Meridian 1
Succession 1000
Succession 1000M
Succession 3.0 Software

What's New for Succession 3.0

Document Number: 553-3001-015
Document Release: Standard 1.00
Date: October 2003

Produced in Canada

Revision history

October 2003

Standard 1.00. This document is up-issued to support Succession 3.0 Software. This document contains important information about upgrading to Succession 3.0, as well as descriptions of new features and enhancements.

Contents

About this document

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

Subject

This document describes features and enhancements implemented for Succession 3.0.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Succession 3.0 Software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel Networks home page:

http://www.nortelnetworks.com/

Applicable systems

This document applies to the following systems:

- Meridian 1 Option 11C Chassis
- Meridian 1 Option 11C Cabinet
- Meridian 1 Option 51C
- Meridian 1 Option 61
- Meridian 1 Option 61C
- Meridian 1 Option 61C CP PII

- Meridian 1 Option 81
- Meridian 1 Option 81C
- Meridian 1 Option 81C CP PII
- Succession 1000
- Succession 1000M Chassis
- Succession 1000M Cabinet
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

Note that memory upgrades may be required to run Succession 3.0 Software on CP3 or CP4 systems (Options 51C, 61, 61C, 81, 81C).

System migration

When particular Meridian 1 systems are upgraded to run Succession 3.0 Software and configured to include a Succession Signaling Server, they become Succession 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a Succession 1000M system.

Table 1
Meridian 1 systems to Succession 1000M systems (Part 1 of 2)

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 11C Chassis	Succession 1000M Chassis
Meridian 1 Option 11C Cabinet	Succession 1000M Cabinet
Meridian 1 Option 51C	Succession 1000M Half Group
Meridian 1 Option 61	Succession 1000M Single Group
Meridian 1 Option 61C	Succession 1000M Single Group
Meridian 1 Option 61C CP PII	Succession 1000M Single Group
Meridian 1 Option 81	Succession 1000M Multi Group

Table 1
Meridian 1 systems to Succession 1000M systems (Part 2 of 2)

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 81C	Succession 1000M Multi Group
Meridian 1 Option 81C CP PII	Succession 1000M Multi Group

Note the following:

- When an Option 11C Mini system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Chassis.
- When an Option 11C system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Cabinet.

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

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)
- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

Intended audience

This document is intended for individuals responsible for the planning, engineering, and administration of Meridian 1, Succession 1000, and Succession 1000M systems.

Conventions

Terminology

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

- Meridian 1
- Succession 1000
- Succession 1000M

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

- Succession 1000M Chassis
- Succession 1000M Cabinet
- Meridian 1 Option 11C Chassis
- Meridian 1 Option 11C Cabinet

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

- Meridian 1 Option 51C
- Meridian 1 Option 61
- Meridian 1 Option 61C
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81
- Meridian 1 Option 81C
- Meridian 1 Option 81C CP PII
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

The call processor in Succession 1000 and Succession 1000M systems is referred to as the “Succession Call Server”.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Product Compatibility* (553-3001-156)
- *Data Networking for Voice over IP* (553-3001-160)

- *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180)
- *Dialing Plans: Description* (553-3001-183)
- *Circuit Card: Description and Installation* (553-3001-211)
- *IP Peer Networking* (553-3001-213)
- *Branch Office* (553-3001-214)
- *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232)
- *System Management* (553-3001-300)
- *Features and Services* (553-3001-306)
- *Software Input/Output: Administration* (553-3001-311)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *Succession 1000 Element Manager: System Administration* (553-3001-332)
- *Automatic Call Distribution: Description* (553-3001-351)
- *IP Trunk: Description, Installation, and Operation* (553-3001-363)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Telephones and Consoles: Description* (553-3001-367)
- *Internet Terminals: Description* (553-3001-368)
- *ISDN Primary Rate Interface: Features* (553-3001-369)
- *Basic Network Features* (553-3001-379)
- *ISDN Basic Rate Interface: Features* (553-3001-380)
- *Software Input/Output: System Messages* (553-3001-411)
- *Software Input/Output: Maintenance* (553-3001-511)
- *ISDN Primary Rate Interface: Maintenance* (553-3001-517)
- *Large System: Upgrade Procedures* (553-3021-258)
- *Large System: Maintenance* (553-3021-500)
- *Succession 1000 System: Overview* (553-3031-010)

- *Succession 1000 System: Planning and Engineering* (553-3031-120)
- *Succession 1000 System: Installation and Configuration* (553-3031-210)
- *Succession 1000 System: Upgrade Procedures* (553-3031-258)
- *i2002 Internet Telephone User Guide*
- *i2004 Internet Telephone User Guide*
- *i2050 Software Phone User Guide*

Online

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

http://www.nortelnetworks.com/

CD-ROM

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

Upgrading to Succession 3.0 Software overview

Contents

This section contains information on the following topics:

Introduction

The focus of the Succession 3.0 Software upgrade procedures is upgrading Meridian 1 Internet-enabled systems. (See “Terminology” on page 23 for an explanation of “Internet-enabled”.) The scenarios and procedures described in this chapter do not apply for upgrades to Meridian 1 systems that are not Internet-enabled to any degree.

In general, there are three types of upgrade that can be performed on Meridian 1 Internet-enabled systems:

1 Software and system

2 Software only

3 System only

Table 2 shows how the types of upgrade relate to current and desired configurations.

Table 2
Types of upgrade of Meridian 1 Internet-enabled systems

	Upgrade from this configuration...		To this configuration	
Type	**System**	**Software**	**System**	**Software**
Software and system	Meridian 1	X11 25.40 or earlier	Succession 1000M	Succession 3.0
Software only	Meridian 1	X11 25.40 or earlier	no change	Succession 3.0
System only	Meridian 1	Succession 3.0	Succession 1000M	no change

Note 1: Within the upgrade scenarios, some procedures apply to Meridian 1 systems with IP Line, others to IP Trunk.

Note 2: To complete a system-only upgrade, you must first complete a software-only upgrade.

Note 3: Meridian 1 systems without IP Line or IP Trunk should be treated as software-only upgrades. In these cases, a subsequent system-only upgrade should be treated as a new installation of IP Line and IP Peer Networking.

There are many scenarios for each type of upgrade. This chapter first presents important information on terminology and specifications, and then proceeds to describe and compare the scenarios in terms of overall approach. The detailed procedures for each scenario are presented in the appropriate Upgrade Procedures NTPs:

- *Small System: Upgrade Procedures* (553-3011-258)

- *Large System: Upgrade Procedures* (553-3021-258)
- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

IMPORTANT!

- The scenarios contain many of the same procedures, but the sequence is different. It is very important to follow the order of the steps provided in the respective scenarios.
- The decision about which type of upgrade to perform and which scenario to follow depends on a number of considerations. Make sure that you read this entire chapter and fully understand it before you decide on an upgrade scenario.

Terminology

The following terms are used in this document:

- **Internet-enabled**. Refers to a Meridian 1 system that is equipped with:
  - IP Line only
  - IP Trunk only
  - both IP Line and IP Trunk

  Note: The system is not equipped with a Succession Signaling Server.

- **System upgrade**. Refers to upgrading a Meridian 1 Internet-enabled system to Succession 3.0 Software with a Succession Signaling Server.
- **Software upgrade**. Refers to any of the following:
  - upgrading any Meridian 1 system to Succession 3.0 Software
  - upgrading the ITG Trunk 2.xx application software (also known as loadware) to IP Trunk 3.01
  - upgrading the IP Line 2.20 or 3.00 software (also known as loadware) to IP Line 3.10

- **Network upgrade**. Refers to upgrading systems and software across a private IP Telephony network in a coordinated way to minimize cost, service interruption, or both. In general, this must be done gradually, system by system.
- **Migration**. Refers to migrating IP Trunk 3.0 nodes from a node-based dialing plan that is managed through Optivity Telephony Manager (OTM) to a Gatekeeper-resolved Network Numbering Plan that is centrally managed through Element Manager. Migration denotes a gradual, low-risk, system-by-system reconfiguration and testing of the UDP and CDP dialing plans, Network Numbering Plan, and network routing.
- **Cutover**. Refers to reconfiguring and cutting over an upgraded Succession 1000M system from using IP Trunks to using IP Peer Virtual Trunks. If a large IP Trunk 3.0 network has been completely migrated to using the Gatekeeper-resolved Network Numbering Plan, then cutover to using IP Peer Virtual Trunks can proceed gradually, system by system, with low risk of service interruption.
- **Coordinated cutover**. For small networks (for example, 2 to 4 systems) it may be practical to coordinate the simultaneous cutover of all systems from using IP Trunks with node-based dialing plans to using the IP Peer Virtual Trunks and Gatekeeper-resolved Network Numbering Plan *in the same maintenance window*. In this case the IP Trunk migration procedures are eliminated.
- **Conversion**. Refers to converting unused IP Trunk cards to Voice Gateway Media Cards.
- **IP Line**. Refers to a software application that allows an Internet Telephone to be connected to a Meridian 1, Succession 1000, or Succession 1000M. It also provides echo cancellation, and compresses and packetizes voice for transmission over an IP data network. The IP Line application runs on the Meridian 1 and Succession Call Server, Succession Signaling Server, and Voice Gateway Media Cards. On the Voice Gateway Media Card, it provides two independent services:
  - UNIStim Line Terminal Proxy Server (LTPS) at system level
  - Voice Gateway (VGW) media ports at customer level

- **IP Trunk**. Refers to the ISDN-Signaling IP Trunk 3.01 application that enables calls in a private telephony network to travel over the converged enterprise IP network. The IP Trunk application runs on Succession Media Cards or ITG-Pentium (ITG-P) cards that are grouped in IP Trunk nodes hosted by Meridian 1 Internet-enabled or upgraded Succession 1000M systems.

  The IP Trunks appear to the Succession Call Server as ISDN Signaling Link (ISL) trunks. MCDN features are supported over IP Trunks, but the Call Servers do not process the H.323 network signaling protocol directly and do not interact with the control signaling for the IP telephony media path. IP Trunk cards have dedicated media ports that are used for all calls.

- **IP Peer Virtual Trunk**. Refers to a software application that supports virtual IP trunks. On Succession 1000M and Succession 1000 systems, IP Peer Virtual Trunk software runs on the Succession Call Server and Signaling Server.

  The IP Peer Virtual Trunks appear to the Call Server as an H.323 protocol trunk route. The Succession Call Server supports MCDN features and the H.323 protocol over IP Peer Virtual Trunks, including control signaling for the IP telephony media path. This enables end-to-end direct media path connections between Internet Telephones and Voice Gateway media ports over IP Peer Virtual Trunks.

  IP Peer Virtual Trunks are called "virtual" because Voice Gateway (VGW) media ports, located on Voice Gateway Media Cards, are allocated to IP Peer Virtual Trunks per call as needed. VGW media ports are customer-level resources that are shared by IP Lines and IP Peer Virtual Trunks.

Hardware and software specifications

Table 3 lists the software components required to upgrade to Succession 3.0 Software.

Note: The information in Table 3 was valid as of date of publication. However, before you begin the upgrade, check the latest General Release Bulletin, Product Bulletins, and the Nortel Networks Software Download website to confirm that you have the latest versions. In particular, if your upgrade package was shipped some weeks before you begin to perform the upgrade, check the Nortel Networks Software Download website, in case there has been a maintenance up-issue in the interim.

Table 3
Succession 3.0 Software (Part 1 of 2)

Item	Version
Succession Call Server	X21 Release 3.00V
Succession Signaling Server (see note below)	SSE 2.10.80
IP Line application (see note below)	IPL 3.10.80
IP Trunk application	IPT 3.01
Optivity Telephony Manager	OTM 2.10
Voice Gateway Media Card firmware (8051XA Controller)	6.7 for Succession Media Card 5.7 for ITG-P card
i2002 Internet Telephone firmware (see note below)	1.59

Table 3
Succession 3.0 Software (Part 2 of 2)

Item	Version
i2004 Internet Telephone firmware (see note below)	1.59
i2050 Software Telephone	v338
Web browser	Microsoft Internet Explorer v.6.0.2600 or later Other web browsers (such as Netscape Navigator) are *not supported*.
Note: The Succession Signaling Server IP Line Terminal Proxy Server (LTPS), Gatekeeper, H.323 Gateway, Element Manager, IP Line loadware, and Internet Telephone firmware are contained on the Succession Signaling Server CD-ROM.	

Stand-alone Gatekeepers

You can install stand-alone Succession 1000 Gatekeepers for Network Numbering Plan resolution to simplify network management for IP Trunk 3.00 and BCM 3.01 networking in large, complex networks.

Prior to upgrading any Meridian 1 Internet-enabled system to Succession 3.0 Software with IP Peer Networking, you can order duplicate sets of the NTDU27CB Succession Signaling Server hardware/software package and power cord, in order to install a Primary and an Alternate stand-alone Gatekeeper for centralized management of the Network Numbering Plan for the IP Trunk 3.00 and BCM 3.01 network.

Collocated stand-alone Gatekeepers can be configured later as Succession Signaling Servers when the systems are upgraded to Succession 3.0 Software, with co-resident Gatekeeper, IP Peer Virtual Trunks, and LTPS for IP Line 3.10.

Trunk Route Optimization and Trunk Anti-Tromboning

Prior to Succession 3.0 Software, network call modification and redirection (such as call transfer and call forwarding) causes tandem IP Trunk 3.01 connections that degrade voice quality. Succession 3.0 Software introduces important improvements to Trunk Route Optimization (TRO) and Trunk

Anti-Tromboning (TAT), which you should implement to avoid tandem IP Trunk connections.

IP Trunk 3.01 introduces an important improvement to Trunk Anti-Tromboning (TAT), which complements the operation of TRO to further reduce voice quality degradation due to tandem IP Trunk 3.01 connections.

Surplus equipment

The D-Channel PC Card from the IP Trunk node and its cabling is not required after IP Trunk cards have been converted to Voice Gateway Media cards. This may be kept as a spare for nodes still running IP Trunk or ITG Trunk applications.

The D-Channel port is no longer used.

Technical support

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Table 4
Customer Technical Services (CTS) (Part 1 of 2)

Location	Contact
Nortel Networks Global Networks Technical Support (GNTS) PO Box 833858 2370 Performance Drive Richardson, TX 75083 USA	North America Telephone: 1 800 4NORTEL
Nortel Networks Corp. (CTS North America) P.O. Box 4000 250 Sydney Street Belleville, Ontario K8N 5B7 Canada	North America Telephone: 1 800 4NORTEL
Nortel Service Center - EMEA	EMEA Telephone: 00 800 8008 9009 or +44 (0)870 907 9009 E-mail: emeahelp@nortelnetworks.com
Nortel Networks 1500 Concord Terrace Sunrise, Florida 33323 USA	**Brazil** Telephone: 5519 3705 7600 E-mail: entcts@nortelnetworks.com **English Caribbean** Telephone: 1 800 4NORTEL **Spanish Caribbean** Telephone: 1 954 858 7777 **Latin America** Telephone: 5255 5480 2170

Table 4
Customer Technical Services (CTS) (Part 2 of 2)

Location	Contact
Network Technical Support (NTS)	**Asia Pacific** Telephone: +61 28 870 8800 **Australia** Telephone:1800NORTEL (1800 667835) or +61 2 8870 8800 E-mail: asia_support@nortelnetworks.com **People's Republic of China** Telephone: 800 810 5000 E-mail: chinatsc@nortelnetworks.com **Japan** Telephone: 010 6510 7770 E-mail: supportj@nortelnetworks.com **Hong Kong** Telephone: 800 96 4199 E-mail: chinatsc@nortelnetworks.com **Taiwan** Telephone: 0800 810 500 E-mail: chinatsc@nortelnetworks.com **Indonesia** Telephone: 0018 036 1004 **Malaysia** Telephone: 1 800 805 380 **New Zealand** Telephone: 0 800 449 716 **Philippines** Telephone: 1 800 1611 0063 or 632 917 4420 **Singapore** Telephone: 800 616 2004 **South Korea** Telephone: 0079 8611 2001 **Thailand**: Telephone: 001 800 611 3007

Choosing an upgrade scenario

The decision as to which scenario to follow will depend on your system and circumstances. The primary difference between the scenarios is whether and when:

- you migrate the IP Trunk nodes to a Gatekeeper-resolved Network Numbering Plan
- you cut over the upgraded system from using IP Trunks to IP Peer Virtual Trunks

After considering the information provided in "Migration and cutover options" on page 31 and "Additional considerations" on page 34, choose the upgrade scenario that best suits your organization.

The scenarios presented in these two chapters are not exhaustive. They are intended to cover the most common situations and the most likely desired configurations. After studying the scenarios, you may decide to contact Nortel Networks for assistance with the upgrade, migration, and conversion procedures. See "Technical support" on page 28.

Migration and cutover options

There are three ways to approach migrating the IP Trunks and cutting over to IP Peer Virtual Trunks:

- pre-upgrade migration followed by gradual cutover
- post-upgrade migration followed by gradual cutover
- coordinated cutover without migration

Table 5 describes the three methods and explains the differences between them.

Table 5
Comparison of upgrade, migration, and cutover methods (Part 1 of 2)

Pre-upgrade migration	Post-upgrade migration	Coordinated cutover
You can migrate a large Meridian 1 Internet-enabled IP Trunk 3.01 network to use Succession Signaling Servers configured as stand-alone Gatekeepers in order to take advantage of a simplified, centrally managed Network Numbering Plan in advance of the first Meridian 1 Internet-enabled system upgrade to Succession 1000M.	You can begin to upgrade Meridian 1 Internet-enabled systems one by one to Succession 1000M in a large IP Trunk 3.0 network that is still using the IP Trunk node-based dialing plans. ***Note:*** Upgraded systems must continue to use the IP Trunks until you have migrated the IP Trunk 3.01 network to use co-resident or stand-alone Gatekeepers.	For a small network of Meridian 1 Internet-enabled systems with IP Trunk (for example, 2–4 systems), and with sufficient planning, technician resources, and length of maintenance window for IP Trunk service interruption, you may choose to skip the procedures to migrate the IP Trunk network. (You will still need to transfer or duplicate the IP Trunk node-based dialing plans to the Gatekeeper-resolved Network Numbering Plan, but you don't migrate the IP Trunks to actually use that numbering plan.)

Table 5
Comparison of upgrade, migration, and cutover methods (Part 2 of 2)

Pre-upgrade migration	Post-upgrade migration	Coordinated cutover
After the IP Trunk 3.01 network migration is complete, you can upgrade the Meridian 1 Internet-enabled systems one by one to Succession 1000M and immediately reconfigure and cut over each upgraded system to use the IP Peer Virtual Trunks and Gatekeeper-resolved Network Numbering Plan. The Succession Signaling Servers configured as stand-alone Gatekeepers can be reconfigured as co-resident Gatekeepers for upgraded Succession 1000M systems.	After you have upgraded the first two Meridian 1 Internet-enabled systems to Succession 1000M with Primary and Alternate Gatekeepers, you can start to migrate a large IP Trunk 3.01 network to use the Succession Signaling Server Gatekeepers to resolve the Network Numbering Plan. However, *only after the IP Trunk 3.01 network migration is complete* can you begin to reconfigure and cut over the systems one by one to use the IP Peer Virtual Trunks.	Upgrade the Meridian 1 Internet-enabled systems one by one to Succession 1000M. Continue to use IP Trunks with node-based dialing plans. Configure Primary and Alternate Gatekeepers with IP Peer Gateway endpoints and Network Numbering Plan. Verify registration of all IP Peer Trunk Gateways with the Gatekeeper. Finally, in a single maintenance window, simultaneously reconfigure and cut over all the upgraded Succession 1000M systems to use the IP Peer Virtual Trunks and Gatekeeper-resolved Network Numbering Plan. Thoroughly test the UDP and CDP dialing plans and Gatekeeper-resolved Network Numbering Plan.
You can immediately convert the unused IP Trunk cards in the upgraded systems to Voice Gateway Media Cards.	You must wait to convert the unused IP Trunk cards to Voice Gateway Media Cards until you have completed the IP Trunk 3.01 network migration and reconfigured the upgraded system to use the IP Peer Virtual Trunks.	You can immediately convert the unused IP Trunk cards in the upgraded systems to Voice Gateway Media Cards.

Additional considerations

A critical consideration is whether the IP Trunk nodes use local node-based dialing plans or whether the entire IP Trunk network was initially configured, or has been migrated, to use a Succession Signaling Server Gatekeeper to resolve the Network Numbering Plan into Call Signaling IP addresses for the H.323 endpoints, including IP Trunk and BCM.

