The NTMF94BA cable provides a shielded RJ45 coupler at the end of the cable's ELAN interface. This provides the connection point to the customer's ELAN equipment.

> ***Note:*** Shielded Category 5 cable must be used for connection from this point to the customer's Hub or Router.

External LAN cabling for EMC compliance

The ITG Wireless card or other ITG products require that the connection from the I/O panel to the customer's hub or router must use Shielded Category 5 cable only.

Preventing ground loops on connection to external customer LAN equipment

The shielded (or unshielded, see step 3) RJ45 coupler is the connection point for the customer's shielded Category 5 LAN cable to the hub, switch, or router supporting the TLAN/ELAN.

> ***Note:*** Shielded Category 5 RJ45 cable must be used when connecting to the customer's TLAN/ELAN 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. It must measure open to ground before plugging it into the shielded RJ45 coupler on the end of the NTMF94BA.

3 If it does not measure open, an unshielded RJ45 coupler must be substituted on the end of the NTMF94BA in order to prevent ground loops to external LAN equipment.

CAUTION
Service Interruption

The serial maintenance ports presented at the DIN 8 Faceplate connector and at the dB-9 female connector of the NTMF94BA cable assembly are identical. Do not connect to both access points simultaneously. This results in incorrect and unpredictable operation of the ITG Wireless card.

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

Category 5 cable can be damaged by overtightening cable ties.

Figure 53
NTMF94EA management port, voice port and serial I/O cable (Meridian 1 large system)

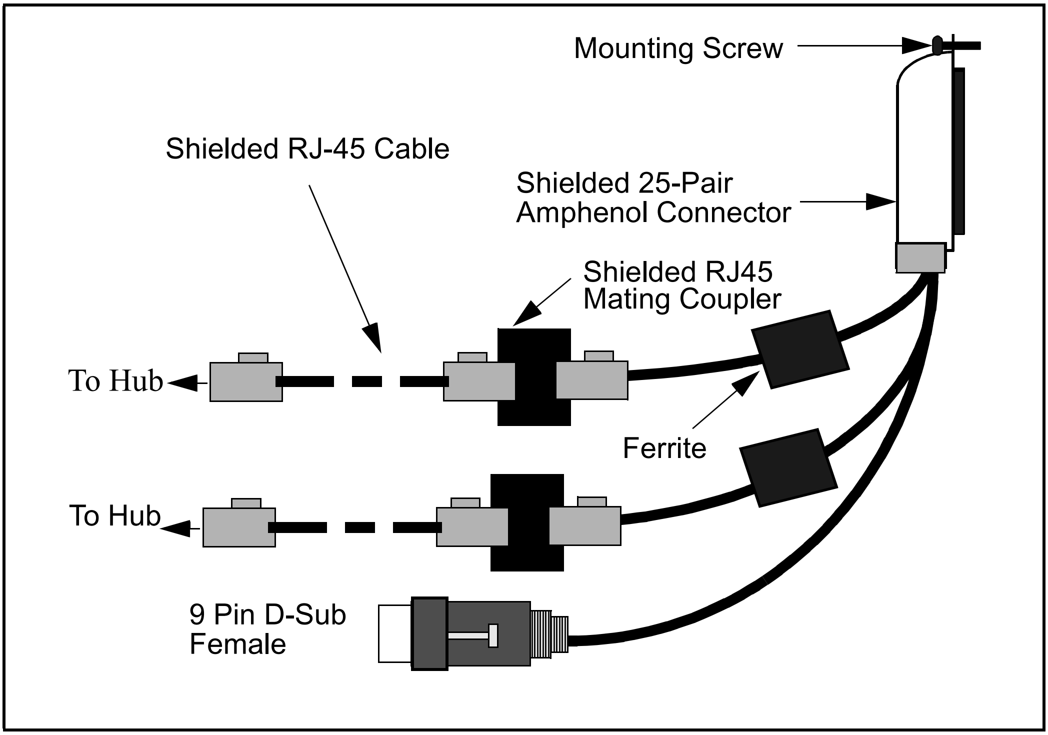
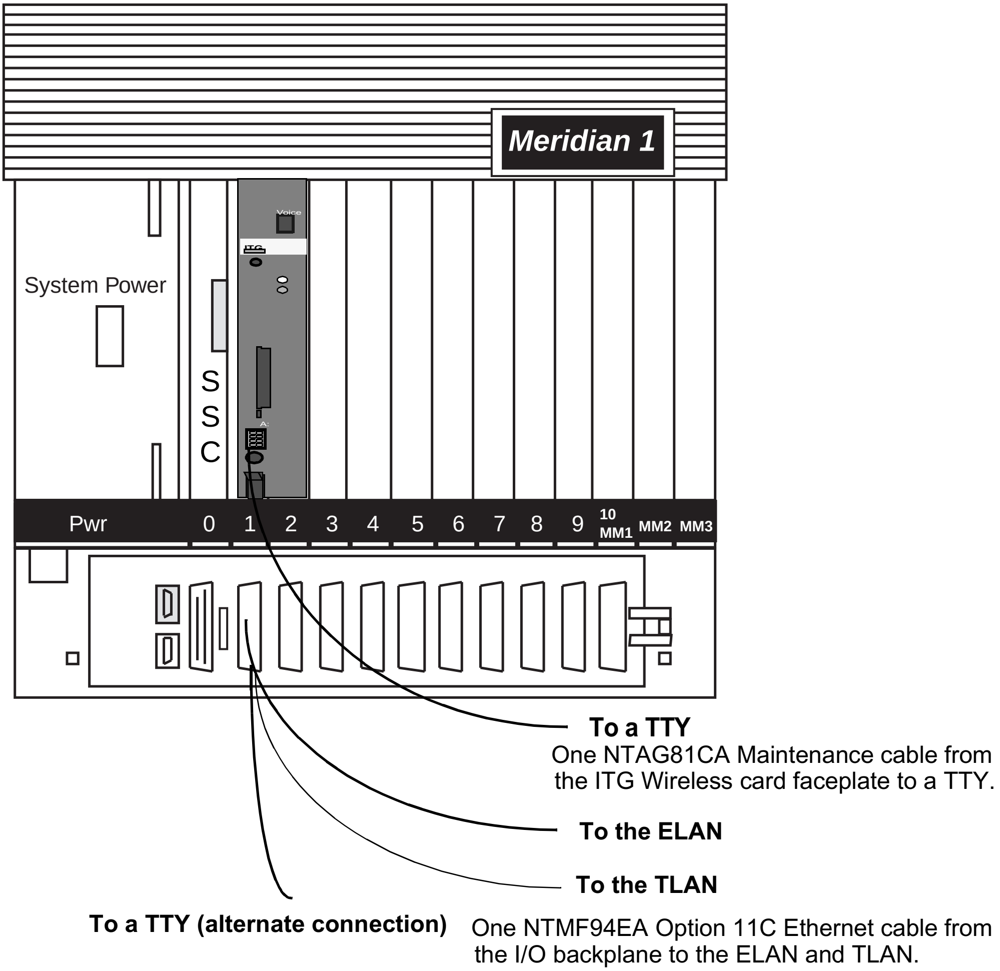