When planning upgrades to Succession 1000M for an existing network of Meridian 1 Internet-enabled systems that are networked using IP Trunk (i.e., ISDN-signaling IP trunks), you must consider:

- the size of the network
- the complexity of the dialing plan
- the complexity of the Network Numbering Plan
- the complexity of the public and private trunk routing
- IP Trunk interoperation with BCM systems in the network

You must also consider:

- schedule and budget
- tolerance for temporary service interruption of the IP Trunk network
- the logistics and availability of technicians to simultaneously reconfigure and cut over multiple upgraded systems to use a Gatekeeper-resolved Network Numbering Plan

If it is not practical to reconfigure and cut over all the upgraded systems simultaneously to use IP Peer Virtual Trunks, choose either a pre- or post-upgrade migration scenario. Separating the migration, upgrade, and cutover elements of the process allows you to adopt a phased approach that maintains uninterrupted service of the IP Trunk network while the Meridian 1 Internet-enabled systems are gradually upgraded to Succession 1000M systems.

For a smaller network of Meridian 1 Internet-enabled systems (for example, 2 to 4 systems) using the node-based IP Trunk dialing plans, it may be practical to upgrade all systems, one by one, to Succession 1000M with IP Trunk, and then simultaneously reconfigure and cut over all the upgraded

systems to use IP Peer Networking Virtual IP Trunks within a single maintenance window. In this case you can choose a coordinated cutover scenario.

If you have already completed the migration of a large network of IP Trunk 3.0 and BCM 3.01 nodes (using any of the migration scenarios), you no longer need to consider migration when upgrading any additional Meridian 1 Internet-enabled systems to Succession 1000M. In these post-migration cases, you can choose a gradual, system-by-system cutover scenario, to immediately reconfigure and cut over each upgraded system to use the IP Peer Virtual Trunks and Gatekeeper-resolved Network Numbering Plan.

WARNING

1 Succession 3.0 Software (Call Server 3.00V, Signaling Server 2.10.80, IP Line 3.10.80) is not backwards compatible with Meridian 1 X11 Release 25.40 and IP Line 3.0 within a single system.

2 Prior to cutting over any upgraded Succession 1000M system belonging to a large IP Trunk network to use IP Peer Virtual Trunks:

a. All ITG Trunk nodes in the network must be upgraded to run IP Trunk release 3.01 and migrated to use the Gatekeeper-resolved Network Numbering Plan.

b. BCM systems using IP trunks must be upgraded to Release 3.01 and migrated to use the Gatekeeper-resolved Network Numbering Plan.

Failure to upgrade and migrate all nodes to IP Trunk 3.01 and BCM Release 3.01 using the Gatekeeper will isolate the non-upgraded nodes in the network from the nodes using Gatekeeper for Network Numbering Plan resolution.

3 Software releases prior to IP Trunk 3.00 and BCM 3.01 do not interoperate with the Succession 3.0 Gatekeeper and therefore cannot support calls to and from the Succession 3.0 system using the IP Peer Virtual IP trunks.

4 IP Trunk 3.00 interoperates with the Succession 3.0 Gatekeeper and IP Peer Virtual IP trunk Gateways, and also with the ITG Trunk 2.xx and BCM 2.50 and 3.00 nodes in the network, because IP Trunk 3.xx supports dual methods of resolving destinations by:

a. node-based dialing plan resolution for interoperation with ITG Trunk 2.xx nodes, BCM 2.50 and 3.00, and IP Trunk 3.00 nodes (if desired — for example, for Network QoS Fallback to PSTN)

b. the Succession 3.0 Gatekeeper Network Numbering Plan resolution for interoperation with IP Peer Gateways, IP Trunk 3.00, and BCM 3.01.

Upgrade scenarios

Table 6 lists the upgrade scenarios.

Table 6
Upgrade scenarios (Part 1 of 5)

Scenario	Description	General tasks
Software and system upgrades		
1	Software and system upgrade using the pre-upgrade migration method. Refer to "Scenario 1: Software and system (pre-upgrade migration)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Install the stand-alone Succession Signaling Server at two sites and configure Primary and Alternate Gatekeepers to avoid a single point of failure. **2** Migrate the entire IP Trunk 3.0 network and an associated BCM network to use the Gatekeeper-resolved Network Numbering Plan. **3** Later, upgrade the Succession Call Server to Succession 3.0 Software, and simultaneously upgrade IP Line node to IP Line 3.1. **4** Cut over the upgraded Succession 1000M system to use IP Peer Virtual Trunks.
2	Software and system upgrade using the post-upgrade migration method. Refer to "Scenario 2: Software and system (post-upgrade migration) in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade two or more Meridian 1 Internet-enabled systems to Succession 1000M systems and simultaneously upgrade IP Line node to IP Line 3.10. Continue to use IP Trunks with local node-based dialing plan. **2** Configure Primary and Alternate Gatekeepers to avoid a single point of failure. **3** Migrate the entire IP Trunk 3.01 network to use the Gatekeeper-resolved Network Numbering Plan. **4** Cut over the upgraded Succession 1000M systems to use IP Peer Virtual Trunks.

Table 6
Upgrade scenarios (Part 2 of 5)

Scenario	Description	General tasks
3	Software and system upgrade using the coordinated cutover method. Refer to "Scenario 3: Software and system (coordinated cutover)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade all Meridian 1 Internet-enabled systems to Succession 1000M. Continue to use IP Trunks with local node-based dialing plan. **2** Coordinate the simultaneous cutover of all the upgraded Succession 1000M systems to use IP Peer Virtual Trunks and the Gatekeeper-resolved Network Numbering Plan.
4	Software and system upgrade of Meridian 1 systems equipped with IP Line only. Refer to "Scenario 4: Software and system (IP Line only)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade the Meridian 1 Internet-enabled system to Succession 1000M system and simultaneously upgrade IP Line node to IP Line 3.10.

Table 6
Upgrade scenarios (Part 3 of 5)

Scenario	Description	General tasks
Software-only upgrades		
5	Software-only upgrade to Succession 3.0 Software. Refer to "Scenario 5: Software only" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade the OTM application. **2** Upgrade the IP Line application. **3** Upgrade the system software to Succession 3.0 Software. **4** Configure IP Telephony Node. **5** Upgrade the IP Trunk application.
System-only upgrades		
6	System-only upgrade of a system whose IP Trunk 3.01 network has previously been migrated. Refer to "Scenario 6: System only (post-migration)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Install Succession Signaling Servers on the Succession 3.0 system that is being upgraded to Succession 1000M. **2** Perform keycode expansion on the Succession Call Server to expand the system limit for IP Peer Virtual Trunks. **3** Cut over the upgraded Succession 1000M system to use IP Peer Virtual Trunks.

Table 6
Upgrade scenarios (Part 4 of 5)

Scenario	Description	General tasks
7	System-only upgrade using the post-upgrade migration method. Refer to “Scenario 7: System only (post-upgrade migration)” in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade one or more Meridian 1 Succession 3.0 Software systems to Succession 1000M by adding one or more Succession Signaling Servers. **2** Perform keycode expansion on the Succession Call Server to expand the system limit for IP Peer Virtual Trunks. **3** Migrate the entire IP Trunk 3.0 network to use the Gatekeeper-resolved Network Numbering Plan. **4** Cut over the upgraded Succession 1000M system to use IP Peer Virtual Trunks.

Table 6
Upgrade scenarios (Part 5 of 5)

Scenario	Description	General tasks
8	System-only upgrade using the coordinated cutover method. Refer to "Scenario 8: System only (coordinated cutover)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade one or more Meridian 1 Succession 3.0 Software systems to Succession 1000M by adding one or more Succession Signaling Servers. **2** Configure the upgraded Succession 1000M systems to use IP Peer Virtual Trunks and Gatekeeper-resolved Network Numbering Plan.
9	System-only upgrade of Meridian 1 systems equipped with IP Line only. Refer to "Scenario 9: System only (IP Line only)" in *Small System: Upgrade Procedures* (553-3011-258) or *Large System: Upgrade Procedures* (553-3021-258) for the detailed list of tasks and procedures.	**1** Upgrade one or more Meridian 1 Succession 3.0 Software systems to Succession 1000M by adding one or more Succession Signaling Servers.

IP Line 3.1

Contents

This section contains information on the following topics:

Overview

Succession 3.0 introduces the IP Line 3.1 application.

The IP Line 3.1 application provides an interface that connects an Internet Telephone to a Meridian 1 PBX, a Succession 1000M Call Server, and a Succession 1000 Call Server.

IP Line 3.1 ports the IP Line 3.0 functionality from Succession 1000 to Meridian 1 and Succession 1000M systems.

Note: IP Line 3.1 does not operate on Meridian 1, Succession 1000M, or Succession 1000 systems running software earlier than Succession 3.0.

IMPORTANT!

Succession 3.0 does not support IP Line 3.0.

Features

IP Line 3.1 introduces the following features:

- ringer and buzz volume adjustment for Internet Telephones. See "Internet Telephone Enhancements" on page 333.
- Russian, Latvian, and Turkish added to the Internet Telephone's Language menu
- registered and configured TNs are displayed in the Set Info menu. See "Internet Telephone Virtual Office" on page 337.
- i2050 Software Phone user-selectable Codec
- new CLI commands
- improved TN display in the command **setInfo** output
- an SNMP alarm is sent when a new master is elected in a node
- separate Operational Management (OM) reports for each Internet Telephone type
- enhanced redundancy for IP Line nodes

The following functionalities, previously available only for Succession 1000, are now available for the Meridian 1 and Succession 1000M systems:

- support for the Succession Signaling Server platform
- end-user features
  - — User-defined Feature Key Labels

- — Corporate Directory
- — Network-Wide Virtual Office
- — Private Zone classification
- — Codec selection, configuration, and registration enhancements

- additional administration and support features
  - — support for Element Manager (Succession 1000M only)
  - — call statistics enhancements
  - — Dynamic Loss Plan; replaces the Static Loss Plan
  - — set-based installation
  - — Login Banner enhancement and password guessing protection

Many of these features were first introduced in the IP Line 3.0 application and are now available for the Meridian 1 and Succession 1000M systems running Succession 3.0 software. For more detailed information on these features, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Table 7
IP Line 3.1 feature support (Part 1 of 3)

Feature	Meridian 1	Succession 1000M	Succession 1000
Support for Succession Media Card	Yes	Yes	Yes
Support for Element Manager	No	Yes	Yes
Support for Succession Signaling Server	Yes	Yes	Yes

Table 7
IP Line 3.1 feature support (Part 2 of 3)

Feature	Meridian 1	Succession 1000M	Succession 1000
Support of the following Internet Telephones: • i2002 • i2004 Support of the following software clients: • i2050 Software Phone	Yes	Yes	Yes
Dynamic Loss Plan *	Yes	Yes	Yes
NAT enhancement	Yes	Yes	Yes
Network-wide Virtual Office	Yes	Yes	Yes
Patching	Partial[a]	Partial[a]	Yes
802.1Q	Yes	Yes	Yes
Corporate Directory	Yes	Yes	Yes
Data Path Capture tool	Yes	Yes	Yes
Call statistics enhancements	Yes	Yes	Yes
User-defined Feature Key Labels	Yes	Yes	Yes
Private Zone	Yes	Yes	Yes
Graceful TPS Disable	Yes	Yes	Yes
Run-time download	Yes	Yes	Yes
Codec selection, configuration, and registration enhancements	Yes	Yes	Yes
Watchdog Timer	Yes	Yes	Yes

Table 7
IP Line 3.1 feature support (Part 3 of 3)

Feature	Meridian 1	Succession 1000M	Succession 1000
Improved Login Banner and Password Guessing Protection	Yes	Yes	Yes
Ringer and buzzer volume adjustment *	Yes	Yes	Yes
Set-based install (Small Systems only)	Yes	Yes	Yes
Maintenance Audit enhancement	Yes	Yes	Yes
Three new languages: Russian, Latvian, Turkish *	Yes	Yes	Yes
Enhanced Redundancy for IP Line nodes*	Yes	Yes	Yes
Codec selection for the i2050 Soft Phone *	Yes	yes	Yes

a. Node level patching is not provided by OTM 2.1. The patching CLI command of the Succession Media Card 32-port line card, Succession Media Card 8-port line card, and ITG-Pentium 24-port line card can be used.

* = introduced in IP Line 3.1

Voice Gateway Media Card

If a Succession Media Card 32-port card, a Succession Media Card 8-port card, or an ITG-P 24-port card is running IP Line 3.1 software, it is known as a Voice Gateway Media Card.

Administration

Element Manager or OTM 2.1 can be used to administer IP Line 3.1.

Element Manager

Element Manager resides on the Succession Signaling Server. Element Manager is used to administer the Succession 1000 and Succession 1000M systems.

OTM 2.1

Since there is no Succession Signaling Server in a Meridian 1, OTM 2.1 is required to administer a Meridian 1 system. OTM 2.1 is also necessary for the creation of the Corporate Directory database. Element Manager does not provide an SNMP alarm browser, so the OTM 2.1 Alarm Manager is recommended when SNMP alarm collection is required.

System configurations

The IP Line 3.1 application functions differently in the following system configurations with Succession 3.0 Software:

- Succession 1000 and Succession 1000M
- Meridian 1
- Branch Office configuration

Succession 1000 and Succession 1000M

A Succession Signaling Server is part of the Succession 1000 and Succession 1000M systems. The Terminal Proxy Server (TPS) executes on the Succession Signaling Server and the voice gateway executes on the ITG-P 24-port or Succession Media Card line card. All Internet Telephones register with the Succession Signaling Server. The Voice Gateway Media Cards provide only the gateway media access for both IP Line and IP Trunks. The Succession Signaling Server is configured as the Leader and acts as the Master for the Node.

Survivability

A secondary Succession Signaling Server can exist in this system configuration. If the primary Succession Signaling Server fails, the secondary Succession Signaling Server takes over, and all Internet Telephones re-register with the secondary Succession Signaling Server. If the secondary Succession Signaling Server also fails, or there is no secondary Succession Signaling Server and the primary Succession Signaling Server fails, a Voice Gateway Media Card is selected as the node master and Internet Telephones register with the Voice Gateway Media Cards.

Additional nodes can be configured in the system. In a multi-node system, the primary node contains the Leader Succession Signaling Server. In the additional nodes, the Voice Gateway Media Cards operate in the following manner. In each node, one Voice Gateway Media Card is configured as a Leader. The Voice Gateway Media Cards that are members of the node provide both the LTPS and voice gateway functionality.

Element Manager stores the CONFIG.INI and BOOTP.TAB files for these nodes on the Succession Call Server. When a transfer operation is requested, it notifies each card in the node to retrieve these files from the Call Server. The Internet Telephone's firmware is uploaded to a directory on the Succession Signaling Server and when it is sent to the Voice Gateway Media Cards, the firmware is stored only in memory on those cards.

Meridian 1

A Meridian 1 system with only IP Line or IP Trunk functionality cannot have a Succession Signaling Server.

In a Meridian 1 system with only IP Line functionality, the TPS and media gateway functionality reside on the Voice Gateway Media Cards. In each node, one Voice Gateway Media Card is configured as a Leader. The Voice Gateway Media Cards in the node provide both the TPS and voice gateway functionality. All Internet Telephones register with the Voice Gateway Media Cards.

Since there is no Succession Signaling Server in this configuration, Element Manager is not available as it requires the Succession Signaling Server platform. OTM 2.1 must be used for system administration and management. There are no Virtual Trunks or Gatekeeper in this configuration. Without the Gatekeeper, the Network Wide Virtual Office feature loses its "Network Wide" functionality but can still be used for Virtual Office operations within the Call Server to which the Internet Telephones are registered.

Branch Office configuration

The IP Line 3.1 application makes no change to Branch Office functionality.

Internet Telephones in the Branch Office first register with the Branch Office LTPS, then are redirected to the Main Office's TPS. If the connection to the Main Office is lost, the Internet Telephones register with the Branch Office TPS and continue to have service because the Internet Telephones are configured with the Branch Office TPS's node IP address (S1/S2 address). The Voice Gateway Media Cards provide the gateway media access for both IP Line and IP Trunks.

For more information about the Branch Office configuration, see *Branch Office* (553-3001-214) NTP.

Codec support and selection

The IP Line 3.1 application provides the gateway functionality for systems running Succession 3.0 software. IP Line 3.1 supports the Codecs and gateway functions not only for IP Line but also for IP Trunk.

IP Line administration has been updated. The following can now be configured using Optivity Telephony Manager (OTM) 2.1 or Element Manager:

- maximum jitter buffer (voice playout) size
- separate jitter buffer settings for different Codecs

Table 8 shows the Codecs that are supported on the Meridian 1, Succession 1000M, and Succession 1000 systems:.

Table 8
Supported Codecs

Codec	Payload size
G.711 a-law, G.711 mu-law, NOVAD	10, 20, and 30 ms
G.729A	10, 20, 30, 40, and 50 ms
G.729AB	10, 20, 30, 40, and 50 ms
G.723.1 [1]	30 ms
T.38 [2]	supported for fax calls on gateway channels
G.711 Clear Channel [2]	supported for fax calls on gateway channels
Note 1: The G.723.1 Codec has bit rates of 5.3 Kbps and 6.3 Kbps. In IP Line 3.1, The G.723.1 Codec can only be configured with a 5.3 Kbps bit rate; however, the system accepts both G.723.1 5.3Kbps and 6.4Kbps from the far end.	
Note 2: T.38 is the preferred Codec type for fax calls over virtual trunks. However, the G.711 Clear Channel Codec is used if the far end does not support the T.38 Codec.	

Dynamic Loss Plan

IP Line 3.0 replaced the Static Loss Plan with a Dynamic Loss Plan.
IP Line 3.1 now offers Dynamic Loss Plan functionality to the Meridian 1 systems. In earlier IP Line applications, loss plan values were retrieved from the CONFIG.INI file and loaded into the gateway's Rx/Tx pad registers. These values were used for every call through the gateway, regardless of the endpoint connection. The Call Server sends pad messages to the gateway card for every call. This allows the Call Server to adjust the gain through the gateway card for every call to match the local endpoint. The loss is adjusted to achieve a target Overall Loudness Rating (OLR) of +10 dB. This change allows the gateway to be used for both IP Line and IP Trunk calls. This also allows better interworking with other IP network devices.

The configuration of the loss plan values is now performed using LD 73 instead of selecting the Country in the OTM or Element Manager GUI. With the introduction of the Dynamic Loss Plan on all systems, the Country selection in OTM and Element Manager is no longer needed. The default value is the North American Loss Plan. When the system is installed in other countries, the customer must have the GPRI package and must enter the NTP specified pad values in LD 73's PDCA prompt Table 15.

United Kingdom

In addition, when a system is installed in the UK, the CLI command **UKLossPlanSet** is entered at the CLI of one card in each node. This adjusts the loss plan of the Internet Telephones to the higher transmit levels required in the UK. Follow the steps in Procedure 1 to set the loss plan for the UK.

Procedure 1
Setting the loss plan for the UK

1. Telnet to the card, connect to the maintenance port, or use OTM 2.1 or Element Manager to access the Voice Gateway Media Card.
2. Log into the IPL> shell.
3. At the IPL > CLI, enter the command **UKLossPlanSet**. Press <cr>.
4. Exit from the login session.

End of Procedure

After the UKLossPlanSet command is entered, the loss plan adjustment is transmitted by that card to all other cards in the node. The loss plan is then adjusted on any registered Internet Telephones, and on other Internet Telephones as they register.

To clear the loss plan adjustment, use the command **UKLossPlanClr.**

Table 9 lists the commands to set and adjust the gains for the UK (or other places where loss plan adjustment of Internet telephones is needed).

Table 9
Internet Telephone Loss Plan commands

IPL> command	Description	Succession Signaling Server
UKLossPlanSet	Increases the Tx level of the Internet Telephone to match the requirement for the UK.	X
UKLossPlanClr	Removes the loss plan adjustment and returns the Internet Telephone to the default loss plan levels.	X
lossPlanPrt	Prints the current Internet Telephone loss plan settings.	X
lossPlanSet <transducer> <rlrOffset> <slrOffset>	Allows a variable offset from the default loss plan to be entered for the specified transducer (handset, handsfree, or headset). The rlrOffset adjusts the level heard at the Internet Telephone. The slrOffset adjusts the level transmitted from the Internet Telephone. Positive numbers reduce the level (add loss). Negative numbers increase the level (add gain).	X
lossPlanClr	Removes the loss plan adjustment and returns the Internet Telephone to the default loss plan levels.	X

CAUTION

Care must be taken when altering the Internet Telephone's loss plan. Increasing the gain increases the possibility of echo and other audio problems. Only adjust the levels when instructed by this document or by Nortel Networks support staff.

Corporate Directory

The Corporate Directory feature is based on the M3900 telephone Corporate Directory feature.

The Corporate Directory database is created using OTM 2.1 and is generated from one of the following:

- configured DN information from the Call Server
- data from a corporate Lightweight Directory Access Protocol (LDAP) server

The Corporate Directory database is downloaded and stored on the Call Server. It is then accessible to the Internet Telephones. The Succession Signaling Server can support Corporate Directory access for the same number of Internet Telephones that are registered.

The Directory key on the Internet Telephone is used to access the directory, select a listing, and then dial a number from the Corporate Directory. The Navigation keys are used to refine the search within the Corporate Directory.

Corporate Directory is configured in LD 11. LD 11 accepts Corporate Directory Allowed/Corporate Directory Disallowed (CRPA/CRPD) Class of Service for the Internet Telephones.

For more information about the operation of the Corporate Directory feature, refer to the following:

- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)
- *Internet Terminals: Description* (553-3001-368)

Support of Element Manager

Element Manager enables the configuration of IP Line 3.1 using Internet Explorer 6.01 on Succession 1000 and Succession 1000M systems.

Each Succession Signaling Server hosts an Element Manager web server, that allows configuration, administration, and maintenance to be performed on the system components. Element Manager is a graphical Web interface. It provides a graphical alternative to the traditional CLI and overlays. The interface is available to users running Internet Explorer 6.x on a PC. No special client software is required.

The Element Manager web server runs on each Succession Signaling Server and the Succession Signaling Server acts as a file server.

When a web browser is opened and the IP address of the Succession Signaling Server is entered, the Element Manager interface is displayed. Element Manager is then used to perform tasks such as configuring an IP Telephony node, checking and uploading loadware and firmware files, and retrieving the CONFIG.INI and BOOTP.TAB configuration files from the Succession Call Server. The Voice Gateway Media Cards are notified to transfer the files from the Call Server using FTP.

OTM 2.1's Navigators incorporate links to each Element Manager web server in a network.

For more information, refer to *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) and *Succession 1000 Element Manager: System Administration* (553-3001-332).

Call Statistics Enhancements

IP Line 3.0 introduced an increased capability to collect call statistics. With IP Line 3.1, these enhancements apply to Meridian 1 and Succession 1000M systems.

LD 32

The following four commands have been added to LD 32:

- ENCT CARDS L S C <customer>
- ECNT ZONE zoneNum <customer>

- ECNT NODE nodeNum
- ECNT SS hostName

Table 10 on page 57 describes the new commands added to LD 32.

Table 10
Additional LD 32 commands (Part 1 of 2)

Command	Description
ECNT CARD L S C <customer>	Counts and prints the number of Internet Telephones registered for the specified card. • If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count for that parameter. A customer cannot be specified in this case. Example: ecnt card 81 << Card 81 >> Number of Registered Ethersets: 5 Number of Unregistered Ethersets: 27
ECNT ZONE zoneNum <customer>	Counts and prints the number of Internet Telephones registered for the specified zone. • If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. Example: ecnt zone 0 0 << Zone 0 Customer 0 >> Number of Registered Ethersets: 4 Number of Unregistered Ethersets: 17

Table 10
Additional LD 32 commands (Part 2 of 2)

Command	Description
ECNT NODE nodeNum	Counts and prints the number of Internet Telephones registered for the specified node. • If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ecnt node 8765 << Zone 8765 >> Number of Registered Ethersets: 3
ECNT SS hostName	Counts and prints the number of Internet Telephones registered for the specified Signaling Server. • If hostName parameter is not entered, the count is printed for all signaling servers. Example: ecnt ss << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Registered Ethersets: 1000

For more information, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

System traffic report

An Internet Telephone Zone Traffic Report 16 in LD 2 is created on the system to add the printing of Internet Telephone data at the zone level. The data is printed for the following categories at the end of each collection period on a per-zone basis.

- total inter/intra calls made
- total inter/intra calls blocked
- percent average inter/intra zone bandwidth used

- percent maximum inter/intra zone bandwidth used
- total inter/intra zone bandwidth threshold exceeded count

The counts are reset after the data is printed.

The "Total inter/intra zone bandwidth threshold exceeded count" prints the number of times a user-configured bandwidth threshold was exceeded for the zone during the collection period. Existing LD 2 commands that set the system threshold are used with a new value defined for the bandwidth threshold.

Table 11
System threshold commands

Command	Description
TTHS TH tv	Prints the current system thresholds.
STHS TH tv -- TV	Sets the system thresholds.
Note 1: The system thresholds TH values 1–4 already exist. A new TH value of 5 is used to designate the zone bandwidth threshold. ***Note 2:*** The system thresholds TV value is the percentage of the zone's maximum bandwidth. The range values are 000–999, where 000 corresponds to 00.0% and 999 corresponds to 99.9%. The default is 90.0%.	

For more information, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

User-defined Feature Key Labels

Definition

IP Line 3.1 lets the Internet Telephone user program the label on the feature key. This label change is saved and then displayed on the feature key.

Availability

Table 12 describes the feature key information for the Internet Telephones.

Table 12
Feature keys

Model	Number of feature keys	Number of feature keys using Shift key	Maximum label character length
i2002	4	N/A	10
12004	6	12	10
i2050	6	12	10

The Feature Key labels for each Internet Telephone are stored in a text file in the c:/u/db/database.rec directory on the Call Server. The label information is retrieved from the file during the sysload of the Call Server into memory. When the Call Server performs an EDD, the information is dumped to the file.

When the Internet Telephone registers with the Call Server, the Call Server looks up the Feature Key label in the memory, based on the TN of the Internet Telephone. If the labels are found, they are sent to the telephone when the key map download occurs. If the labels are not found, the Call Server sends out the key number strings or key functions.

For more information about programmable line (DN)/feature keys (self-labeled), refer to *Internet Terminals: Description* (553-3001-368).

Private Zone configuration

Private Zones are available for the Meridian 1, Succession 1000, and Succession 1000M.

Lack of DSP resources

DSP resources for each customer are placed in one common pool. A DSP channel is allocated to an IP-to-circuit-switched call based on a round-robin searching algorithm within the pool.

If an available resource cannot be found, the overflow tone is heard. For most installations, this approach works because all Internet Telephone users share the IP Line DSP resources. The DSPs can be provisioned using a DSP-to-Internet Telephone ratio similar to trunk resources, since the DSPs are used only for circuit-switched access or conference calls.

When IP-to-PSTN calls are used, such as with ACD agents or other users who consistently are using trunk resources when making calls, it becomes difficult to provision the system in a way that guarantees an available DSP channel when these users need it. If the other users suddenly make a lot of conference calls or trunk calls, the DSP resources can be deplete. As a result, calls cannot be made. This occurs because all DSP channels are in one pool.

DSP resources and Private Zones

To address this situation, IP Line 3.1 adds the Private Zone Configuration feature for DSP configuration and allocation to the zone configuration. This feature enables the configuration of one or more gateway channels as a private resource. This guarantees DSP availability for critical or ACD agent Internet Telephones.

A zone can be configured as shared or private in LD 117.

Shared Zone

The current default zone type is a shared zone. Internet Telephones configured in shared zones use DSP resources configured in shared zones. If all the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked.

Select gateway channels in the following order:

1 Select a channel from the same zone as the Internet Telephone is configured.

2 Select any available channel from the shared zones' channels.

Private Zone

The Private Zone enables DSP channels configured in a private zone to be used only by the Internet Telephones that have also been configured for that

private zone. If more DSP resources are required by these Internet Telephones than what are available in the zone, DSPs from other shared zones are used.

Internet Telephones configured in shared zones cannot use the private zones' channels.

Select the gateway channels in the following order:

1. Select a channel from the same private zone as the Internet Telephone is configured.
2. Select any available channel from the pool of shared zones' channels.

LD 117 - zone configuration

DSP channels and Internet Telephones are set as shared or private based on zone configuration. In LD 117, zone configuration can be set to either shared or private using the parameter <zoneResourceType>.

A zone is configured in LD 117 as follows:

NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]

CHG ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]

By default, a zone is configured as shared (zoneResourceType=shared).

Example

The command to add a new zone, zone 10, is as follows:

```
new zone 10

Zone 10 added. Total number of Zone = n
(where n is the total number of zones)
```

Site details

Use the **prt zone** command to see details for all configured zones. Table 13 gives a sample output of the prt zone command.

Table 13
Sample output from prt zone command

			Intrazone				Interzone				
Zone	State	Type	Bandwidth (Kbps)	Strategy	Usage (%)	Peak (Kbps)	Bandwidth (Kbps)	Strategy	Usage (%)	Peak (Kbps)	HO/BRCH
0	ENL	SHARED	100000	BQ	0	0	100000	BQ	0	0	HO
1	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO
4	ENL	PRIVATE	10000	BQ	0	0	10000	BQ	0	0	HO
10	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO

Resource sharing for shared and private zones

If a resource-critical Internet Telephone is configured for a private zone, and there are not enough resources found within that zone, the search continues into the shared zones within the same customer for an available DSP channel.

However, if an Internet Telephone is configured in a shared zone, the PBX/Call Server limits its search to the pool of shared DSP channels. The search does not extend into the private zones' channels.

When configuring the allocation of shared versus private resources, consideration must be given to the number of private resources that are needed. Configure enough DSP resources to prevent the Internet Telephones configured in shared zones from running out of channels.

WARNING

The Call Server does not search for channels in Private Zones if it is configured to use only Shared Zones. Only Internet Telephones configured in the same Private Zone can use the Private Zone voice gateway channels.

Since the channels in the Private Zone are not accessible to Internet Telephones in the Shared Zone, ensure that only enough private channels are configured to cover the Internet Telephones in the Private Zone. Do not configure more channels than are required in the Private Zone, as the Shared Zone Internet Telephones cannot access these channels.

Run-time configuration changes

IP Line 3.1 enables most changes to be made without disabling or rebooting the Voice Gateway Media Cards. After adding configuration information for a new Voice Gateway Media Card and downloading the BOOTP file to the Leader, a new Voice Gateway Media Card can be added to an existing node without rebooting the other cards.

The following exceptions require a reboot:

- role changing; that is, changing a Leader to Follower or changing Follower to Leader
- changing the node IP subnet masks or gateway IP addresses requires a reboot of all cards in the node
- changing the IP address of a particular card so it can retrieve its new IP address information

Supported run-time changes

IP Line 3.1 supports run-time changes for the following:

- changes to the CONFIG.INI file
- add card or delete card changes to the BOOTP.TAB file

Configuration changes have an effect only on new calls. Existing calls are not interrupted. The following are exceptions:

- If the active Call Server ELAN link's configuration data is changed (for example, a changed IP address), then active calls are released.

  Note: If the non-active Call Server is changed (for example, survivable side IP address), then the calls are not affected.

  When the ELAN connections are taken down to implement the configuration change, the Internet Telephones and gateway channels registrations are unregistered on the Call Server. The Call Server releases the calls. When the link is re-established, the TPS synchronizes the call states and releases the active calls. Service is interrupted during this re-establishment period and the following are affected:

  — New Internet Telephones cannot register.

  — Registered Internet Telephones cannot establish new calls.

  — The Voice Gateway Media Card's faceplate displays S009.

  Once the ELAN link comes back up, the Line Terminal Proxy Server (LTPS) re-registers the telephones with the Call Server and all service is resumed.

- If the Codec list is changed, the Voice Gateway Media Card's DSPs might need to be reloaded. For instance, one DSP image contains G.711, FAX, and G.729A/G.729AB. The other DSP image contains G.711, FAX, and G.723.1. If the user has a node configured with the G.729AB Codec and the user performs an administrative change to use G.723.1 (or vice versa), the DSPs must be reloaded.

  After the CONFIG.INI file containing the administrative change is downloaded to a Voice Gateway Media Card, the card's DSPs are

reloaded as they become idle. For instance, if all DSPs are idle on the card, the new image is loaded to all of them at once. If one or more DSPs have active calls, the DSP is not reloaded until the active calls have been released. This can cause some DSPs to be reloaded later than others.

This functionality is supported by both Element Manager and OTM 2.1.

Network-Wide Virtual Office

Network-Wide Virtual Office is supported for the Succession 1000 and Succession 1000M systems.

IP Line 3.1 provides the Network Wide Virtual Office feature. This feature enables a user to use any Internet Telephone within the network.

The Virtual Office feature provides a call service to “travelling” users who want to use a different physical Internet Telephone (other than the telephone they normally use). Users can log in to another Internet Telephone using their DN and pre-configured Station Control Password (SCPW).

Once logged in, users have access to their DNs, autodial numbers, key layout, feature keys, and voice mail indication/access that are configured on their own home/office Internet Telephones. For example, if users go to another office or to a different location within the same office, they can log in to any available Internet Telephone and have all the features of their home/office Internet Telephone. When the user logs off the Internet Telephone, the features that were “transferred” to that telephone are removed.

Network Wide Virtual Office and the Gatekeeper

Network Wide Virtual Office is limited to a single Gatekeeper zone. As long as Virtual Offices share the same Gatekeeper, a Virtual Office login can redirect an Internet Telephone to any of the systems.

Requirements

A Succession Signaling Server or standalone Gatekeeper is required in the network.

Supported Internet Telephones

Virtual Office is supported for the i2002 and i2004 Internet Telephones, and the i2050 Software Phone. An i2004 or i2050 user can log in from an i2002 Internet Telephone under certain conditions. See “Set-type checking and blocking” on page 68.

Table 14 on page 67 shows which user can log in to particular telephones.

Table 14
Virtual Office login from various telephones

Internet Telephone User	Virtual Office login
An i2002 Internet Telephone user...	...can Virtual Office login from i2002, i2004, and i2050.
An i2004 Internet Telephone user...	...can Virtual Office login from i2004 and i2050. ...can log in under certain conditions when the user attempts a Virtual Office login from an i2002 Internet Telephone. See “Set-type checking and blocking” on page 68.
An i2050 Software Phone user...	...can virtually login from i2004 and i2050. ...can log in under certain conditions when the user attempts a Virtual Office login from an i2002 Internet Telephone. See “Set-type checking and blocking” on page 68.

Configure Virtual Office User Allowed (VOUA) and Virtual Office Login Allowed (VOLA) on the Internet Telephones as follows:

- The Internet Telephone where the user wants to virtually log in (destination) must have Virtual Office User Allowed (VOUA) configured.
- The Internet Telephone from which the user wants to log in (source) must have Virtual Office Login Allowed (VOLA) configured.

Failed password attempt

Three failed password attempts to log in using the Virtual Office feature locks the user out from Virtual Office login at the Call Server for one hour. The Call Server lock can be removed by an administrator using a LD 32 command to disable and re-enable that TN. Refer to *Succession 1000 System: Maintenance* (553-3031-500) or *Software Input/Output: Maintenance* (553-3001-511) for more information.

Passwords and Internet Telephone registration

An Internet Telephone registers using the TN (in its EEPROM). A valid user ID and password are used to determine the Home TPS for the Internet Telephone during the Virtual Office connection. A Gatekeeper is required if the Home TPS is not the TPS where the Internet Telephone is registered when the Virtual Office login is initiated.

Virtual Office capabilities

Virtual Offices provides the following capabilities:

1 A network-wide connection server (Gatekeeper) is equipped to provide addressing information of call servers, based on a user's DN.

2 A key sequence is entered at an Internet Telephone to initiate the login sequence. Then the current network DN and a user-level password is entered. The password is the Station Control Password configured in LD 11. If a SCPW is not configured, the Virtual Office feature is blocked.

3 The user can log out when leaving the location.

For more detailed information about Virtual Office, see *Internet Terminals: Description* (553-3001-368).

Set-type checking and blocking

If the registration is a regular request (not a Virtual Office login), the Succession Call Server checks the configured TN type against the actual set type. If they do not match, the registration is blocked.

However, if the registration request is a virtual login, this check is not performed. All sets are allowed to be registered onto any IP TN type when the login is through Virtual Office.

Special checking on the DN/ Feature keys is performed when an i2004 or i2050 user logs in from an i2002 Internet Telephone.

Special checking prevents a user from logging in from an Internet Telephone that cannot display an incoming call, because the Internet Telephone used to log in does not have the DN/Feature key(s) to display the incoming call.

If the login were allowed to occur, it could result in the Internet Telephone ringing without providing the user a way to answer the call. The configuration of the logging-in user is examined for DN/Feature key types that receive incoming calls. If these appear on any keys not present on the type of Internet Telephone being used for the login, the login is blocked.

> ***Note:*** The login from i2002 Internet Telephones is blocked for users configured for ACD.

The i2002 Internet Telephone supports only 4 feature keys. Therefore, a restricted VO login is applied to i2004 and i2050 TNs when they log in using an i2002 Internet Telephone. When the i2004 or i2050 user logs in from an i2002 Internet Telephone, it is blocked if the user's configuration has one of the following:

- key 0 defined as ACD
- any key from key 4 to key 15 defined as AAK, CWT, DIG, DPU, GPU, ICF, MCN, MCR, MSB, PVN, PVR, SCR or SCN

Enhanced Redundancy for IP Line Nodes

The Enhanced Redundancy for IP Line nodes feature now allows Internet Telephones with 3-digit Node IDs to register to nodes configured with 4- digit Node IDs.

The rules are as follows:

- if the Node ID on the system has three digits or less, the Node ID from the Internet Telephone must match exactly

- if the Node ID on the system has four digits and:
  - — the Node ID from the Internet Telephone has fewer than 3 digits, reject the registration
  - — the Node ID from the Internet Telephone has 4 digits, the Node ID must match exactly
  - — if the Node ID from the Internet Telephone is 3 digits and they match the first 3 digits of the node's 4-digit Node ID (left to right), then allow the Internet Telephone to register. If the first three digits do not match, reject the registration.

This allows an installer to configure up to 10 nodes

(3 digit Node Id base + 0 - 9 for the 4th digit)

and program different S2 addresses into the Internet Telephones. This allows a given node's registered Internet Telephones to spread across the spare "phone registration capacity" of the other nodes in the system in the event of TLAN or node failure and provides redundancy.

Example

For example, the installer configures two nodes on a system with Node IDs 3431 and 3432. An Internet Telephone configured with Node ID 343 can register with either node.

If the Internet Telephone presented one of the following Node IDs, it would be rejected for registration

- 3
- 34
- 3433

The TN must still match before the phone is allowed to register.

If the customer does not want to use this feature, program 2- or 4-digit Node IDs and retain the "exact match" requirement.

Data Path Capture tool

IP Line 3.1 contains the Data Path Capture tool, a built-in utility used to capture audio information. This tool helps debug audio-related gateway problems and allows after-the-fact analysis of what the user heard.

The Data Path Capture process is controlled by a set of CLI commands.

Operational Management report enhancement

IP Line 3.1 enhances the Operational Management (OM) report.

The statistics are now broken out by Internet Telephone type. There are separate sections for the i2002 and i2004 Internet Telephones, the i2050 Software Phone, and the gateway channel section.

Password enhancement

If performing one of the following actions:

- Telnetting to the Voice Gateway Media Card
- Telnetting to the Succession Signaling Server
- logging in to the TTY

and the NPW1 is less than eight characters long, it is no longer necessary to add spaces at the end to make a password length of eight characters. The software does it automatically.

> ***Note:*** FTP transfers still require spaces to be added to equal eight characters due to the VxWorks requirement.

SNMP election notification

An SNMP alarm is sent when an election occurs and a new node master is elected.

The SNMP alarm ITG4045 is sent with the node ID and the card IP address of the new master.

See “Alarms” on page 73.

electShow CLI command

The CLI command `electShow` displays information about all cards registered in the node. It also lists any configured cards that are not registered.

The `electShow` command can be entered from any card in the node.

The nodeMaster field indicates if a card is currently the master.

Internet Telephones

IP Line 3.1 supports the following:

- i2002 Internet Telephone
- i2004 Internet Telephone
- i2050 Software Phone

Language support

The TPS offers three new languages: Latvian, Russian, and Turkish. These languages can be chosen from the Internet Telephone’s Language menu.

This feature is applicable to all of the Internet Telephones, except the i2050 Software Phone.

All of the screen messages and soft key labels match the language selected from the Option Menu on the telephone, including the three new languages: Russian, Latvian, and Turkish.

The default entry from the keypad keys is always English.

802.1Q Support

The i2002 and 2004 Internet Telephones support 802.1Q. 802.1Q. This support enables the definition of Virtual LANs (VLANs) within a single LAN. This improves bandwidth management, limits the impact of broadcast and multicast messages, and simplifies VLAN configuration and packet prioritization.

Modem support for the i2050

Selecting the check box in the i2050's **Configure Audio Properties** menu results in the i2050 only registering the best bandwidth Codecs: G.729A, G.729AB, and G.723.

This restricts the Codecs selected by the Call Server to those most suitable for modem connections.

One or more of these Codecs must be configured in OTM or Element Manager to support this. The system cannot be configured only for G.711 to support this feature.

Error indication

If an i2050 Software Phone calls a system or telephone on a node that is only configured with G.711, the following occurs:

- the user receives a fast busy signal
- an SNMP alarm ITG2010 is sent
- a message is printed on the LTPS console and in the syslog file

Voice Gateway Media Card administration

Alarms

IP Line 3.1 introduces an alarm that is sent when a node master is elected:

eventType = eventTypeCommunications = 0
alarmCause = alarmCauseUnknown = 202
specificProblems = "ITG4043"

perceivedSeverity = alarmSeverityWarning = 4
additionalText = “Latest election has changed the LTPS master of node”
<node ID> to card
<card's TLAN IP addr>

Overlays

LD 11

New Classes of Service (CLS) have been added to LD 11 for the Virtual Office and Corporate Directory features.