Figure 54
I/O cabling for NTEZ04AA ITG Wireless card – in Meridian 1 Option 11C



To a TTY
One NTAG81CA Maintenance cable from the ITG Wireless card faceplate to a TTY.

To the ELAN

To the TLAN

To a TTY (alternate connection)

One NTMF94EA Option 11C Ethernet cable from the I/O backplane to the ELAN and TLAN.

Appendix B: I/O, maintenance and extender cable description

Contents

This section contains information on the following topics:

This appendix describes the NTMF94DA, NTAG81CA and NTAG81BA cables.

NTMF94DA I/O cable

The NTMF94DA provides the ELAN/ TLAN ports that provide the interface from the ITG Wireless 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 55 on page 196. Table 19 on page 197 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 and Succession Communication Server for Enterprise 1000. The screw ties the LAN cable shield to the Meridian 1 and Succession CSE 1000 frame ground for EMC compliance.

The NTMF94DA cable provides a factory installed, shielded, RJ45 to RJ45 coupler at the end of both the ELAN and TLAN ports. An unshielded coupler is provided to prevent ground loops (if required). See page 198 for a test that helps decide if the unshielded coupler must be used. Both ends of the RJ45 ports of the cables are labeled as to which is the TLAN and which is the ELAN. The ports provide the connection point to the customer's ELAN and TLAN equipment. Shielded Category 5 cable must be used 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 55
NTMF94DA ELAN, TLAN & RS-232 Serial Maintenance I/O cable