The Class of Service for the Virtual Office feature has been added. The Class of Service prompt includes the Virtual Office Login Allowed/Denied (VOLA/VOLD) and Virtual Office User Allowed/Denied (VOUA/VOUD) for Virtual Office.

LD 11 includes CRPA/CRPD Class of Service input for the Corporate Directory feature on the Internet Telephones. See Table 15.

Table 15
LD 11 prompts and responses (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add new data or change existing data
TYPE:	aaaa	Telephone type where aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 3000, 390X, i2002, i2004, i2050 Response accepted if the Digital Sets (DSET) package 88 and Aries Sets (ARIE) package 170 are equipped The number of i2002, i2004, and i2050 Internet telephones is also restricted by the Internet Telephone ISM setting.
TN	l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems

Table 15
LD 11 prompts and responses (Part 2 of 2)

Prompt	Response	Description
....	.....	.....
CLS	(VOLA) VOLD	Virtual Office Login Allowed on this TN Virtual Office Login Denied on this TN
	(VOUA) VOUD	Virtual Office User Allowed Virtual Office User Denied
	CRPA (CRPD)	Corporate Directory Allowed for this TN Corporate Directory Denied for this TN

LD 14

With IP Line 3.1, there are two minor changes to the administration of the Voice Gateway Media Cards in LD 14.

See "Configure physical TNs (LD 14) (p. 75)" for information on the VGW and XTRK prompts.

Configure physical TNs (LD 14)

Use LD 14 to define the physical TNs for the Voice Gateway Media Card.

Use LD 14 to disable the Voice Gateway Media Cards. The OTM 2.1 IP Telephony application requires Voice Gateway Media Cards to be in a disabled state before transmitting card properties.

See Table 16 for a list of the prompts and responses in LD 14.

Table 16
Configure physical TNs in LD 14 (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data
TYPE	VGW	Voice Gateway

Table 16
Configure physical TNs in LD 14 (Part 2 of 2)

Prompt	Response	Description
TN		Terminal Number of the first ITG Physical TN
	l s c u c u	For Large Systems For Small Systems
DES	x...x	Description for gateway channel.
		Identify the channel using the card's TLAN IP address or MAC address.
XTRK	aaa	Extended Trunk
	ITG8	ITG 486 8-port card
	ITGP	ITG-P 24-port card
	MC8	Succession Media Card 8-port card
	MC32	Succession Media Card 32-port card
ZONE	0 – 255	Zone number to which this ITG Physical TN belongs. Verify that the zone exists in LD 117.
CUST	xx	Customer number, as defined in LD 15

LD 20

For the TYPE prompt, the Internet Telephone type (for example, i2002) response is available as a customer response.

LD 81

Two changes have been made to LD 81.

1. The FEAT prompt prints for the Internet Telephone type (for example, i2002).
2. The FEAT prompt accepts VOLA, VOLD, VOUA, and VOUD for the Virtual Office feature.

LD 82

No new prompts have been added to LD 83; however, the Internet Telephone type (for example, i2002) is printed.

LD 117

With Line 3.1, Two new prompts have been added to LD 117 to translate an Internet Telephone's DN to its IP address and its IP address to its DN.

1 PRT DNIP <DN> [<CustomerNO>]

2 PRT IPDN <IPAddress>

Search criteria

If a customer number is entered, only that customer is searched for the designated DN. If no customer number is entered, the database for all customers on the system is searched.

The **PRT DNIP** command accepts a partially defined DN; that is, a DN entered with only partial leading digits. For example, entering a DN of 34 with no customer number results in output for any DN in the system starting with 34.

PRT DNIP output

The PRT DNIP command generally produces the following output:

- an initial line displaying the DN and Customer number. If there is output for multiple customers, this line is repeated before each customer's output.
- information for each occurrence of the DN on any internet telephone for that customer
  - TN
  - set type
  - key number of DN appearance and type of DN
  - current IP address of the Internet Telephone

— configured zone for the Internet Telephone

— state of the Internet Telephone's registration

Sample output

The following is a sample output of PRT DNIP.

```
=> PRT DNIP 4000 0 (only search customer 0 for DN)
CUST 00 DN 4000
TN Type Key IP Address Zone Status
------------------------------------------------------------------
061-01 i2002 03 SCR 47.11.215.41 000 REG
061-00 i2004 00 SCR 47.11.215.39 000 REG
=> prt dnip 4000 (same DN in different customers)
CUST 00 DN 4000
TN Type Key IP Address Zone Status
------------------------------------------------------------------
061-01 i2002 03 SCR 47.11.215.41 000 REG
061-00 i2004 00 SCR 47.11.215.39 000 REG
CUST 01 DN 4000
TN Type Key IP Address Zone Status
------------------------------------------------------------------
061-10 i2004 05 MCR 47.11.215.38 001 REG
```

PRT IPDN

The PRT IPDN command produces the following output:

- an initial line displaying the IP address for the search
- a second line displaying the customer number, TN, set type, zone and registration status of the Internet Telephone using the specified IP address
- information for all DNs configured on that Internet Telephone
- key number of DN appearance and type of DN
- DN
- configured CPDN for the DN

Sample output

The following is a sample output of PRT IPDN

```
=> PRT IPDN 47.11.215.38
IP 47.11.215.38
CUST 01 TN 061-10 TYPE i2004 ZONE 001 REG
Key DN CPND Name
-------------------------------------------
00 SCR 4010 I2004_1 VLN61-10
05 MCR 4000 i2004_cust1 vln61_10
```

Partial IP addresses

Partial IP addressed can be entered. Partial IP addresses can be entered with only the leading digits of the IP address (for example, 142.10), or as the IP address with zeroes at the end (for example, 142.10.0.0).

The following examples for "PRT IPDN <IP_ADDR>" shows a partial IP address of 47.0.0. The zeroes in the <IP_ADDR> are handled as if they are trimmed off.This means that the output of **PRT IPDN 47** is the same as that of **PRT IPDN 47.0.0**.

A sample of Internet Telephones has been configured in the following manner:

IP Address	TN	DN
47.11.216.138	063-20	4120
47.11.216.140	061-02	4002
47.11.215.39	061-00	4000
47.11.215.38	063-00	4100
47.11.215.41	063-01	4101

Example 1

To print the information on the Internet Telephones whose IP address starts with 47.11.215, enter the following:

=> prt ipdn 47.11.215

The following output is printed:

```
IP 47.11.215.38
CUST 01  TN 063-00  TYPE i2004  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4100     I2004_Cust_1 VLN63_00

IP 47.11.215.39
CUST 00  TN 061-00  TYPE i2004  ZONE 000  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4000     I2004_Cust_0 VLN61_00


IP 47.11.215.41
CUST 01  TN 063-01  TYPE i2001  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4101     I2001_Cust_1 VLN63_01
```

Example 2

Alternatively, to print the information on the Internet Telephones whose IP address starts with 47.11.215, enter the following:

=> prt ipdn 47.11.215.0

The following output is printed:

```
IP 47.11.215.38
CUST 01  TN 063-00  TYPE i2004  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
```

```
00 SCR   4100     I2004_Cust_1 VLN63_00

IP 47.11.215.39
CUST 00  TN 061-00  TYPE i2004  ZONE 000  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4000     I2004_Cust_0 VLN61_00

IP 47.11.215.41
CUST 01  TN 063-01  TYPE i2001  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4101     I2001_Cust_1 VLN63_01
```

Example 3

To print the information on the Internet Telephones whose IP address starts with 47.11.216, enter the following:

=> prt ipdn 47.11.216

The following output is printed:

```
IP 47.11.216.138
CUST 01  TN 063-20  TYPE i2002  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4120     I2002_Cust_1 VLN63_20

IP 47.11.216.140
CUST 00  TN 061-02  TYPE i2002  ZONE 000  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4002     I2002_Cust_0 VLN61_02
```

Example 4

Alternatively, to print the information on the Internet Telephones whose IP address starts with 47.11.216, enter the following:

=> prt ipdn 47.11.216.0

The following output is printed:

```
IP 47.11.216.138
CUST 01  TN 063-20  TYPE i2002  ZONE 001  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4120     I2002_Cust_1 VLN63_20

IP 47.11.216.140
CUST 00  TN 061-02  TYPE i2002  ZONE 000  REG
Key      DN       CPND Name
-------------------------------------------
00 SCR   4002     I2002_Cust_0 VLN61_02
```

Graceful Disable TPS CLI commands

Graceful Disable TPS CLI commands are used to gracefully disable the TPS and Voice Gateway services. Table 17 on page 83 lists the new commands.

The following Graceful TPS CLI commands are available at the IP Line shell:

Table 17
Graceful Disable commands

IPL> command	Description	Succession Signaling Server
disServices	Causes the Voice Gateway Media Card or Succession Signalling Server to gracefully switch the registered resources to the other Voice Gateway Media Cards or Succession Signalling Servers located in the same node. This command does not interrupt established calls	X
enlServices	Enables all the Voice Gateway Media Cards or Succession Signalling Servers to accept registrations of resources	X
forcedisServices	Forces all registered resources on the Voice Gateway Media Card or Succession Signalling Server to re-register with the other Voice Gateway Media Cards or Succession Signalling Servers in the node. This command will interrupt established calls	X
loadBalance	Causes the Voice Gateway Media Card or Succession Signalling Server to attempt to balance the registration load between this card/server and the rest of the node components.	X

Succession Signaling Server

Contents

This section contains information on the following topics:

Overview

Succession 3.0 Software introduces the Succession Signaling Server to Meridian 1 systems, making up the Succession 1000M portfolio.

> ***Note:*** The Succession Signaling Server already exists for Succession 1000 Release 2.0 systems. The information in this chapter is new only to Meridian 1 customers migrating to Succession 1000M.

The Succession Signaling Server is an industry-standard, PC-based server that provides a central processor to drive signaling for Internet Telephones

and IP Peer Networking (see Figure 1 on page 87). It provides signaling interfaces to the IP network using software components that run on the VxWorks™ real-time operating system. The Succession Signaling Servers can be installed in a load-sharing redundant configuration for higher scalability and reliability.

The Succession Signaling Server handles H.323 signaling, Internet Telephone signaling, and the Gatekeeper software.

Figure 1
Succession Signaling Server

Equipment identification

The product code for the Succession Signaling Server is NTDU27.

Power

The power cord connector is located on the rear, left-hand corner of the Succession Signaling Server. When the green power LED on the left-hand side illuminates, the power is on. The Power On/Off switch is on the front faceplate. The power supplies are factory installed and not customer replaceable.

Cooling

The Succession Signaling Server has forced air cooling. The fan runs whenever the Succession Signaling Server is on. The air flow is front-to-back.

Card slots

The Succession Signaling Server has no available card slots.

Connectors (front)

Figure 2 on page 88 shows the DB-9 serial port, the CD-ROM drive, and the floppy drive on the front of the Succession Signaling Server. The front DB-9 serial port can support a login session for Command Line Interface (CLI) management.

Figure 2
Connectors on the front of the Succession Signaling Server

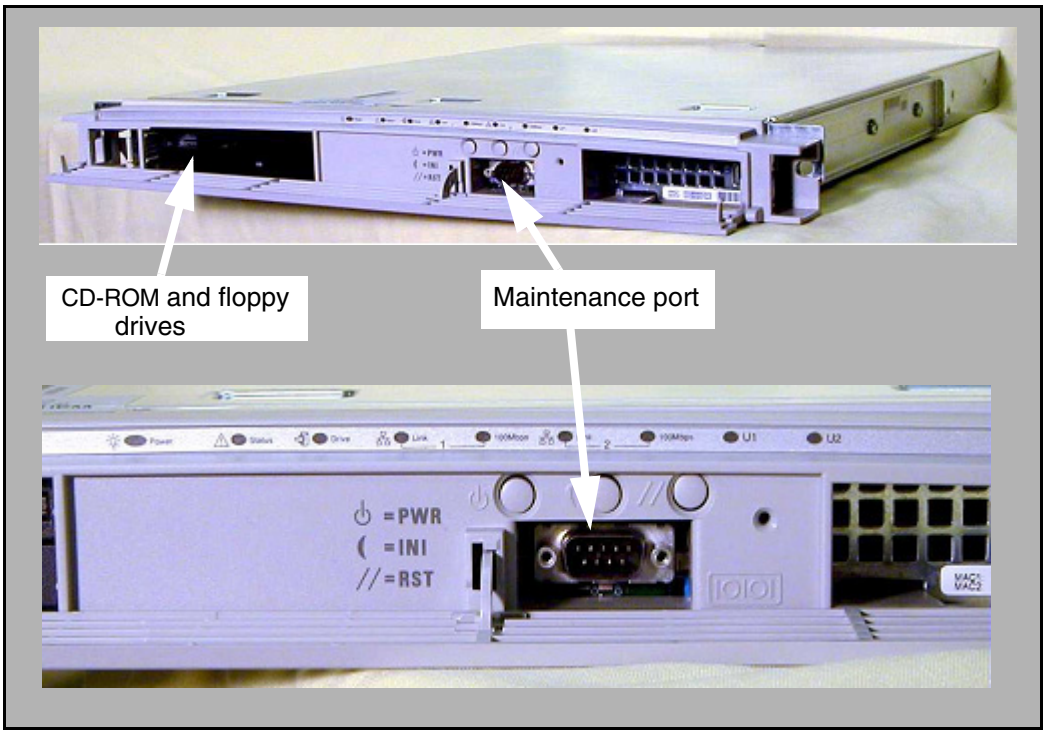
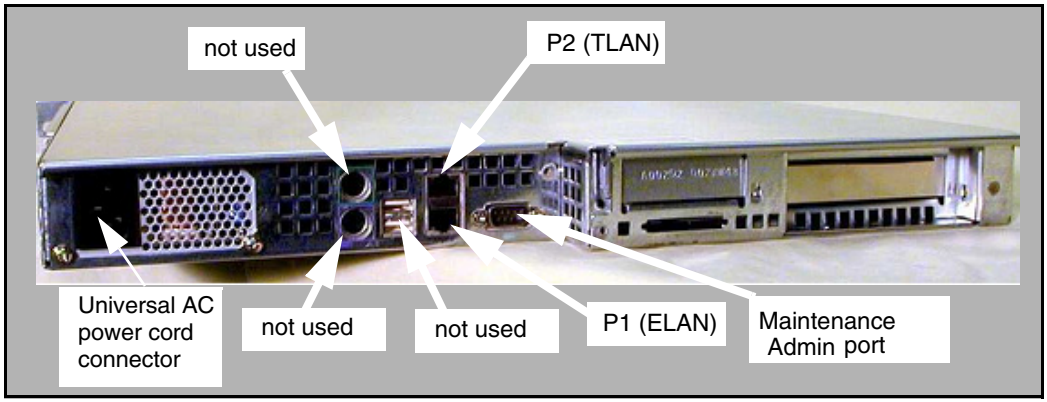


Figure 3 on page 89 shows the cable connectors on the back of the Succession Signaling Server.

Figure 3
Connectors on the back of the Succession Signaling Server



Connectors (rear)

The AC power cord connector is at the back of the Succession Signaling Server on the left side.

The P2 (TLAN) port connects the Succession Signaling Server to a Layer 2 Switch port on the TLAN subnet.

The P1 (ELAN) port connects the Succession Signaling Server to a Layer 2 Switch port on the ELAN subnet.

The maintenance port connects the Succession Signaling Server to maintenance and administration terminals.

There are three unused ports. Do not plug any device into these ports.

Software applications

The following software components operate on the Succession Signaling Server:

- Internet Telephone Terminal Proxy Server (TPS)
- H.323 WAN Gateway Signaling software (Virtual Trunk)

- Gatekeeper software
- Element Manager Web server

Internet Telephone Terminal Proxy Server

The Terminal Proxy Server (TPS) provides the signaling interface for the Internet Telephones. The TPS supports a maximum of 10,000 Internet Telephones on each Succession Signaling Server. In conjunction with the Call Server, the TPS delivers a full suite of telephone features.

The Unified Network IP Stimulus protocol (UNIStim) is the single point of contact between the various server components and the Internet Telephone. UNIStim is the stimulus-based protocol used for communication between an Internet Telephone and a Terminal Proxy Server on the Voice Gateway Media Card.

IP Peer Networking supports the i2002 and i2004 Internet Telephones and the i2050 Software Phone (soft client) for IP telephony. Each Internet Telephone can be configured through the Dynamic Host Configuration Protocol (DHCP) to register with a Call Server for feature control.

The TPS on the Succession Signaling Server also manages the firmware for the Internet Telephones which are registered to it. Accordingly, the TPS also manages the updating of the firmware for those Internet Telephones. For more information on upgrading the firmware see *IP Line: Description, Installation, and Operation* (553-3001-365) and *Branch Office* (553-3001-214).

H.323 WAN Gateway Signaling software (Virtual Trunk)

H.323 is a protocol standard that specifies the components, protocols, and procedures that provide multimedia communication services over packet networks.

The H.323 WAN Gateway Signaling software (Virtual Trunk) provides the industry-standard H.323 signaling interface to H.323 WAN Gateways. This software uses a Gatekeeper to resolve addressing for systems at different sites.

The H.323 WAN Gateway supports direct, end-to-end voice paths using Virtual Trunks with the following benefits:

- elimination of multiple IP Telephony to circuit-switched conversions
- improved voice quality
- simplified troubleshooting
- interoperability

Gatekeeper software

The IP Peer Networking feature provides a Gatekeeper where all systems in the network are registered.

The Gatekeeper software provides telephone number to IP address resolution. Since all systems in the network are registered to the Gatekeeper, this eliminates the need for manual configuration of IP addresses and numbering plan information at every site. As a result, it also eliminates the duplication of numbering plan information among sites. However, static registration and manual configuration are still supported for backward compatibility.

For more information about the Gatekeeper, refer to “Gatekeeper” on page 153.

Element Manager web server

The Element Manager web server functions on the Succession Signaling Server platform. Use the web browser interface in conjunction with Optivity Telephony Management (OTM) and the Command Line Interface (CLI) to configure and maintain the elements in the Succession 1000 and Succession 1000M systems.

For more information on Element Manager, refer to *Succession 1000 Element Manager: System Administration* (553-3001-332).

Redundancy

To provide redundancy in the event the Succession Signaling Server fails, install an additional Succession Signaling Server. A redundant Succession Signaling Server also provides load-sharing for the TPS.

The Gatekeeper (Primary, Alternate, or Failsafe) must reside on the Leader Succession Signaling Server. In the event of Leader Succession Signaling Server failure, the Follower Succession Signaling Server assumes the role of the Leader Succession Signaling Server.

The following is the sequence of events in the event of Follower Succession Signaling Server failure:

1 The Internet Telephones are distributed between the two Succession Signaling Servers (load-sharing). The H.323 WAN Gateway runs on the Leader Succession Signaling Server.

2 The Leader Succession Signaling Server fails.

3 The Follower Succession Signaling Server takes on the role of the Leader Succession Signaling Server and acquires the Leader Succession Signaling Server's IP address if necessary.

4 The Time To Live (TTL) of the Internet Telephones that were registered with the failed Succession Signaling Server expires. This causes those Internet Telephones to reset and register with the new Leader Succession Signaling Server.

Note: Only the Internet Telephones registered with the failed Succession Signaling Server are reset.

5 The new Primary Succession Signaling Server assumes responsibility for the H.323 WAN Gateway.

6 Normal operation resumes.

Note: The same functionality is available without a redundant Succession Signaling Server. Voice Gateway Media Cards in other Succession Media Gateways can assume a TPS role and become a source for Internet Telephone registration.

Hardware installation

This section describes how to install the Succession Signaling Server in a 19-inch rack, and connect it to the ELAN and TLAN.

Materials required

To install the Succession Signaling Server, obtain the following items:

- the Succession Signaling Server

  Note: Save the packaging container and packing materials in case you must reship the product.

- the power cable for the Succession Signaling Server. Check that the power cord is the exact type required in the host region. Do not modify or use the supplied AC power cord if it is not the correct type
- the serial cable for the Succession Signaling Server
- the Ethernet cables for networking
- the contents of the accessories pouch to install the Succession Signaling Server in a 19-inch rack. The accessories pouch should contain the following items:

  — two chassis support brackets (A)

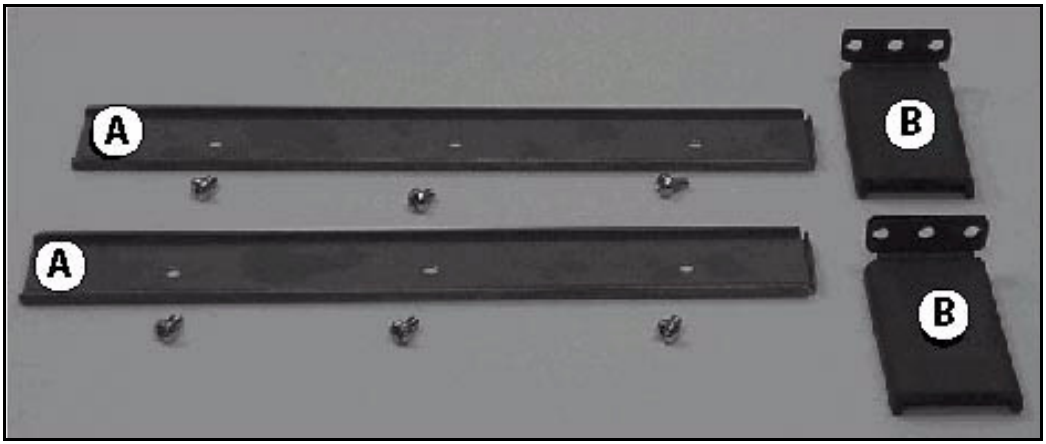
  — two rack-mounting brackets (B)

  — six rack-mount bracket screws (10-25 x 1/4” panhead Phillips)

  — two bezel door long rack-mount screws.

  Refer to Figure 4. If any parts are missing, contact your supplier immediately.

Figure 4
Succession Signaling Server brackets



CAUTION
The load rating for this mounting kit is 50 pounds (23 kilograms). If you exceed this limit, damage or injury can occur.

Preparing for rack mounting

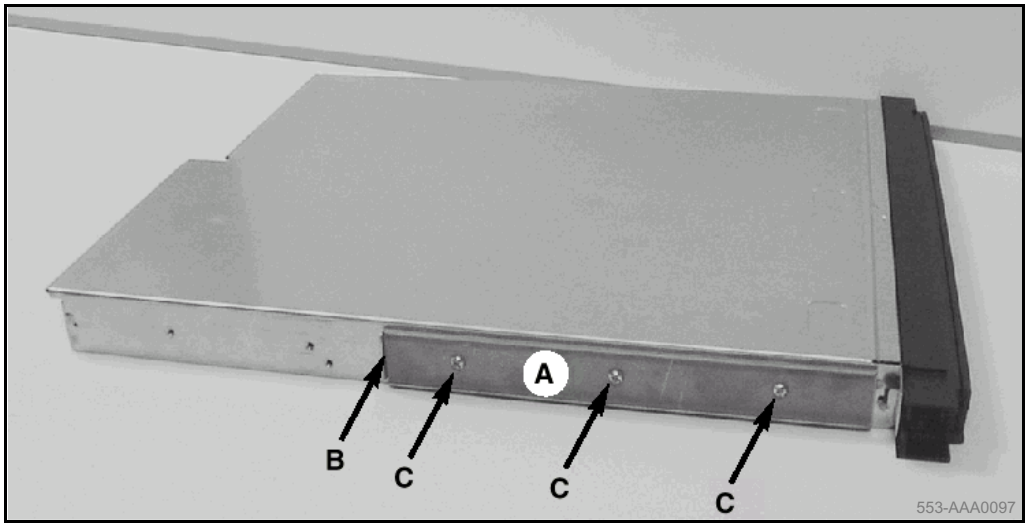
Procedure 2
Preparing the Succession Signaling Server for rack mounting

Note: The Front Mount Bracket assembly is not intended for use as a slide rail system. The Succession Signaling Server must be firmly attached to the rack.

1 Make sure the Succession Signaling Server is not plugged-in to an electrical outlet.

2 Align the end of the rail with the flange (B) toward the back of the Succession Signaling Server. See Figure 5 on page 95.

Figure 5
Chassis support bracket



3 Align the screw holes in the rack-mount rail to the mating holes in the side of the Succession Signaling Server chassis. Use three screws (C) on each side.

Note: Hand-tighten the screws to prevent cross-threading, then use a Phillips screwdriver to secure them.

4 Attach the bezel door to the faceplate of the Succession Signaling Server, as shown in Figures 6 and 7 on page 96.

Figure 6
Left hinge mount

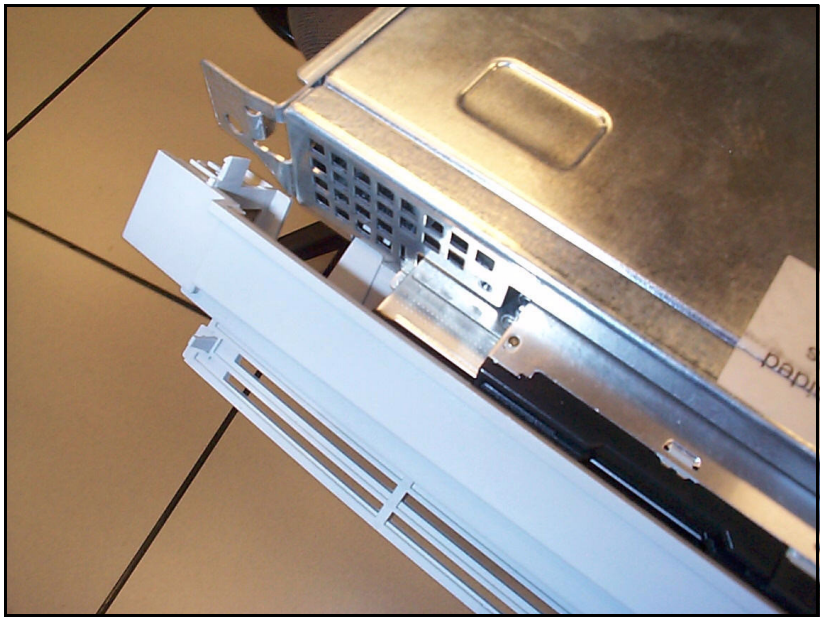
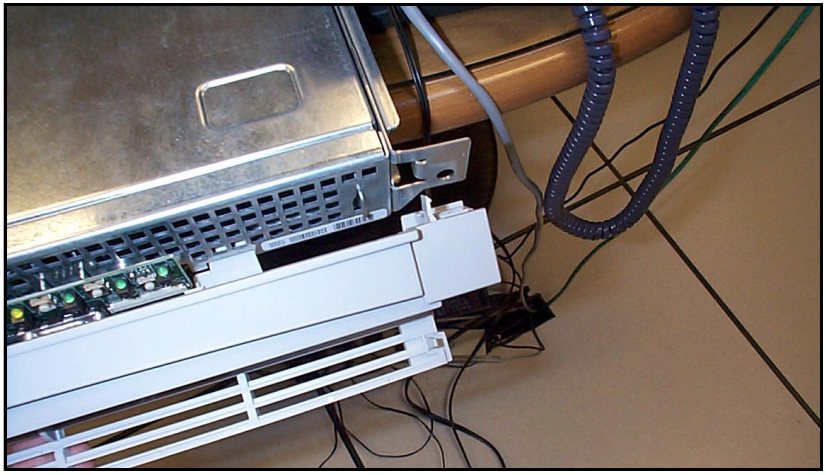
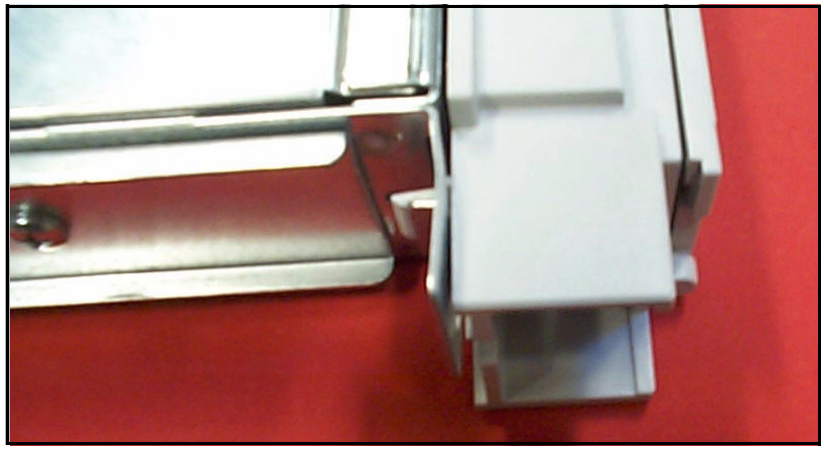


Figure 7
Right hinge mount



When the door is attached to the Succession Signaling Server and rack-mount apparatus, it should appear as shown in Figure 8.

Figure 8
Snapped-in bezel door



End of Procedure

Rack mounting

Read the following warnings carefully before installing the Succession Signaling Server in the rack.

DANGER OF ELECTRIC SHOCK
DISCONNECT AC POWER

Make sure the server is completely disconnected from any ac power source before performing this procedure. Pressing the Power button DOES NOT turn off power to this server. Some circuitry in the server can continue to operate even though the front panel Power button is off. Failure to disconnect the server from its ac power source can result in personal injury or equipment damage.

DANGER OF ELECTRIC SHOCK
GROUNDING THE RACK INSTALLATION

To avoid the potential for an electrical shock hazard, include a third wire safety grounding conductor with the rack installation. If server power cords are plugged into ac outlets that are part of the rack, then provide proper grounding for the rack itself. If server power cords are plugged into wall ac outlets, the safety grounding conductor in each power cord provides proper grounding only for the server. Provide additional, proper grounding for the rack and other devices installed in it.

WARNING
MAIN AC POWER DISCONNECT

You must install an ac power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server(s).

Damage to Equipment
OVERCURRENT PROTECTION

The server is designed for an AC line voltage source with up to 20 amperes (A) of over-current protection. If the power system for the equipment rack is installed on a branch circuit with more than 20 A of protection, provide supplemental protection for the server. If more than one server is installed in the rack, the power source for each server must be from a separate branch circuit.

Procedure 3
Rack-mounting the Succession Signaling Server

1 Attach the rack-mount brackets (‘B’ as shown in Figure 4 on page 94) to the equipment rack. Install the left and right side at an equal height. Use standard length screws from the accessories pouch, and screw them into the top and bottom drill holes of the bracket.

Figure 9
Installed rack-mount bracket

2 When both brackets are fixed in place, do the following:

a. Align the rack-mount brackets on the Succession Signaling Server with the slide rail system on the rack posts. Refer to Figure 10 on page 100.

b. Slide the Succession Signaling Server in place.

Refer to Figure 10 on page 100.

Figure 10
Rack-mounting the Succession Signaling Server

3 Tighten the screws through the faceplate of the Succession Signaling Server to the rack-mount bracket.

Note: Do not apply excessive torque while tightening the bolts. The bezel door is plastic and does not require or withstand overtightening.

End of Procedure

Connecting and powering up the Signaling Server

WARNING
Do not modify or use a supplied ac power cord if it is not the exact type required in the region where the Succession Signaling Server is installed and used.

Be sure to replace the cord with the correct type.

In geographic regions that are susceptible to electrical storms, Nortel Networks recommends that you plug the Succession Signaling Server into an ac surge suppressor.

Procedure 4
Connecting and powering up the Signaling Server

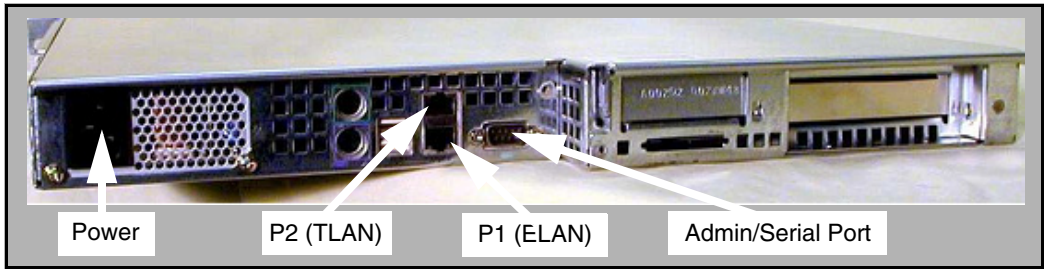
1 Connect the Succession Signaling Server to the TLAN subnet.

Insert the RJ-45 Category 5 (or better) TLAN Ethernet cable into the P2 (TLAN) port on the back of the Succession Signaling Server. The P2 (TLAN) port is the top of the two Ethernet ports shown in Figure 11.

2 Connect the Succession Signaling Server to the ELAN subnet.

Insert the RJ-45 Category 5 (or better) ELAN Ethernet cable into the P1 (ELAN) port. The P1 (ELAN) port is the bottom of the two Ethernet ports shown in Figure 11.

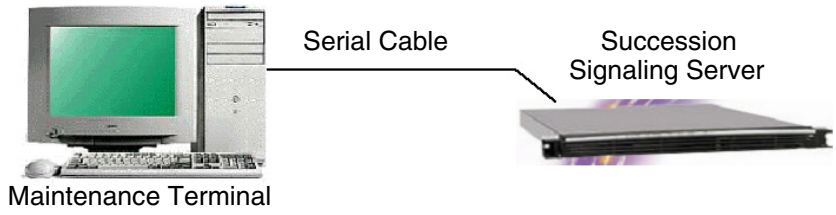
Figure 11
Succession Signaling Server ELAN and TLAN connectors



3 Connect a maintenance terminal to the Succession Signaling Server.

a. Connect a DTE–DTE null modem serial cable (supplied with the Succession Signaling Server) from the serial port on the back of the Succession Signaling Server (see Figure 11) to a maintenance terminal. The connection looks like that shown in Figure 12 on page 102.

Figure 12
Maintenance terminal to Succession Signaling Server connection



b. Set the COM port on the maintenance terminal as follows:

- Terminal type: VT100
- Speed: 19 200
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

Note: The Succession Signaling Server ships with the Admin/Serial port set to 19 200 Bit/s. Other available speeds are 9600, 38 400, and 115 200 Bit/s. Once the Succession Signaling Server software has been installed, the port speed can be changed using the Tools Menu on the Succession Signaling Server Install Tool. See Procedure 9 on page 133.

4 Set up the maintenance terminal.

The maintenance terminal can be set up any time, except during data transmission. Do not configure the terminal during data transmission to avoid data loss.

a. Turn on the power for the maintenance terminal.

b. Enter setup mode by pressing the <**SETUP**> key located on the top row of the special function keys. The terminal screen displays the current setup values.

c. Change the value in each field on each setup screen as necessary. Use the keys listed in Table 18 on page 103 to view and change setup values.

Table 18
SDI key function

Key	Function
Arrow key	Move from field to field
<Enter>	Scroll through possible values or cause requested action to occur (depends on type of field)
<Next Screen>	Move to next setup screen
<Prev Screen>	Move back to last screen

d. Save changes by returning to the *General setup* screen, moving the cursor to the Saved field, and pressing *<Enter>*.

To configure the maintenance terminal, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

5 Connect the Succession Signaling Server power cord.

a. Check that the power cord is the type required in the region where the Succession Signaling Server is used.

Do not modify or use the supplied ac power cord if it is not the correct type. Refer to in *Succession 1000 System: Installation and Configuration* (553-3031-210) for a detailed power cord description.

b. Attach the female end of the power cord to the mating AC power receptacle on the left side of the Succession Signaling Server's back panel. See Figure 11 on page 101. Plug the male end of the AC power cord into the AC power source (wall outlet).

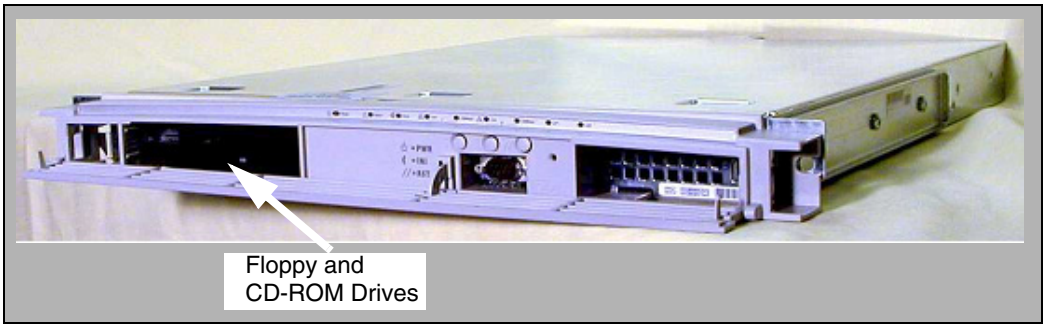
6 Power up the Succession Signaling Server.

a. Open the bezel door (Figure 13 on page 104) to access the Power switch:

i. Grasp the tab at each end of the hinged bezel door.

ii. Gently pull the tabs out and down to open the hinged bezel door.

Figure 13
Succession Signaling Server with open bezel door



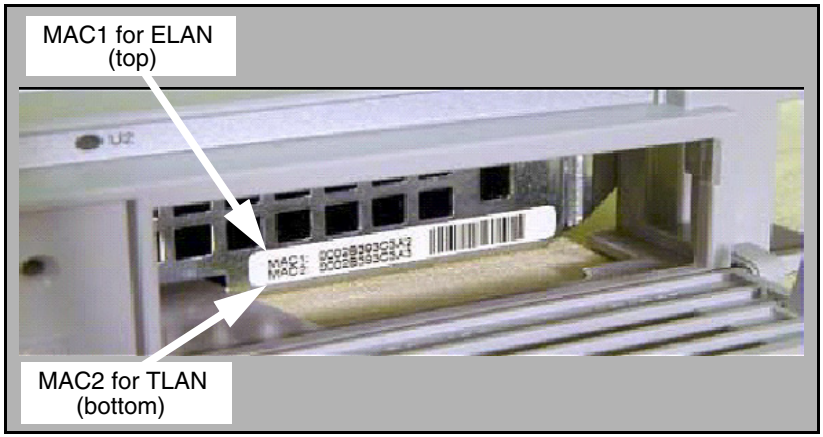
Note 1: The MAC addresses are visible on the lower right-hand side when the bezel door is open. See Figure 14.

Note 2: MAC1 is Port 1 for ELAN, and MAC2 is the Port 2 for TLAN.

Note 3: Though the MAC1/ELAN address is the top address, Port 1 is the bottom Ethernet port on the back of the Succession Signaling Server.

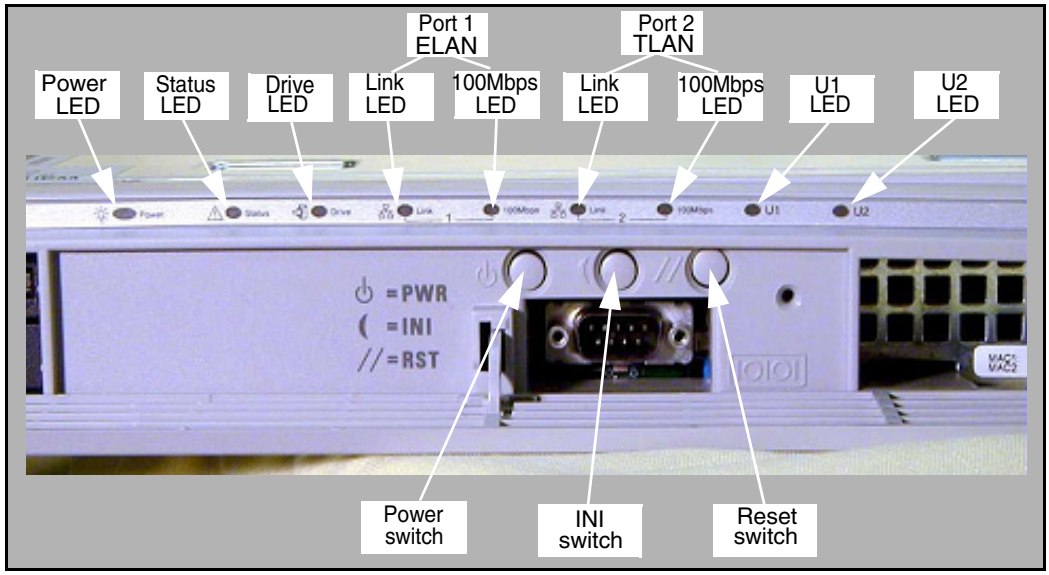
Note 4: Figure 15 on page 105 shows the LEDs that correspond to these connections.

Figure 14
MAC address



b. Press the Power switch (Figure 15). Notice that the green LED power indicator is lit.

Figure 15
Succession Signaling Server indicators and power switch



The Succession Signaling Server LED indicators show the following:

- Power—Green LED on, power on; LED off, power off
- Status—Red LED off, CPU running; LED on, CPU halted
- Drive—Green LED flashing, Hard Drive or CD ROM Drive active
- Link—Green LED, Ethernet port active
- 100 Mbps—Green LED on, Ethernet port running at 100 Mbps; LED off, Ethernet port running at 10 Mbps

Note: When the power is turned off on a Succession Signaling Server, the two Link LEDs for Port 0 and Port 1 continue to flash. Depress the Power button for approximately seven seconds to completely turn the power off.