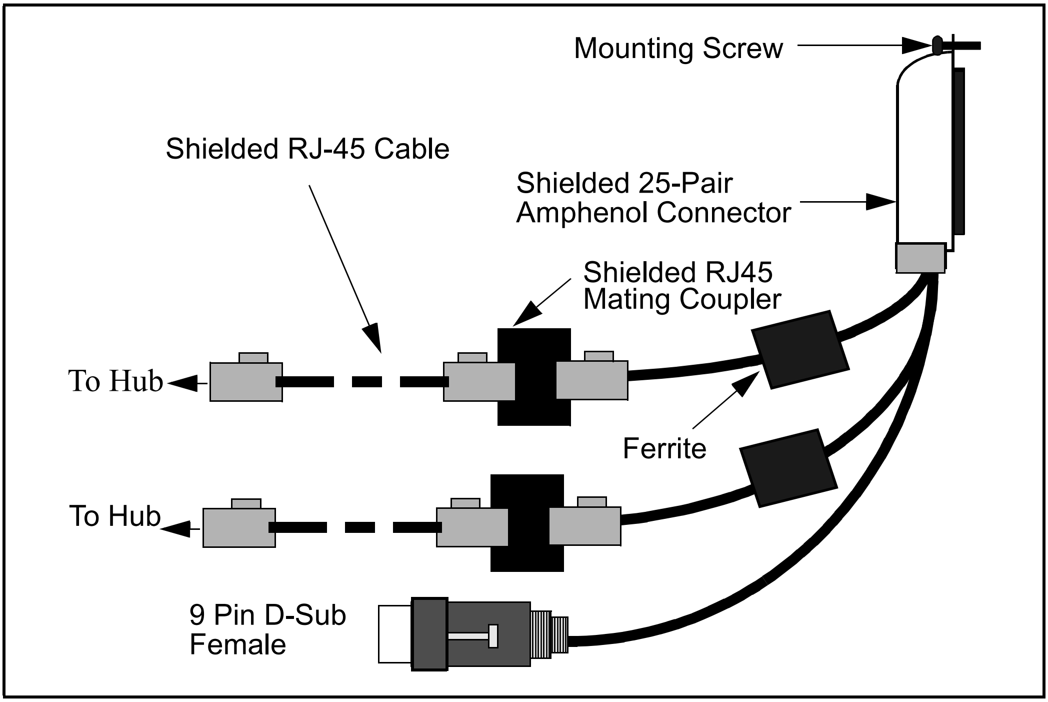


Table 19
NTMF94DA cable pin description

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	BDC dB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RX dB+	P4-3	GRN/WHT
P1-19	TX dB+	P4-1	ORG/WHT
P1-43	RX dB-	P4-6	WHT/GRN
P1-44	TX dB-	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 TLAN and ELAN. Shielded Category 5 RJ45 cable must be used to connect to the customer's TLAN/ELAN 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, the unshielded RJ45 coupler (provided) must be installed on the end of the NTMF94DA to prevent ground loops to external LAN equipment.

CAUTION
Service Interruption

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 results in incorrect and unpredictable ITG Wireless card operation

NTAG81CA maintenance cable description

Connect the NTAG81CA cable between the 9-pin D-type RS232 input on a standard PC and the MAINT connector on the NT8R17AB faceplate.Refer to Figure 56 and Table 20 for further information.

Figure 56
NTAG81CA Maintenance cable

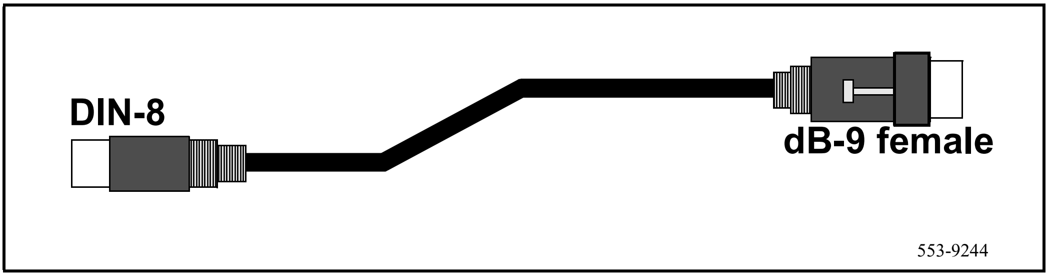


Table 20
NTAG81CA maintenance cable pin description

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

The 3m NTAG81BA cable connects the NTAG81CA cable to a PC or terminal. It has a 9-pin D-type connector at both ends, one male, one female. It can also be used to extend the serial port presented by the NTMF94DA I/O panel cable. Refer to Figure 57 and Table 21 for further information.