7 Refer to the Succession Signaling Server Product Guide on the resource CD-ROM shipped with the Succession Signaling Server for additional operating information.

End of Procedure

Software installation

This section describes the Succession Signaling Server Install Tool and explains how to install Succession Signaling Server software and perform basic configuration.

Software for the Succession Signaling Server is installed using the Install Tool, which runs from the Succession Signaling Server Software CD-ROM. The Install Tool program also upgrades existing Succession Signaling Server software to the latest version.

> ***Note:*** The Succession Signaling Server is out-of-service during software installation or upgrade.

To perform a software installation or upgrade, reboot the Succession Signaling Server with the Software CD-ROM in its drive. No floppy disk is required, since the software CD-ROM is bootable.

The Install Tool installs all software, including the operating system, applications, and Web files. The Install Tool also copies software files for the Voice Gateway Media Cards and Internet Telephones, which are used to upgrade these components. For a new Succession Signaling Server, the Install Tool prompts for IP Telephony parameters to perform basic system configuration.

After the Succession Signaling Server software is installed, further system configuration is performed using Element Manager.

Materials required

The following items are required to install the software:

- A power cable and serial cable (provided with the Succession Signaling Server hardware), and Ethernet cables for networking

- The Succession Signaling Server Software CD-ROM. Order or download the CD-ROM image from the Nortel Networks Electronic Software Download site. Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for instructions on downloading the image.

Creating the Succession Signaling Server CD

A single ".iso" file is provided to create the Software CD. This file is a ready-to-burn ISO9660 CD image that creates a bootable CD that is compliant with the El Torito specification. You must use CD writer software that can create a CD from this image. As the CD image is pre-configured, your software automatically creates a bootable Software CD. Refer to the software's help pages to create a CD from an ISO file. Also review the associated README file that is associated with the Nortel Networks Succession Signaling Server Software download.

Procedure 5
Creating a Succession Signaling Server software CD-ROM

1 Use the software option to "burn" or "create" a CD from the CD image. Do not drag-and-drop, as this can result in a file copy and a CD-ROM that does not work. Do not write the ISO file to the CD-ROM.

Note: Select the disk-at-once write option.

2 Close the session.

3 Label the CD appropriately, for example, Succession Signaling Server, sse-x.xx.xx.

End of Procedure

The Software CD must be readable in a standard CD-ROM drive. After you create a CD from the CD image, the CD contains several directories and files. If you cannot create a CD, refer to the CD writer's software documentation.

Installing the software

Before proceeding, you must complete Procedure 4 "Connecting and powering up the Signaling Server" on page 101.

Procedure 6
Installing the Succession Signaling Server software

After you complete step 1 below, this procedure takes approximately 15 minutes.

1 From your Planning and Engineering group, obtain the following network and IP Telephony data for this Succession Signaling Server:

- node ID for the IP Telephony node
- node IP address for the IP Telephony node
- hostname for the Succession Signaling Server
- ELAN IP address, subnet mask, and gateway
- TLAN IP address, subnet mask, and gateway
- ELAN IP address of the Succession Call Server
- Gatekeeper role (refer to *IP Peer Networking* (553-3001-213) for details on the Gatekeeper)
- Primary and Alternate Gatekeeper IP addresses for this networked system (refer to *IP Peer Networking* (553-3001-213))

2 Insert the Software CD-ROM into the Succession Signaling Server CD-ROM drive, and press the RST button on the front panel to cold-reboot the Succession Signaling Server.

Note: The Software CD-ROM should be bootable. If not, create a boot floppy using the files in the `/mkboot` directory on the Succession Signaling Server Software CD-ROM.

3 If this a software upgrade or a re-installation on an existing system, observe the boot sequence. Enter ‘c’ at the boot menu shown in Figure 16 on page 109.

Note: Entering ‘c’ at the “ISP 1100 Boot” banner speeds up this process, as the keyboard input is buffered.

Figure 16
Upgrade boot sequence

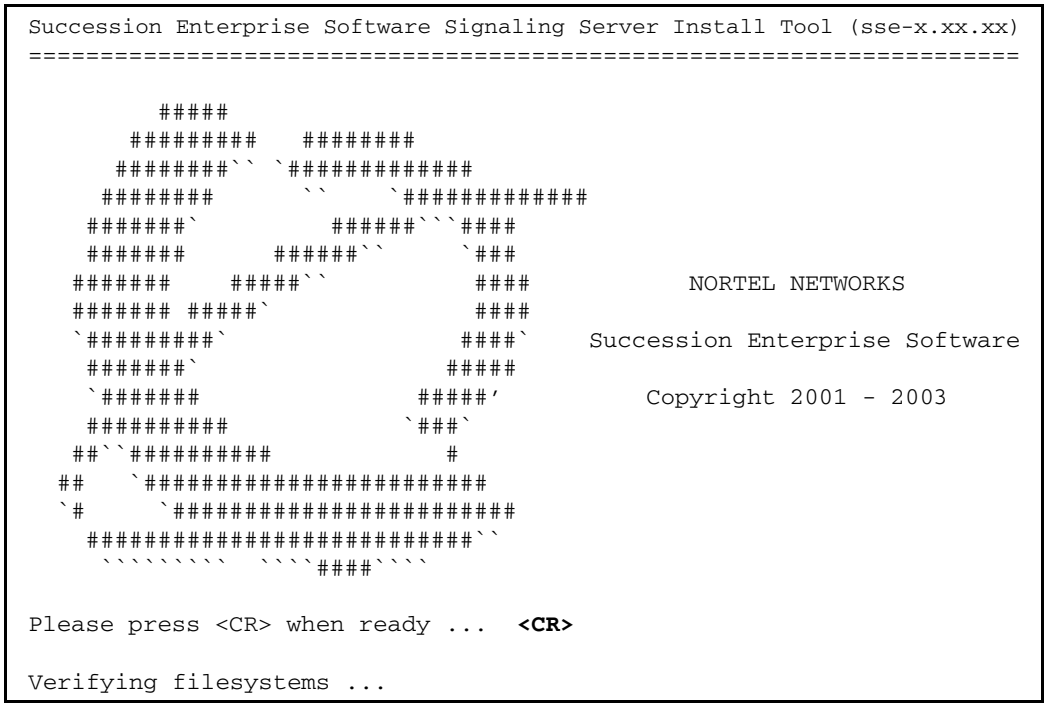
```
        ISP 1100 Boot
Copyright 2003 Nortel Networks, Inc.

CPU: PC PENTIUM
Version: x
BSP version: 1.2/0
Creation date: May 31 2002, 15:44:38
ataDrv 1.0: ATAPI Drive Found
Controller 1 drive 0
Controller 1 drive 1
ATAPI Controller 1 #drives found = 1
Read boot parameters from:
[C]DROM
[H]ard Disk
5 [H]
```

If you do not enter ‘c’ within the 5-second time-out, the Succession Signaling Server boots to the existing software on the hard disk.

4 When the Install Tool banner appears (Figure 17 on page 110), press <CR> to perform system checks and begin software installation.

Figure 17
Install Tool banner screen



The system verifies the file systems.

- When the software runs for the first time on a new system, the hard disk will not be partitioned, so the test normally fails. Upon failure, the menu in Figure 18 on page 111 appears.

Figure 18
First boot of a new system

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The filesystems verification failed! (This is normal for a new
system.)

The hard disk must be (re)partitioned and (re)initialized. This will
erase all data on the hard disk. The system will then reboot and
the Install Tool will restart.

        Please enter:
<CR> -> <a> - Partition and initialize the hard disk, then reboot.

        Enter Choice> a
```

a. Enter ‘a’ to start the new installation.

The system displays the messages:

```
Partitioning hard disk ...
Hard disk partitioning succeeded.

Creating filesystems ...
Filesystems creation succeeded.

Rebooting system ...
```

b. The Install Tool banner screen (Figure 17 on page 110) reappears. Press <CR> to verify the filesystems.

The disk check reports:

```
Filesystems verification succeeded.
```

c. Confirm or enter the date and time (Figure 19 on page 112).

Figure 19
Date and time

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
=========================================================================

You should ensure the system date and time are correct prior to
installation, since all files copied or created during install will
be time-stamped.

If the date or time are correct, you can press <CR> to accept the
current values.

Current date is: WEDNESDAY 13-02-2002
Enter new date (dd mm yyyy): 17 01 2002
Date is set to: FRIDAY 17-01-2002
Current time is: 09:47:18
Enter new time (hh mm ss): 08 38 30
Time is set to: 08:38:30
Current date and time is:
FRIDAY 17-01-2001, 08:38:30
```

- When reinstalling the software on an existing system, the system verifies the file systems. The disk check reports:

  ```
  Filesystems verification succeeded.
  ```

  The system summary appears (Figure 20 on page 113). Enter ‘a’ to continue the installation.

Figure 20
System Summary

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

            ----------------------------------------
                        SYSTEM INFORMATION
            ----------------------------------------

+==============================================================+
|  Hostname: SS_Node276_Ldr          S/W Ver: x.xx.xx          |
|                                                              |
|      Role: Leader                  Set TPS: Enabled          |
|   Node ID: 276                    Vtrk TPS: Enabled          |
|   Node IP: 192.168.20.100           GK Svc: None             |
|  H.323 ID: SS_Node276_Ldr            CS IP: 192.168.10.10    |
|                                                              |
|   ELAN IP: 192.168.10.20           TLAN IP: 192.168.20.20    |
|   ELAN SM: 255.255.255.0           TLAN SM: 255.255.255.0    |
|   ELAN GW: 192.168.10.1            TLAN GW: 192.168.20.1     |
|  ELAN MAC: 00:02:b3:c5:51:c6      TLAN MAC: 00:02:b3:c5:51:c7|
+==============================================================+

        Please enter:
<CR> -> <a> - Continue with Install Tool.
        <q> - Quit.

        Enter Choice>
```

5 Test the disk.

- If the hard drive has never been tested or is corrupt, enter ‘a’ at the menu shown in Figure 21 on page 114.

Figure 21
Hard disk test

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The Install Tool cannot determine when the hard disk was last tested.

The hard disk must be tested before installation can continue.
This test will take approximately 14 minutes.


        Please enter:
<CR> -> <a> - Test the hard disk.

        Enter Choice> a
```

- If the hard disk has not recently been tested, enter ‘a’ at the menu shown in Figure 22.

Figure 22
Not recently tested

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The Install Tool has detected that the hard disk has not been tested
recently.

It is recommended to test the hard disk now. This test will take
approximately 14 minutes.

        Please enter:
<CR> -> <a> - Test the hard disk.
        <b> - Skip the hard disk test.

        Enter Choice> a
```

- If the hard disk has been checked in the last 24 hours, enter ‘a’ at the menu shown in Figure 23 on page 115.

Figure 23
Tested within 24 hours

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The Install Tool has detected that the hard disk has been tested
recently.

It is recommended to skip the hard disk test.

If you select to test the hard disk anyway, it will take
approximately 14 minutes.

        Please enter:

<CR> -> <a> - Skip the hard disk test.
        <b> - Test the hard disk.
         Enter Choice> a
```

The following messages print out:

```
Testing hard disk ...
Testing partition /u (4194241 blocks) ...

xxx% complete

Testing partition /p (4194241 blocks) ...
xxx% complete

Hard disk testing succeeded.
```

where xxx = 0 to 100.

Note: If the physical check did not pass, contact your technical support group.

Figure 24
Install Tool Main Menu

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

                        M A I N    M E N U

The Install Tool will install Signaling Server software and related
files. You will be prompted throughout the installation.

        Please enter:
<CR> -> <a> - To perform a complete installation/upgrade (Signaling
              Server s/w, Internet Telephone f/w, Media Card l/w,
              basic Signaling Server configuration).
        <b> - To install/upgrade Signaling Server software only.
        <c> - To copy Internet Telephone firmware only.
        <d> - To copy Media Card loadware only.
        <e> - To perform basic Signaling Server configuration only.
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice>
```

6 At the Main Menu (Figure 24), enter ‘a’ to install Succession Signaling Server software. Option ‘a’ performs options b, c, d, and e.

The following sample lines output to the screen:

```
Copying "/cd0/sse30047.p3/disk.sys" to "/u/disk.sys".
Processing the install control file ...
"/cd0/sse30047.p3/install.dat" parsed.
```

The screen shown in Figure 25 on page 117 shows actions that can be performed.

Figure 25
Installation Status

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

        ------------------------------------------------
                    INSTALLATION STATUS SUMMARY
        ------------------------------------------------

+=================+========+========+==============================+
|     Option      | Choice | Status |           Comment            |
+=================+========+========+==============================+
| software        |  yes   |        | new install x.xx.xx          |
+-----------------+--------+--------+------------------------------+
| firmware        |  yes   |        | copy ALL                     |
+-----------------+--------+--------+------------------------------+
| loadware        |  yes   |        | copy ALL                     |
+-----------------+--------+--------+------------------------------+
| configuration   |  yes   |        | set as N/A                   |
+-----------------+--------+--------+------------------------------+

        Please enter:
<CR> -> <y> - Yes, start complete installation.
        <n> - No, cancel complete installation and return to the Main
              Menu.

        Enter Choice>
```

7 Enter ‘y’ to start the installation. The screens shown in Figures 26 to 30, which start on page 118, appear.

Figure 26
Installation output

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

You have selected to install version 3.00.xx on the system. As
this is a new install, all necessary directories and files will
be created on the hard disk.

Starting new install of version 3.00.xx.

Initializing protected partition ...
"/p" initialized.

Creating directory ... (many directories are created here) ...
Copying ... (many files are copied here) ...

Boot ROM "/p/load/bootrom.bin" installed.
```

Figure 27
Success

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

Software version 3.00.xx was installed successfully.

All files were copied to the hard disk.
```

Figure 28
Internet Telephone firmware

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The installation source contains multiple Internet Telephone firmware
files.

Copying "/cd0/0602Bxx.bin" to "/u/fw/0602Bxx.bin".
Copying "/cd0/0603Bxx.bin" to "/u/fw/0603Bxx.bin".
```

Figure 29
VGMC loadware

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

The installation source contains multiple Voice Gateway Media Card
loadware files.

Copying "/cd0/IPL3xxxx.p2" to "/u/fw/IPL3xxxx.p2".
Copying "/cd0/IPL3xxxx.sa" to "/u/fw/IPL3xxxx.sa".
```

8 If this is an upgrade, existing Succession Signaling Server configuration files are retained.

The system echoes the ELAN MAC address.

```
For future reference, the ELAN MAC address is:
"00:02:b3:c5:5l:c6".
```

This address is on the face of the Succession Signaling Server, on the right-hand side when the bezel door is open. See Figure 14 on page 104.

Note: The ELAN MAC address must be configured in the Element Manager node configuration page.

Go to step 17 on page 126 to complete the installation.

9 If this is a new installation, set the Succession Signaling Server as Leader or Follower. See Figure 30.

- If there is not already a Leader Succession Signaling Server in the IP Telephony node, enter ‘a’ at the prompt to set this Succession Signaling Server as Leader.
- If there is already a Leader Succession Signaling Server in the IP Telephony node, enter ‘b’ at the prompt to set this Succession Signaling Server as Follower. Then go to step 15 on page 124. Figure 36 on page 125 appears.

For more information about Leader and Follower Succession Signaling Servers, see *Succession 1000 System: Overview* (553-3031-010) and *IP Line: Description, Installation, and Operation* (553-3001-365).

Figure 30
Leader/Follower Succession Signaling Server configuration

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================


In this step, you define the role of this Signaling Server.

If you set this Signaling Server as a Leader, then data networking
and IP Telephony parameters must be entered now. (This will pre-
configure the IP Telephony node files.)

If you set this Signaling Server as a Follower, then data networking
and IP Telephony parameters must be configured through Element
Manager.

NOTE: This will over-write all existing data network and IP
      telephony configuration on this Signaling Server.

        Please enter:
<CR> -> <a> - Set this Signaling Server as a Leader.
        <b> - Set this Signaling Server as a Follower.
        <q> - Quit.

        Enter Choice>
```

Figures 32 and 33 on page 122 show required configuration data. These screens appear one after the other.

10 Configure the node IP using the TLAN IP and a node ID. The IP information is for a temporary IP Telephony node. This ensures the existing node is not impacted. This pre-configures the IP Telephony node files.

Note: IP addresses shown in Figures 32 and 33, and Figure 37 on page 126 are examples.

Figure 31
Leader Succession Signaling Server

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

Please define the data networking and IP Telephony parameters for
this Leader Signaling Server now.

Node ID          : 276

Hostname         : SS_Node276_Ldr

ELAN IP          : 192.168.10.20
ELAN subnet mask: 255.255.255.0
ELAN gateway IP : 192.168.10.1

TLAN IP          : 192.168.20.20
TLAN subnet mask: 255.255.255.0
TLAN gateway IP : 192.168.20.1

Node IP          : 192.168.10.20
```

11 Enter the ELAN IP address at the Call Server IP prompt. See Figure 32 on page 122.

- If installing the Succession Signaling Server in an office that is not a Branch Office, enter the ELAN IP address of the Succession Call Server.
- If installing the Succession Signaling Server in a Branch Office, enter the ELAN IP address of the Branch Office H.323 WAN Gateway.

Figure 32
Succession Call Server ELAN IP

```
 Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
 ========================================================================

 If you know it, please enter the ELAN address of the Succession
 Call Server that this IP Telephony node will register to.

 Call Server IP  : 192.168.10.10
```

12 Select the Gatekeeper Service to be provided by this Succession Signaling Server. See Figure 33 on page 123.

- If there is a Primary and Alternate Gatekeeper in the network, enter ‘a’ to configure this Succession Signaling Server as a Failsafe Gatekeeper.
- If this Succession Signaling Server will be the Primary Gatekeeper, enter ‘b’.
- If this Succession Signaling Server will be the Alternate Gatekeeper, enter ‘c’.
- If this Signaling Server will not run the Gatekeeper application, enter ‘d’.
- If network information is unknown, enter ‘d’.

Refer to *IP Peer Networking* (553-3001-213) for more information on the Gatekeeper.

Figure 33
Gatekeeper type

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================


Please select the Gatekeeper service that this Signaling Server
will provide.


        Please enter:
<CR> -> <a> - Failsafe Gatekeeper.
        <b> - Primary Gatekeeper.
        <c> - Alternate Gatekeeper.
        <d> - No co-resident Gatekeeper.

        Enter Choice>
```

13 Enter the Primary Gatekeeper IP address, the Alternate Gatekeeper IP address, or both, depending on the option entered in step 12 on page 122. See Figure 34.

- If option ‘a’ was entered in step 12, you must enter the addresses of the Primary Gatekeeper and the Alternate Gatekeeper.
- If option ‘b’ was entered in step 12, you can enter the address of the Alternate Gatekeeper.
- If option ‘c’ was entered in step 12, you must enter the address of the Primary Gatekeeper.
- If option ‘d’ was entered in step 12:
  - — If this Succession Signaling Server will not run the Gatekeeper application, the Primary Gatekeeper address is optional. If it is entered, the address of the Alternate Gatekeeper is prompted, but it is also optional.
  - — If network information is unknown, do not enter an address.

The Gatekeeper configuration can be updated at any time using Element Manager.

Figure 34
Gatekeeper IP addresses

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

If you know them, please enter the addresses of the Gatekeepers that
this IP Telephony node will register to.

Primary GK IP   :
Alternate GK IP :
```

14 Enter ‘a’ to configure the Succession Signaling Server to run the Gatekeeper, TPS, and Virtual Trunks. See Figure 35 on page 124. Go to step 16 on page 125.

Figure 35
Succession Signaling Server application configuration

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

Please select the application configuration for this
Gatekeeper.

        Please enter:
<CR> -> <a> - Co-resident (GK + TPS + VTRK).
        <b> - Standalone (GK only).

Enter Choice> a
```

15 If this is a Follower Succession Signaling Server, enter the hostname for the Follower from the menu in Figure 36 on page 125.

Figure 36
Follower Succession Signaling Server configuration

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

This Follower Signaling Server will obtain its data network and IP
telephony configuration from the Leader Signaling Server at boot.

To identify this Signaling Server, please enter a Hostname now.

Hostname : SS_Node276_Folwr
```

16 Confirm the parameters. The example in Figure 37 on page 126 is for a Leader Succession Signaling Server. A Follower Succession Signaling Server confirmation screen is similar, but only has the hostname parameter.

Note: The GK configuration parameter changes according to the GK service and application configuration that you select.

Figure 37
IP Telephony parameter configuration

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

You have entered the following parameters for this Leader
Signaling Server:

Node ID          : 276
Hostname         : SS_Node276_Ldr
ELAN IP          : 192.168.20.100
ELAN subnet mask: 255.255.255.0
ELAN gateway IP : 192.168.10.1
TLAN IP          : 192.168.20.20
TLAN subnet mask: 255.255.255.0
TLAN gateway IP : 192.168.20.1
Node IP          : 192.168.20.100
Call Server IP   : 192.168.10.10
GK configuration: No Gatekeeper
Primary GK IP    : 0.0.0.0
Alternate GK IP : 0.0.0.0

        Please enter:
<CR> -> <y> - Yes, these parameters are correct.
        <n> - No, these parameters are not correct.

  Enter Choice>
```

The system echoes the ELAN MAC address.

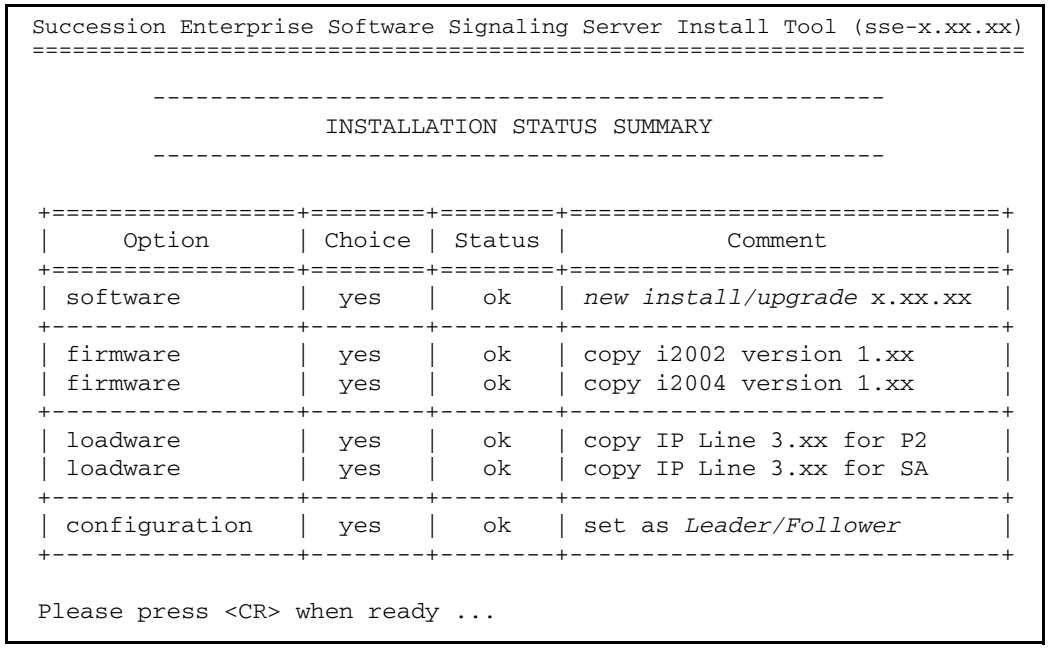
```
For future reference, the ELAN MAC address is:
"00:02:b3:c5:5l:c6".
```

This address is on the face of the Succession Signaling Server, on the right-hand side when the bezel door is open. See Figure 14 on page 104.

Note: The ELAN MAC address must be configured in the Element Manager node configuration page.

17 To complete the installation, the Installation Status Summary screen is displayed as shown in Figure 38 on page 127.

Figure 38
Installation Status Summary



```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

         ------------------------------------------------
                      INSTALLATION STATUS SUMMARY
         ------------------------------------------------

+=================+========+========+==============================+
|     Option      | Choice | Status |           Comment            |
+=================+========+========+==============================+
| software        |  yes   |   ok   | new install/upgrade x.xx.xx  |
+-----------------+--------+--------+------------------------------+
| firmware        |  yes   |   ok   | copy i2002 version 1.xx      |
| firmware        |  yes   |   ok   | copy i2004 version 1.xx      |
+-----------------+--------+--------+------------------------------+
| loadware        |  yes   |   ok   | copy IP Line 3.xx for P2     |
| loadware        |  yes   |   ok   | copy IP Line 3.xx for SA     |
+-----------------+--------+--------+------------------------------+
| configuration   |  yes   |   ok   | set as Leader/Follower       |
+-----------------+--------+--------+------------------------------+

Please press <CR> when ready ...
```

18 Exit to the Main Menu (Figure 24 on page 116). Enter ‘q’ at the Main Menu to quit the installation process. Figure 39 on page 128 appears. Enter ‘q’ again.

Figure 39
Quit

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================
You have selected to quit the Install Tool.
Before quitting and rebooting the system, remove all disks (floppy,
CDROM) from the drives.

        Please enter:
<CR> -> <m> - Return to the Main Menu.
        <q> - Quit and reboot the system.

        Enter Choice> q

Rebooting system ...
```

19 Remove the CD-ROM from the drive, and reboot the system.

Note: After software installation and reboot, a Follower Succession Signaling Server sends out BOOTP requests and waits for a response. Since the Follower Signaling Server is not yet configured, there is no BOOTP response. Do not wait for this response; go directly to "Adding a Follower Succession Signaling Server to a node" on page 131.

End of Procedure

After the software is installed and the Succession Signaling Server has rebooted, the Follower uses BOOTP requests to obtain network and node configuration data from the Leader.

Use Element Manager to ensure the Follower Succession Signaling Server is installed into the IP Telephony node (refer to *Succession 1000 System: Installation and Configuration* (553-3031-210)).

Logging in to the Succession Signaling Server

Use this procedure to log in to the vxWorks™ shell to access the Succession Signaling Server from a maintenance terminal.

Procedure 7
Logging in to the Succession Signaling Server

Before you begin, make sure the DTE–DTE null modem cable (supplied with the Succession Signaling Server) runs between the back port of the Succession Signaling Server and the maintenance terminal.

1 Make sure the Succession Signaling Server is powered up and connected to the maintenance terminal. Refer to Procedure 4 on page 101.

The Succession Signaling Server must boot successfully before the user can log in.

2 Press <**cr** > to invoke the login prompt.

3 Enter the login credentials.

Note: If the Succession Signaling Server has connected to the Succession Call Server (the startup messages indicate if the PBX link is up), use the PWD1 login to access the Succession Signaling Server.

a. Enter the default Succession Signaling Server Command Line Interface (CLI) login **admin.**

b. Enter the Succession Signaling Server Command Line Interface (CLI) password.

- If this Succession Signaling Server has just been installed and you are logging in for the first time, enter the default password **cseadmin.**

  The system immediately prompts you to change the default password.

- If this is not the first login to the Succession Signaling Server, enter the appropriate password.

  If you have forgotten the password, reset it from the Tools Menu (see Procedure 9 on page 133).

End of Procedure

To log out of the Succession Signaling Server, enter `exit` at the command line.

Verifying a successful configuration

To ensure that the Succession Signaling Server Ethernet connections are configured correctly (ELAN and TLAN), perform a ping test to one or more of the other devices connected to the network, particularly the Succession Call Server.

Procedure 8
Verifying the Succession Signaling Server Ethernet connection

1. Log in to the Succession Signaling Server, using Procedure 7 on page 129.
2. Ping the IP address of the Succession Signaling Server. Enter the command:

   `ping x.x.x.x`

   Where **`x.x.x.x`** is the Succession Signaling Server ELAN IP address.
3. Ping the IP address of the Succession Call Server. Enter the command:

   `ping x.x.x.x,3`

   Where **`x.x.x.x`** is the Succession Call Server ELAN IP address.
4. If desired, repeat step 3 for other devices connected to the network.

End of Procedure

Upgrading memory

For capacity reasons, the memory on the Succession Signaling Server has been increased from 256MB to 512MB. 256MB is more than sufficient for Succession 1000 Release 1.0 and 2.0 systems in smaller environments (less than 5000 Internet Telephones).

This change is effective on all Succession Signaling Servers shipped with Succession 3.0 Software. To enable customers to redeploy their current NTDU27AA 01, 02 or 03 Succession Signaling Servers into a large Succession 3.0 environment, a Succession Signaling Server Memory Upgrade Kit (NTDU80CA) is available. Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for detailed instructions on installing this kit.

IP Telephony node configuration

This section lists the procedures to use Element Manager to perform IP Telephony node configuration that is an integral part of the Signaling Server. For more details, refer to *Signaling Server: Installation and Configuration* (553-3001-212) and *IP Line: Description, Installation, and Operation* (553-3001-365).

An IP Telephony node is defined as a collection of Succession Signaling Servers and Voice Gateway Media Cards (VGMC). Each network node has a unique Node ID, which is an integer value. A node has only one Leader Succession Signaling Server. All other Succession Signaling Servers and VGMCs are defined as Followers. An IP Telephony node must be configured to make a Succession 1000 or Succession 1000M system operational. For more information about IP Telephony nodes and their configuration, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

The IP Telephony node database files are backed up, along with the customer database, by using the EDD command in LD 43. Refer to *Software Input/Output: Maintenance* (553-3001-511) for details about this command.

Element Manager requires Microsoft Internet Explorer 6.026 or higher. Element Manager is not supported on the Netscape browser. Browser caching must be turned off in Internet Explorer.

For more information on Element Manager, refer to *Succession 1000 Element Manager: System Administration* (553-3001-332).

Importing IP Telephony node files

Use this procedure to import existing IP Telephony nodes, including those that have been pre-configured during software installation of a Succession Signaling Server (see Procedure 6 on page 108).

Adding a Follower Succession Signaling Server to a node

Use this procedure to add a follower Succession Signaling Server to an IP Telephony node.

After software installation and reboot, the Follower Succession Signaling Server sends out BOOTP requests, and waits for a response. Since the Follower Succession Signaling Server has not booted successfully before, it waits for a BOOTP response that will not arrive. Do not wait for this response; perform this procedure immediately.

Note: The first time the Follower Succession Signaling Server is installed, the FTP fails. The failure occurs because the Follower cannot obtain the system login and password, and does not have the current CONFIG.INI file with the Succession Call Server IP address. In subsequent Follower installations, FTP succeeds.

Importing and upgrading an IP Trunk node

To work with IP Trunk nodes, the IP Trunk cards must first be converted to Voice Gateway Media Cards. They can then be added to new and existing IP Telephony nodes. To import and upgrade an IP Trunk node to an IP Telephony Node, refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258), *Large System: Upgrade Procedures* (553-3021-258), or *Small System: Upgrade Procedures* (553-3011-258).

Reviewing and submitting IP Telephony node configuration

Use this procedure to review IP Telephony node configuration before submitting. If the configuration is correct, they data can be submitted.

Transferring IP Telephony files

Use this procedure whenever you change the IP telephony node configuration. This procedure transfers the node data files to the other nodes in the system. You can transfer the data files to one, many, or all other nodes in the system.

Note: After completing this procedure, reboot the Succession Signaling Server if you changed its configuration.

Backing up IP Telephony node configuration files

Use this procedure as an alternative to the EDD command in LD 43 to perform a data dump. The data dump backs up new and updated IP Telephony node files on the Succession Call Server at the same time as it backs up the customer database.

Maintenance

Succession Signaling Server tools menu

From the Tools Menu in the Succession Signaling Server Install Tool, you can perform the following tasks:

- set the system time and date
- repartition and initialize the hard desk
- reset the Administrator login and password
- test the hard disk
- change the web server security flag

Use Procedure 9 to access the options in the Succession Signaling Server Install Tools menu.

Procedure 9
Using the Tools Menu in the Succession Signaling Server Install Tool

1 At the Install Tool Main Menu (Figure 24 on page 116), enter ‘t’ to access the Tools menu. The Tools Menu appears, as shown in Figure 40 on page 134.

Figure 40
Tools menu

```
Succession Enterprise Software Signaling Server Install Tool (sse-x.xx.xx)
================================================================================

                  T O O L S   M E N U

This is the Tools Menu. Please select one of the options below.

Please enter:
<CR> -> <a> - To set system date and time.
        <b> - To partition and initialize the hard disk.
        <c> - To reset the Administrator login and password.
        <d> - To test the hard disk.
        <e> - To change the web server security flag.
        <m> - To return to the Main Menu.

Enter Choice>
```

2 Under the Tools menu, you can enter:

- 'a' to set the date and time (default).
- 'b' to repartition and reinitialize the hard disk. This option results in a reboot. Leave the Succession Signaling Server Software CD-ROM in the drive so that the Install Tool can restart. Then, reinstall the Succession Signaling Server software as described in Procedure 6 on page 108.
- 'c' to delete the Administrator login and password.
- 'd' to test the hard disk.
- 'e' to change the Web server security flag. See "Procedure 10 on page 135".

End of Procedure

Restricting Web access to ELAN

By default, Element Manager can be accessed from management workstations (Web browsers) on any subnet. A security flag can be enabled to restrict Element Manager access to hosts on the ELAN subnet only.

Procedure 10
Changing the Web server security flag

If this Succession Signaling Server's IP Telephony node is already managed using Element Manager, then ensure that the Succession Signaling Server has the latest node files before performing this procedure, by performing a node file transfer.

1 Open the Tools Menu in the Succession Signaling Server Install Tool.

   a. Load the Succession Signaling Server Install Tool.

   b. At the Main Menu, enter 't' to open the Tools Menu.

2 Enter 'e' to change the Web server security flag. The current value of the flag displays:

```
Currently, the flag is set to: DISABLED
```

3 Change the flag:

   a. To disable the Web server security flag, enter 'a'. The new value of the flag displays.

   b. To enable the Web server security flag, enter 'b'. The new value of the flag displays.

   c. To exit this menu without changing the Web server security flag, enter 'q'.

4 Enter 'm' to exit the Succession Signaling Server Install Tool.

5 Import the IP Telephony node files for the web security flag change to take affect. Use "Importing IP Telephony node files" on page 131.

   If this is a first-time Succession Signaling Server or node installation, the pre-configured IP Telephony node files are imported. If this is an upgrade of the Succession Signaling Server, the web server security flag change is saved to the master copy of the node files on the Succession Call Server.

End of Procedure

Setting the Succession Signaling Server port speed

Administrators can change the port speed of the Succession Signaling Server for a maintenance terminal connection.

Procedure 11
Changing the Succession Signaling Server port speed

1. Log in to the Succession Signaling Server. See "Logging in to the Succession Signaling Server" on page 128.
2. Enter **`stty 9600`** to change the port speed to 9600 baud.

   Note: Acceptable values for the maintenance port speed are 9600, 19 200, 38 400 and 115 200.
3. Change the port speed on the terminal, terminal emulator, or PC (which can require a terminal emulator reset).
4. Press **<cr>** several times until the command line prompt is visible at the new speed.
5. Enter the `exit` command to log out of the CLI.

End of Procedure

Command line interface commands

This section contains Succession Signaling Server Command Line Interface (CLI) commands. The commands are available at two levels:

- **`IPL->prompt`** – for technicians and installers
- **`->prompt`** – for advanced troubleshooting

Patch commands (Table 27 on page 146) are entered at the PDT shell. All other commands are entered at the vxWorks shell.

You must log into the Succession Signaling Server to use CLI, using Procedure 7 on page 129.

Many of these commands are also available in Element Manager. The tables in this section list the available commands, and indicate if each command is available in Element Manager.

For more information on CLI commands, refer to *IP Line: Description, Installation, and Operation* (553-3001-365). For more information on Element Manager, refer to *Succession 1000 Element Manager: System Administration* (553-3001-332).

General purpose IPL> commands

Table 19 lists the general purpose IPL> commands. These commands must be entered at the vxWorks shell.

Table 19
General purpose commands (Part 1 of 3)

IPL> command	Description	Element Manager
i	Displays the current task list.	✓
routeAdd	Adds a route to the network routing table.	
routeShow	Displays the current host and network routing tables.	✓
ping “host”, “numpackets”	Sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packets responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. The “numpackets” parameter specifies how many packets to send. If it is not included, ping runs until it is stopped by Ctrl-C (also exits the IPL> Command Line Interface). Example: IPL> **ping** “47.82.33.123”, 10	
itgCardShow	Displays Voice Gateway Media Card information.	✓
itgMemShow	Displays memory usage.	
ifShow	Displays detailed IP address information, including MAC addresses.	✓
IPInfoShow	Displays IP address information.	✓
swVersionShow	Displays software version.	

Table 19
General purpose commands (Part 2 of 3)

IPL> command	Description	Element Manager
isetShow	Displays general information for all registered Internet Telephones. For example, the command displays the IP address of the Internet Telephone, the VTN that the Internet Telephone is associated with, indicates the type of Internet Telephone such as i2001, i2002, i2004, CPVIP, or i2050, and provides the type of registration and the new registration status.	
isetShowByTN	Displays general information about all registered Internet Telephones, sorted by TN.	
isetShowByIP	Displays general information about all registered Internet Telephones, sorted by IP address.	
pbxLinkShow	Displays information about the link to the CPU, including the configuration and link status.	✓
itgAlarmTest	Generates **ITGxxxx** test alarms.	
electShow	Displays a list of cards in the node and information about each.	
elmShow	Displays a list of supported languages.	
cardRoleShow	Shows the actual role of the card.	✓
ipstatShow	Displays the IP protocol statistics.	✓
rudpShow	Displays the status of the RUDP links on the card. This includes the Succession 1000 or Succession 1000M CPU and to all Internet Telephones registered with the card.	✓
vgwShowAll	Displays voice gateway channels.	✓
servicesStatusShow	Displays the status of services (iset/vtrk/gk).	✓

Table 19
General purpose commands (Part 3 of 3)

IPL> command	Description	Element Manager
loadBalance	Attempts to balance the registration load of telephones between this Succession Signaling Server and the rest of the node components.	✓
soHelpMenu	Shows all the Succession Signaling Server switch-over CLIs that are available to the user.	

File transfer IPL> commands

Table 20 lists the file transfer IPL> commands. These commands must be entered at the vxWorks shell.

Table 20
File transfer commands

IPL> command	Description	Element Manager
bootPFileGet	Sends an updated bootptab file from the host to the card.	
bootPFilePut	Send the bootptab file to the specified host.	
configFileGet	Sends an updated config.ini file from the host to the card.	
currOMFilePut	Sends the current OM file to the specified host.	
omFilePut	Sends the current OM file to the specified host.	
hostFileGet	Transfers any file from OTM to ITG.	
hostFilePut	Transfers any file from ITG to the specified host.	

Reset IPL> commands

Table 21 lists the reset IPL> commands. These commands must be entered at the vxWorks shell.

Table 21
Reset commands

IPL> command	Description	Element Manager
isetReset “tn” l s c u	Resets the Internet Telephone on Succession 1000M Large Systems.	
isetReset “tn” c u	Resets the Internet Telephone on Succession 1000 and Succession 1000M Small Systems.	
isetResetAll	Resets all registered Internet Telephones.	
resetOM	Resets the operational measurement file timer. This command resets all operational measurement parameters collected since last log dump.	

Upgrade IPL> commands

Table 22 lists the upgrade IPL> commands. These commands must be entered at the vxWorks shell.

Table 22
Upgrade commands

IPL> command	Description	Element Manager
umsPolicyShow	Displays the current upgrade policy.	✓
umsUpgradeAll	Upgrades all registered telephones according to policy and firmware file.	✓
umsUpgradeTimerShow	Shows the upgrade schedule.	
umsUpgradeTimerCancel	Cancels the scheduled upgrade.	

Internet Telephone Installer Password IPL> commands

Table 23 lists the Internet Telephone Installer Password IPL> commands. These commands must be entered at the vxWorks shell.

Table 23
Internet Telephone Installer Password commands (Part 1 of 3)

IPL> command	Description	Element Manager
nodePwdEnable	Enables the administrative Internet Telephone Installer Password setting. After this command is entered, all Internet Telephones registering display the password screen.	✓
nodePwdDisable	Disables both the administrative and the temporary Internet Telephone Installer Password settings. After this command is entered, all Internet Telephones display the original Node ID and TN screen during registration.	✓
nodePwdShow	Displays the settings of the Internet Telephone Installer Password. The command displays the current password, the state of password entry (enable/disable), the temporary password, and the number of uses and time to expiry.	
nodeTempPwdClear	Deletes the temporary Internet Telephone Installer Password. It also resets the uses and time parameters to zero.	✓
clearLockout <TN | IP>	Clears the lockout at the TPS for a particular Internet Telephone resulting from three consecutive failed attempts to enter either the Internet Telephone Installer Password or the Temporary Internet Installer Password.	