Figure 57
NTAG81BA Maintenance Extender cable

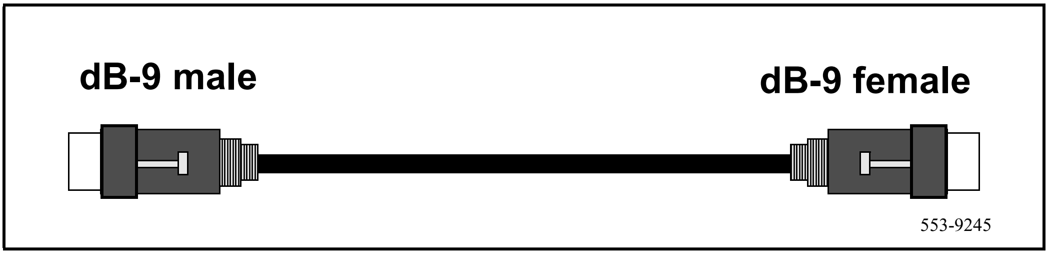


Table 21
NTAG81BA Maintenance cable pin description

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 C: Product integrity

Contents

This section contains information on the following topics:

Overview

This chapter describes the reliability, environmental, and Electro-Magnetic Containment (EMC) requirements of the of the Pentium ITG Wireless card used in the Wireless IP Gateway.

Reliability

Reliability is measured by the Mean Time Between Failures (MTBF).

Mean Time Between Failures

The ITG Wireless card Mean Time Between Failure (MTBF) is 46 years. Failures per 10^6 hours of operation are 2.483, based on 40 degrees C (140 degrees F).

EMC compliance

EMC compliance requirements depend on the regulations in effect for the country where the Meridian 1 and Succession Communication Server for Enterprise 1000 system is located. CISPR 22 Class B defines more stringent EMC limits than CISPR 22 Class A requirements (that is, equipment that meets CISPR 22 Class B exceeds CISPR 22 Class A requirements and can be used globally).

ITG Wireless card provisioning rules for EMC compliance

Meridian 1 Large Systems

The Pentium ITG Wireless card is approved for CISPR 22 Class A, and FCC Part 15 Class A limits, and approved to CISPR 22 CLass B limits.

Option 11C

For CISPR Class A compliance, no limits are imposed on the number of Pentium ITG Wireless cards that can be provisioned in each Option 11C cabinet.

For CISPR Class B compliance, provision a maximum of two Pentium ITG Wireless cards in each Option 11C cabinet.

Option 11C Mini or Succession CSE 1000

For CISPR Class A compliance and CISPRC Class B compliance, no limits are imposed on the number of ITG Wireless cards that can be provisioned.

Shielded Category 5 cable for external ITG Wireless card LAN connections

Only Shielded Cat 5 cable must be used to connect from the 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 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 I/O panel.

Refer to “Preventing ground loops on connection to external customer LAN equipment” on page 185 for information on how to conduct a test for ground loops.

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 22 for a display of acceptable temperature and humidity ranges for the ITG Wireless card.

Table 22
ITG environmental specifications (Sheet 1 of 2)

Specification	Minimum	Maximum
Normal Operation		
Recommended Relative humidity	15° C 20%	30° C 55% (non- condensing)
Absolute Relative humidity	10 ° C 20% to	45° C 80% (non-condensing)

Table 22
ITG environmental specifications (Sheet 2 of 2)

Specification	Minimum	Maximum
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 Wireless card, listed by geographic region. Specifications for the ITG Wireless card meet or exceed the standards listed in these regulations.

Safety

Table 23 provides a list of safety regulations met by the ITG Wireless card, along with the type of regulation and the country/region covered by each regulation.

Table 23
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 24 lists electro-magnetic emissions regulations met by the ITG Wireless card, along with the country's standard that lists each regulation.

Table 24
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 25 lists electro-magnetic immunity regulations met by the ITG Wireless card, along with the country's standard that lists each regulation.

Table 25
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 D: 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. A typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format can have a value from 0 to 255, where 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 26, 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 26, 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 26
CIDR format remainders

Remainder of CIDR format value divided by eight	Binary value	Dotted decimal value
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix E: DHCP Supplementary Information

Contents

This section contains information on the following topics:

Introduction to DHCP

In order to understand how the Wireless IP handset acquires the needed network configuration parameters automatically, the following section briefly describes the Dynamic Host Configuration Protocol (DHCP) protocol. It is recommended that readers, unfamiliar with the subject, read this section.

These topics are included to assist in configuration and maintenance of the DHCP server and to ensure correct implementation with the Wireless IP handset.

DHCP is an extension of BootP. Like BootP, it operates on the client-server model. Unlike BootP, DHCP has more message types. DHCP allows the dynamic allocation of IP addresses to different clients. It can be used to configure clients by supplying the network configuration parameters such as gateway or router IP addresses.

In addition, DHCP has a lease system that controls the duration an IP address is leased to a client. The client can request a specific lease length, or the administrator can determine the maximum lease length. A lease can range from one minute to 99 years. When the lease is up or released by the client the DHCP server automatically retrieves it and reassigns it to other clients if necessary. This is an efficient and accurate way to configure clients on the fly, saving the administrator from an otherwise repetitive task. In doing so, IP addresses can be shared among clients that do not require permanent IP addresses.

DHCP messages

There are seven different DHCP messages. Each message relates certain information between the client and server.

Table 27
DHCP message types

DHCP Message Types	Description
DHCPDISCOVER	Initiates a client request to all servers.
DHCPOFFER	Offer from server following client request.
DHCPREQUEST	Request a particular server for services.
DHCPAK	Notify client that requested parameters could be met.
DHCPNAK	Notify client that requested parameters could not be met.
DHCPDECLINE	Notify server that offer is unsatisfactory and is not accepted.
DHCPRELEASE	Notify server that IP address is no longer needed.

DHCP Message Format

The DHCP message format shown in Table 28 on page 213 is common to all DHCP messages. Each message is made of 15 fields, 14 fixed-length fields and one variable length field. The fixed-length fields must be the specified number of bytes as indicated in the brackets. If there is not enough data, or there is no data at all, zeros are used to fill in the extra spaces.

Table 28
DHCP message format

<table>
<tr><td>0</td><td colspan="12"></td><td>1</td><td colspan="6"></td><td>2</td><td colspan="9"></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Operation (1)</td><td colspan="8">Hardware type(1)</td><td colspan="8">Hardware Address Length (1)</td><td colspan="8">Hops (1)</td></tr>
<tr><td colspan="32">Transaction ID (4)</td></tr>
<tr><td colspan="16">Seconds (2)</td><td colspan="16">Flags (2)</td></tr>
<tr><td colspan="32">Client IP address (4)</td></tr>
<tr><td colspan="32">Your IP address (4)</td></tr>
<tr><td colspan="32">Server IP address (4)</td></tr>
<tr><td colspan="32">Gateway IP address (16)</td></tr>
<tr><td colspan="32">Client hardware address (16)</td></tr>
<tr><td colspan="32">Server name (64)</td></tr>
<tr><td colspan="32">File name (129)</td></tr>
<tr><td colspan="32">Options (312)</td></tr>
</table>

The Options field is the only field with a variable length. It is optional, but very important as it transports additional network configuration parameters. The DHCP options are the actual sub-fields that are used in this project.

DHCP Message exchange

For a client to receive services from a DHCP server, an exchange of DHCP messages between the client and server must take place. The sequence and types of DHCP message exchanged can differ, but the mechanism of acquiring and supplying information remains the same.

Usually the client initiates the exchange with a DHCP message broadcast. Using a broadcast allows the client to send messages to all the servers on the network without having an associated IP address. The broadcast is local to the LAN unless a DHCP relay agent is present to forward the packet.

At this point, the client has no information about the server or the IP address it is going to receive (unless it is requesting a renewal), so the fields in the DHCP message are empty. However, the client knows its own MAC address and includes it in the Client hardware address field. The client may also have a list of parameters it would like to acquire and can request them from the DHCP server by including the Parameter Request List option (Option Code 55) in the DHCPDISCOVER message.

When the DHCP server sees the broadcast, it responds by broadcasting its own DHCP message. The server, since it knows more about the network, is able to fill in most of the information in the message. For example, information such as server IP address and gateway IP address are included in their respective fields. Since the client does not have an IP address yet, the server uses the client's MAC address to uniquely identify it. When the client sees the broadcast, it matches its MAC address against the one in the message.

Using this method, the server and client can supply or receive information through the exchange of their DHCP messages.

DHCP Options

DHCP Options are the sub fields of the Options field. They carry additional network configuration information requested by the client such as IP address lease length and subnet mask.

Each DHCP option has an associated option code and a format for carrying data. Usually the format is as follows:

Option code Length Data

There are two categories of DHCP options, standard and non-standard. The standard options are predefined by the industry while non-standard options are user-defined to fit the needs of a particular vendor or site.

There are a total of 255 DHCP option codes where option codes 0 and 255 are reserved, 1-77 are predefined, 78-127 can be used for Vendor Specific options and 128-254 are designated for Site Specific options. This arrangement allows for future expansion and is to be used as a guideline for choosing option codes.

IP Acquisition Sequence

This section discusses the mechanics and sequence of the DHCP message exchange as the Wireless IP handset uses DHCP for IP acquisition. Although the Wireless IP handset requests many network configuration parameters as well as an IP address, the following cases focus on the concept of "how" instead of "what" information is acquired. Also, the Wireless IP handset is used as the sample client but most of the illustrations apply to other DHCP clients as well.

Case 1

Case 1 is a typical situation where the Wireless IP handset requests services from a DHCP server. This is illustrated in Figure 41 and explained below.

1 The Wireless IP handset initiates the sequence by broadcasting a DHCPDISCOVER message.

2 A DHCP server on the network sees the broadcast, reads the message, and records the MAC address of the client.

3 It checks its own IP address pool(s) for an available IP address and broadcasts a DHCPOFFER message if one is available. (Usually the server ARPs or PINGs the IP address to make sure it is not being used.)

4 The Wireless IP handset sees the broadcast and after matching its MAC address with the offer, reads the rest of the message to find out what else is being offered.

5 If the offer is acceptable, it sends out a DHCPREQUEST message with the DHCP server's IP address in the Server IP address field.

6 The DCHP server matches the IP address in the Server IP address field against its own to find out who the packet belongs to.

7 If the IPs match and there is no problem supplying the requested information, it assigns the IP address to the client by sending a DHCPACK.

8 If the final offer is not rejected, the IP acquisition sequence is complete.

Case 2

The IP acquisition becomes unsuccessful if either the server or the client decides not to participate. If the DHCP server cannot supply the requested information:

1 It sends a DHCPNAK message and no IP address is assigned to the client. This can happen if the requested IP address has already been assigned to a different client (see Figure 42 on page 265). If the Client decides to reject the final offer (after the server sends a DHCPACK message):

2 the Client sends a DHCPDECLINE message to the server, telling it the offer is rejected.

3 the Client must restart the IP acquisition by sending another DHCPDISCOVER message, in search of another offer.

Case 3

Finally, when a client is finished with a particular IP address, it sends a DHCPRELEASE message to the server which reclaims the IP address. If the client requires the same IP address again, it can initiate the process as follows:

1 Wireless IP handset broadcasts a DHCPREQUEST to a particular DHCP server by including the server's IP address in the Server IP Address field of the message. Since it knows which IP address it wants, it requests it in the DHCP message.

2 The DHCP server sends a DHCPACK message if all the parameters requested are met.

Case 1 is similar to Case 3, except the first two messages have been eliminated. This reduces the amount of traffic produced on the network (see Figure 43).

Multiple DHCPOFFERS

In some networks, if more than one DHCP server is present, a client can receive multiple DHCPOFFER messages. Under these situations, the IP acquisition sequence depends on the client. The client can wait for multiple offers, or just go with the first offer it receives. If it accepts multiple offers, it compares them before choosing one with the most fitting configuration parameters. When a decision is made, the message exchange is the same as if there is only one DHCP server and proceeds as in the previous Cases. The servers that have not been chosen to provide the service do not participate in the exchange.

With multiple DHCP servers on the same network, a problem can occur if any two of the servers have overlapping IP address range and no redundancy. DHCP redundancy is a property of DHCP servers, which allows different DHCP servers to serve the same IP address ranges simultaneously. Administrators must be aware that not all DHCP servers have this capability.

Appendix F: ITG Wireless commands

Contents

This section contains information on the following tables:

Table 29
ITG Wireless card shell commands (Sheet 1 of 4)

Command	Description
General-Purpose Commands:	
shellPasswordSet	Change the default ITG shell password.
itgCardShow	Show card info.
itgChanStateShow	Show state of channels. e.g. busy or idle.
itgHelp	Shows the complete command list. “?” also shows the list.

Table 29
ITG Wireless card shell commands (Sheet 2 of 4)

Command	Description
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.
firmwareVersionShow	Prints out firmware version number.
numChannelsShow	Prints out number of available channels.
swVersionShow	Prints out software version.
resetOM	Resets the operational measurement file timer.
logFileOn	Turns on logging.
logFileOff	Turns off logging.
logStatus	Shows whether logging is on or off.
emodelSim	Allows user to interactively determine QoS score.
File Transfer Commands:	
swDownload	Loads new version of s/w from OTM PC to ITG Wireless card.
configFileGet	Sends an updated config.ini file from OTM 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 OTM to the ITG Wireless card.
bootpFileGet	Sends an updated bootptab file from the OTM PC to the ITG Wireless card.
GKTableGet	Sends an updated gatekeeper information file from OTM PC to the ITG Wireless card.
hostFileGet	Transfers any file from the OTM PC to the ITG Wireless card.
currOmFilePut	Sends the current OM file from ITG to OTM.

Table 29
ITG Wireless card shell commands (Sheet 3 of 4)

Command	Description
prevOmFilePut	Sends the previous OM file from ITG to OTM.
traceFilePut	Sends the trace file from ITG to OTM.
currLogFilePut	Sends the current log file from ITG to OTM.
prevLogFilePut	Sends the previous log file from ITG to OTM.
currGKOmFilePut	Sends the current gatekeeper OM file from the ITG Wireless card to the OTM PC.
prevGKOmFilePut	Sends the previous gatekeeper OM file from the ITG Wireless card to the OTM PC.
currGKLogFilePut	Sends the current gatekeeper log file from the ITG Wireless card to the OTM PC.
prevGKLogFilePut	Sends the previous gatekeeper log file from the ITG Wireless card to the OTM PC.
GKTablePut	Sends the gatekeeper information file from the ITG Wireless card to the OTM PC. This contains the TimeToLive values for the client and gateway, and the alias-password table.
hostFilePut	Transfers any file from the ITG Wireless card to the OTM PC.
GKEndptInfoPut	Transfers endpoint information from the ITG Wireless card to the OTM PC.
GKCallInfoPut	Transfers call information from the ITG Wireless card to the OTM PC.
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.
NVRIPShow	Prints the values of the IP parameters that reside in NVRAM.
nvramLeaderSet	Sets the leader bit in NVRAM.

Table 29
ITG Wireless card shell commands (Sheet 4 of 4)

Command	Description
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 ITG Wireless card.
DSP Commands:	
DSPReset	Resets the specified DSP
DSPNumShow	Prints number of DSPs on ITG Wireless card.
Gatekeeper Query Commands:	
GKGenInfoShow	Prints all registered Gateways with lists of DNs.

Table 30
General-Purpose Commands (Sheet 1 of 3)

Synopsis: Description:	**itgCardShow** Show card info.
Synopsis: Description:	**ldrResTableShow** Show backup leader and followers for a given leader.
Synopsis: Description:	**itgChanStateShow** Show state of channels. e.g. busy or idle.

Table 30
General-Purpose Commands (Sheet 2 of 3)

Synopsis:	**itgMemShow**
Description:	Show memory usage
Synopsis:	**ifShow**
Description:	Show detailed IP information, including MAC addresses.
Synopsis:	**IPinfoShow**
Description:	This command returns 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 ITG Wireless card commands and a short description.
Synopsis:	**shellPasswordSet**
Description:	Change the default ITG shell password.
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**

Table 30
General-Purpose Commands (Sheet 3 of 3)

Description:	Turns on logging.
Synopsis: Description:	**logFileOff** Turns off logging.
Synopsis: Description:	**logStatus** Shows whether logging is on or off.
Synopsis: Description:	**emodelSim** Allows user to interactively determine QoS score.

Table 31
File transfer commands (Sheet 1 of 5)

Synopsis:	**swDownload** hostname, username, password, directory path, filename
Description:	Updates the software on the ITG Wireless card with the binary file received from an FTP server corresponding to the *hostname* IP address. The ITG Wireless card ftp client performs a get which downloads the file to the ITG flash bank. A checksum is calculated to verify correct delivery. Once the new software version is successfully downloaded, the ITG Wireless card must be rebooted with cardReset in order to run the new software. *Hostname* refers to the either IP address of the FTP host, or the ITG Wireless card itself or another ITG Wireless card when a PC card in the A: drive of the ITG Wireless card contains the software binary file.
Example:	ITG> swDownload “47.82.32.246”, “anonymous”,”guest”, “/software”,”vxWorks.mms”

Table 31
File transfer commands (Sheet 2 of 5)

Synopsis: Description: Example:	**configFileGet** hostname, username, password, directory path, filename Updates the config.ini file on the ITG Wireless 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. ITG> ConfigFileGet “ngals042”, “anonymous”,”guest”, “/ configDir”,”config.ini”
Synopsis: Description: Example:	**bootPFileGet** hostname, username, password, directory path, filename Updates the bootptab file on the ITG Wireless 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. ITG> bootpFileGet “47.82.xx.xxx”,“anonymous”,”guest”,“/ bootpDir”,”bootptab”
Synopsis: Description: Example:	**GKTableGet** hostname, username, password, directory path, filename Updates the gk_gen_info file on the ITG Wireless card with the gk_gen_info file on the specified host, account and path. The GKTableGet task on the ITG Wireless card initiates an FTP session with the given parameters and downloads the file to the flash file system. ITG> GKTableGet “47.82.xx.xxx”,“anonymous”,”guest”,“/gatekeeper”, ”gk_gen_info”
Synopsis: Description: Example:	**hostFileGet** hostname, username, password, directory path, filename, ITGFileName, listener Gets any file from the host and does a get via FTP to the ITG Wireless card. ***Note:*** 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. ITG> hostFileGet “47.82.xx.xxx”, “anonymous”,”guest”, “/ hostfileDir”,”hostFile.txt”, “/C:ITGFILEDIR/ITGFILE.TXT”, -1

Table 31
File transfer commands (Sheet 3 of 5)

Synopsis:	**currOmFilePut** hostname, username, password, directory path, filename
Description:	The omFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the ITG Wireless 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 ITG Wireless 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 ITG Wireless card’s call trace file to the specified location on the host.
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 ITG Wireless 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 ITG Wireless card’s logfile the to specified location on the host.
Example:	ITG> prevLogFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/currDir”, ”logFile”

Table 31
File transfer commands (Sheet 4 of 5)

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 ITG Wireless 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 ITG Wireless 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 ITG Wireless card’s gatekeeper call trace file to specified location on the host.
Example:	ITG> GKtraceFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/trcDir”,”trcFile”
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 ITG Wireless card’s gatekeeper log file to specified location on the host.
Example:	ITG> currGKLogFilePut “47.82.xx.xxx”,“anonymous”,”guest”,“/currDir”,”GKlogFile”

Table 31
File transfer commands (Sheet 5 of 5)

Synopsis: Description: Example:	**prevGKLogFilePut** hostname, username, password, directory path, filename The logFilePut task on the ITG active leader/backup leader card initiates an FTP session with the given parameters and uploads the ITG Wireless card's previous gatekeeper log file to specified location on the host. ITG> prevGKLogFilePut "47.82.xx.xxx","anonymous","guest","/prevDir", "GKlogFile"
Synopsis: Description: Example:	**hostFilePut** hostname, username, password, directory path, filename, ITGFileName Transfers any file on the ITG Wireless card from location ITGFileName and does a put via FTP to the host specified by hostname, username, password and directory path. Note: ITGFileName is the full path, i.e. path/filename, of where the file is taken from on the ITG Wireless card. ITG> hostFilePut "ngals042", "anonymous","guest", "/hostDir","hostFile", "/C:/CONFIG/CONFIG1.INI"

Table 32
IP Configuration Commands (Sheet 1 of 2)

Synopsis: Description: Example:	**NVRIPSet "IP address"** Sets the IP address in NVRAM. **ITG> NVRRIPSet "47.23.34.19"**
Synopsis: Description: Example:	**NVRGWSet** "IP gateway" Sets the default gateway address in NVRAM. **ITG> NVRRGWSet "47.0.0.1"**
Synopsis: Description: Example:	**NVRSMSet"subnet mask"** Sets the subnet mask in NVRAM. **ITG> NVRRSMSet "255.255.240.0"**

Table 32
IP Configuration Commands (Sheet 2 of 2)

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**
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 33
Card Commands

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

Table 34
DSP Commands

Synopsis: Description: Example:	**DSPReset *DSPNumber*** Resets the specified DSP **ITG>DSPReset 0**
Synopsis: Description: Example:	**DSPNumShow *DSPNumber*** Prints number of DSPs on ITG Wireless card. **ITG>DSPNumShow 0**

Table 35
Gatekeeper Query Commands

Synopsis: Description:	**GKGenInfoShow** Prints the information for all registered ITG Wireless 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)

Table 36
Operational Measurement Queries

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

Table 37
Log File Commands

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

Index

Meridian 1 and Succession Communication Server for Enterprise 1000

802.11 Wireless IP Gateway

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.

Publication number: 553-3001-206
Document release: Standard 2.00
Date: April 2002

NORTEL NETWORKS™