Table 23
Internet Telephone Installer Password commands (Part 2 of 3)

IPL> command	Description	Element Manager
nodePwdSet “password”	Sets and enables the administrative Internet Telephone Installer (node) Password. This is also known as the node level Internet Telephone Installer Password. If a null password (0 characters in length) is configured, all Internet Telephones that attempt to register after this command has been issued display a prompt for node password before the TN can be modified. The “password” parameter must be null or 6 to 14 digits in length; The valid characters are 0 – 9 * #. The null password causes the Node ID and Password screen on the Internet Telephone to be skipped during restart. This command can be entered at any time; the new password entered overwrites the prior password.	✓

Table 23
Internet Telephone Installer Password commands (Part 3 of 3)

IPL> command	Description	Element Manager
nodeTempPwdSet “tempPwd”, uses, <time>	Sets the temporary Internet Telephone Installer Password. This password is disabled by default. The password must be a string 6 to 14 digits in length. A null password cannot be entered. The valid tempPwd characters are 0 – 9 * #. The uses parameter is a numeric value from 0-1000. This parameter specifies the number of uses for which the temporary password is valid. The range for the time parameter is 0 – 240 hours, which is a maximum of 10 days. The time parameter specifies the duration in hours that the password is valid. • If the uses parameter is set to zero, the time parameter is mandatory. As a result, the password only expires based on time. • If the uses parameter is non-zero, the time parameter is optional. • If both the uses and time parameters are entered, the password expires on whichever comes first, that is, uses is reduced to zero or the time has expired. • If both uses and time are entered and both are set to zero, it is the same as not setting the temporary password at all. This command can be entered at any time and the new parameters overwrite the existing temporary password’s parameters.	✓

Enable IPL> commands

Table 24 lists the enable IPL> commands. These commands must be entered at the vxWorks shell.

Table 24
Enable commands

IPL> command	Description	Element Manager
enlServices	Enables acceptance of resources registration.	✓
enlVTRK	Enables acceptance of Virtual Trunks registration.	✓
enlTPS	Enables the TPS application and the registration process.	✓
enlGK	Puts local Gatekeeper in service.	✓

Graceful disable IPL> commands

Table 25 lists the graceful disable IPL> commands. These commands must be entered at the vxWorks shell.

Table 25
Graceful disable commands (Part 1 of 2)

IPL> command	Description	Element Manager
disiAll	Gracefully disables both the LTPS and voice gateway service on the Voice Gateway Media Card. Gracefully disables the LTPS on the Succession Signaling Server.	✓
disiTPS	Gracefully disables the LTPS service on the Voice Gateway Media Card. Prevents new Internet Telephones registering on the card, and all registered Internet Telephones are redirected to another card when idle.	✓

Table 25
Graceful disable commands (Part 2 of 2)

IPL> command	Description	Element Manager
enaAll	Enables both the LTPS and voice gateway service on the Voice Gateway Media Card. Enables the LTPS on the Succession Signaling Server.	
enaTPS	Enables the LTPS service.	
disServices	Gracefully switches the registered resources to the other Succession Signaling Servers located in the same node. This command will not interrupt established calls.	✓
disVTRK	Gracefully switches the registered Virtual Trunks to the other Succession Signaling Servers located in the same node.	✓
disTPS	Gracefully switches the registered Line TPS to the other Succession Signaling Servers located in the same node.	✓
disGK	Puts the local Gatekeeper out of service and puts the alternate Gatekeeper in service.	✓

Forced disable IPL> commands

Table 26 lists the forced disable IPL> commands. These commands must be entered at the vxWorks shell.

Table 26
Forced disable commands

IPL> command	Description	Element Manager
forcedisServices	Forces all registered resources on the Succession Signaling Server to unregister and let Gatekeeper go out of service.	✓
forcedisVTRK	Forces all registered Virtual Trunks on the Succession Signaling Server to unregister.	✓
forcedisTPS	Forces the Line TPS on the Succession Signaling Server to unregister.	✓
forcedisGK	Forces the local Gatekeeper out of service.	✓

Patch IPL> commands

Table 27 lists the patch commands. These commands must be entered at the PDT shell.

Table 27
Patch commands (Part 1 of 2)

IPL> command	Description	Element Manager
pnew	Creates memory patches for the card.	✓
pload	Loads a patch file from the filesystem on Flash memory into DRAM memory.	✓
pins	Puts a patch into service that has been loaded into memory using pload.	✓
pout	Removes a patch from the DRAM memory.	✓

Table 27
Patch commands (Part 2 of 2)

IPL> command	Description	Element Manager
poos	Deactivates a patch by restoring the patched procedure to its original state.	✓
plis	Gives detailed patch status for a loaded patch.	✓
pstat	Gives summary status for one or all loaded patches.	✓

IP Peer Networking Phase 2

Contents

This section contains information on the following topics:

Overview

Succession 3.0 software supports IP Peer Networking Phase 2. IP Peer Networking Phase 2 allows the customer to distribute Succession 1000 and Succession 1000M system functionality over a Wide Area Network (WAN) using either standard H.323 Gateways or Nortel Networks IP Gateways (for example, Succession Signaling Server).

IP Peer Networking Phase 2 brings the same features to the Succession 1000M system as IP Peer Networking brings to the Succession 1000 system, plus enhancements. See "IP Peer Networking Phase 2 enhancements" on page 159 for more information on these enhancements. IP Peer Networking enables the Meridian 1 to provide an industry-leading PBX feature set on an IP PBX that can be distributed throughout a customer's IP network.

Key advantages of IP Peer Networking are as follows:

- provides global coverage of line and trunk interfaces
- enables the networking of multiple systems across an IP network
- enables the customer to provision Internet Telephones anywhere on the connected network (LAN/MAN/WAN) and also enables them to provide LAN-connected modules (such as a router, Layer 2 switch, Layer 3 switch, bridge, or hub)
- enables the Succession 1000 and Succession 1000M to provide an industry-leading PBX
- consolidates voice and data traffic on a single Quality of Service (QoS)-managed network. Network-wide feature transparency is provided using the Nortel Networks protocol: Meridian Customer Defined Network (MCDN).
- enables Call Servers to internetwork over IP facilities without using circuit switching.

  IP Peer Networking uses direct IP media paths to connect two IP devices. Media streams route directly between Internet Telephones and Gateways over the IP network, using IP Peer H.323 Trunks (Virtual Trunks). This minimizes voice quality issues caused by delay and transcoding between circuit-switched voice and IP packets.

IP Peer Networking uses an H.323 Gatekeeper to simplify the configuration of IP components. The H.323 Gatekeeper manages a centralized numbering plan for the network. For more information on the Gatekeeper refer to the section "Gatekeeper" on page 153.

The existing system must be upgraded with the Succession 3.0 software for IP Peer Networking and a Succession Signaling Server must also be installed and configured to provide the H.323 signaling for IP Peer H.323 Trunks.

The Succession Signaling Server is an industry-standard, PC-based server that provides a central processor to drive H.323 signaling for Internet Telephones and IP Peer Networking. Refer to "Succession Signaling Server" on page 85 for more information about the Succession Signaling Server.

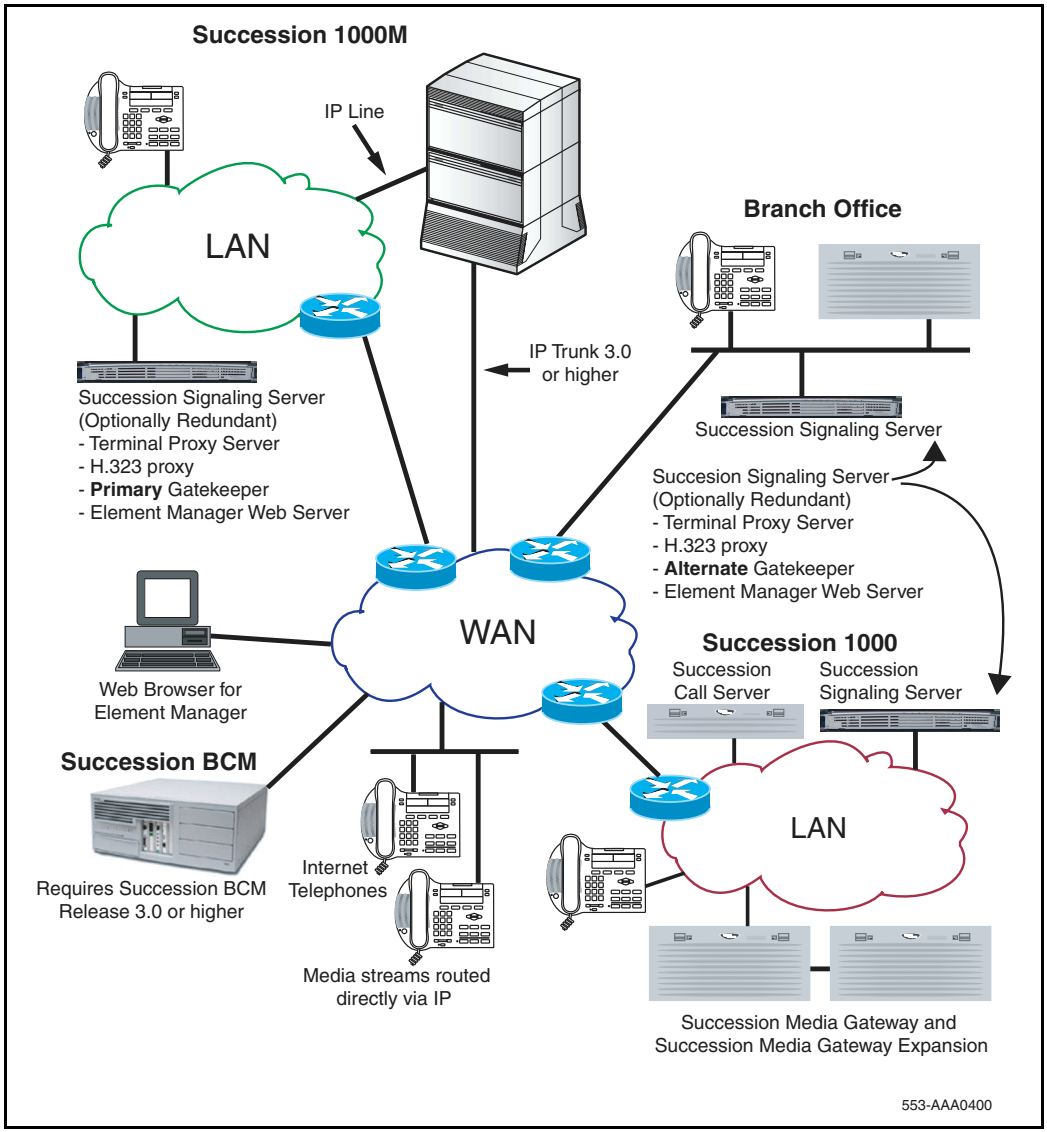
IP Peer H.323 Trunks

IP Peer H.323 Trunks are software components configured on virtual loops, similar to Internet Telephones. An IP Peer H.323 Trunk acts as the bridge between existing call processing features and the IP network. It enables access to all trunk routing and access features in the MCDN networking feature set. IP Peer H.323 Trunks do not require dedicated Digital Signaling Processor (DSP) resources to provide these features. IP Peer H.323 Trunks include all of the features and settings available to ISDN Signaling Link (ISL)-based TIE trunks, and are configured within trunk routes. Voice Gateway Media Card resources are only allocated for IP Peer H.323 Trunks when it is necessary to transcode between IP and circuit-switched devices.

> ***Note:*** Voice Gateway Media Card is the generic term that refers to both the ITG-Pentium (ITG-P) Line Cards (dual-slot/24-port card) and the Succession Media Card (single-slot/32-port card).

Figure 41 on page 152 illustrates an IP Peer Networking configuration.

Figure 41
IP Peer Networking



Gatekeeper

All Succession 1000 and Succession 1000M systems in the IP Peer network must register with the Gatekeeper.

The Gatekeeper provides the following:

- endpoint and Gateway registration
- call admission control
- address translation and telephone-number-to-IP lookup
- centralized numbering plan administration

Note: The Gatekeeper (Primary and Alternate) can operate in stand-alone mode, without connecting to the Succession Call Server.

The Gatekeeper is H.323 compliant and can provide Gatekeeper features to other H.323-compliant Nortel Networks endpoints (for example, to Succession 1000 and IP Trunk 3.x endpoints). A static IP address must be configured for these endpoints, as well as the telephone numbers that the endpoints can terminate.

Gatekeeper components

The Gatekeeper consists of the following major components:

- Gatekeeper Network Protocol Module (GKNPM)
- Database Module (DBM)
  - primary and alternate databases
- Web server
- vxWorks shell

Gatekeeper Network Protocol Module

The Gatekeeper Network Protocol Module (GKNPM) interfaces with the H.323 stack and is responsible to send and receive all H.323 Registration, Admission, and Status signaling (RAS) messaging.

When a RAS request message arrives over the network, the H.323 stack informs the GKNPM of the incoming request. The GKNPM uses H.323 Application Programming Interfaces (APIs) to retrieve the relevant data. For example, if the incoming request is an Admission Request (ARQ), the GKNPM extracts the originator's endpointIdentifier and the desired terminator's destinationInfo fields from the ARQ message.

After all relevant information has been extracted from the incoming RAS request, the GKNPM passes the request to the Database Module (DBM) for resolution. The DBM consults its numbering plan configuration and informs the GKNPM of the result. The GKNPM then sends the relevant RAS response to the RAS request originator.

Database Module

The Database Module (DBM) is responsible for the following:

- configuring the numbering plan
- reading and updating the primary and alternate databases on disk
- resolving all registration and admission requests which the GKNPM passes to the DBM

The Gatekeeper numbering plan configuration is stored in XML format in two databases on disk. The primary database is used for call processing and the alternate database is used for configuration changes.

The DBM interfaces with the primary and alternate databases on disk. All call processing requests that the GKNPM passes to the DBM are resolved using the primary database. The DBM uses the information that the GKNPM extracted from the RAS request (for example, ARQdestinationInfo) to search its database. In the case of an ARQ message, the DBM attempts to find a registered endpoint that can terminate this call.

The Web server interfaces with the DBM for viewing, adding, deleting, or modifying numbering plan configuration data. All changes to the numbering plan database are carried out on the alternate database. Changes to the numbering plan database do not affect call processing immediately. The database must first be cut over to the main database.

Web server

Gatekeeper configuration is performed using Element Manager. The administrator can view, modify, or delete all numbering plan configuration data, make changes in operation, or restore the previous database if the changes are unsuitable. Element Manager also provides various diagnostic and traffic measurement tools.

vxWorks Shell

The Wind River vxWorks shell provides access to the operating system for maintenance and debug operations.

IP Peer Networking and Gatekeeper management

This section briefly describes the steps required to configure IP Peer Networking and manage the Gatekeeper database. For detailed information, refer to *IP Peer Networking* (553-3001-213).

Implementation summary

Note: Many of these steps can be performed out of the sequence presented below.

1 Configure the IP Peer H.323 Trunk routes using Element Manager or LD 16. Configure the Route Data Blocks and associate the IP Peer H.323 Trunk routes with the IP network by configuring the following parameters:

- **a** route information
- **b** network management information (for example, Access Restrictions)
- **c** bandwidth zone
- **d** Succession Signaling Server host name for the route
- **e** protocol identifier
- **f** associated Node ID

2 Configure the IP Peer H.323 Trunks using Element Manager or LD 14.

3 Configure the network routing within the Succession Call Server.

- **a** Configure networking features such as routing calls based on digits dialed.
- **b** Configure dialing plan information for calls that must be routed to circuit-switched trunks (for example, to PSTN interfaces). You can route these calls using a feature such as Network Alternate Route Selection (NARS). Configure IP Peer H.323 Trunk routes in NARS the same way as traditional trunks.

4 Configure the Primary, Alternate, and Failsafe Gatekeepers at installation and initial setup.

5 Configure the Gatekeeper database to provide a central database of addresses that are required to route calls across the network, using Element Manager.

a Log in to Element Manager.

b Verify that the Gatekeeper is the Primary Gatekeeper and is active.

c Configure the system-wide settings.

d Create the CDP domains.

e Add the RAS endpoints.

f Add the endpoint prefixes.

g Add the Numbering Plan entries for each endpoint, including the Cost Factor for each entry.

h Add the default routes.

i Add the Gatekeeper zones (if required).

j Test the Numbering Plans.

k Perform database cutover.

l Perform the following operations, as necessary:

i. Take the Gatekeeper out-of-service.

ii. Perform database cutover.

iii. Perform database rollback.

iv. View traffic reports.

m Log out of Element Manager.

Configuring IP Peer Networking

Customers can use the following interfaces to configure IP Peer Networking components:

- Element Manager
- Command Line Interface (CLI)
- Optivity Telephony Manager (OTM)

  Note: OTM can be used to launch Element Manager. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for detailed information on OTM.

Element Manager enables you to configure and maintain certain aspects of the system through a web browser. Element Manager must be installed on each Succession Signaling Server within the system. Element Manager requires Microsoft Internet Explorer 5.5 or later. For a detailed description of Element Manager, refer to *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) and *Succession 1000 Element Manager: System Administration* (553-3001-332).

You can also perform configuration functions through the Command Line Interface (CLI). Refer to "Feature Implementation" in *IP Peer Networking* (553-3001-213) for IP Peer configuration information.

The *IP Peer Networking* (553-3001-213) NTP has a summary of tasks required to implement IP Peer Networking in your IP network. Refer to the *IP Peer Networking* (553-3001-213) for detailed procedures.

Once you install and configure the components, you can configure the IP Peer Networking feature. Configuring IP Peer Networking in a network is similar to configuring a traditional circuit-switched network that uses a "star" topology. All systems form the outer points of the star, with respect to address resolution (the systems form a grid with respect to media paths). These systems are configured to route network-wide calls into the IP network over a route configured with IP Peer H.323 Trunks. The IP Peer H.323 Trunks are configured to use the Gatekeeper. The Gatekeeper, in conjunction with the Gateway software at each site, acts as the center of the "star".

Feature packaging

The following package is required for IP Peer Networking:

- H323 Virtual Trunk (H323_VTRK) package 399

The following ISM parameter is required for IP Peer Networking:

- IP PEER H.323 TRUNK parameter

IP Peer Networking Phase 2 enhancements

IP Peer Networking Phase 2 supports the following enhancements.

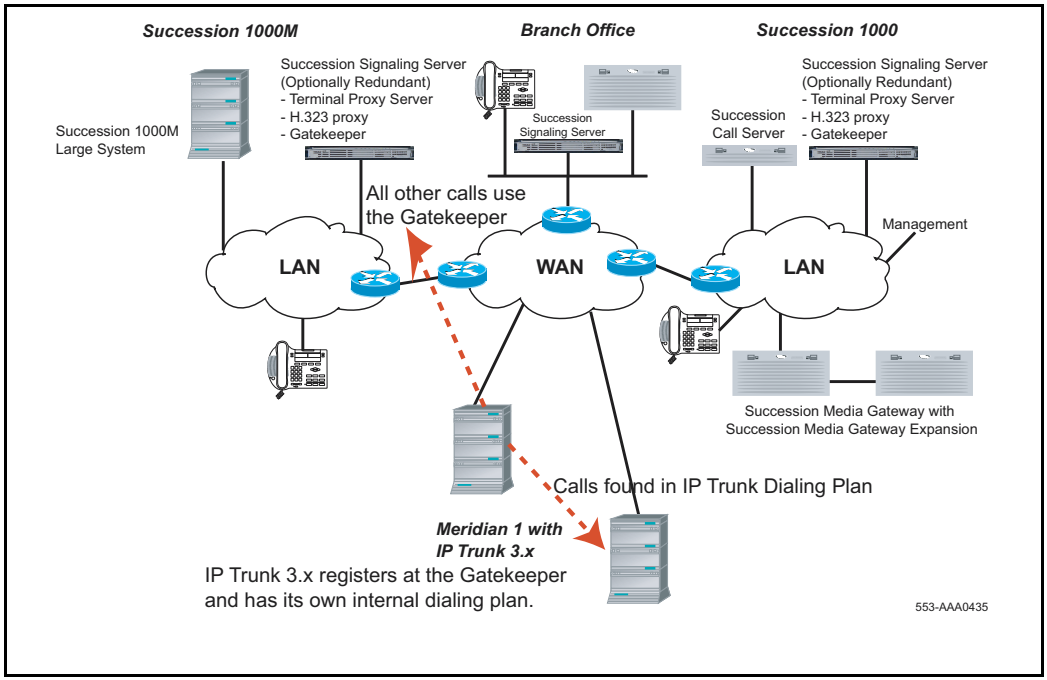
Interoperability

Succession 3.0 software networks with Meridian 1 Release 25.xx or later. Nortel Network's Meridian Customer Defined Network (MCDN) protocols over PRI trunks gives the rich feature set currently available to networks of Meridian 1 systems.

IP Trunk 3.0x

IP Peer Networking Phase 2 interworks with IP Trunk 3.0x. It also supports all the MCDN features that IP Trunk 3.0x support, including Trunk Route Optimization (TRO).

Figure 42
IP Peer to Meridian 1 IP Trunk 3.0x Interworking



With IP Trunk, the numbering plan is configured for each site. With IP Peer Networking, the Gatekeeper maintains the numbering plan for all sites. IP Trunk 3.0x maintains a point-to-point configuration. If a call is routed using IP Trunk 3.0x and the path is found, then the session is established. If the route path is not found, the lookup process is handed off to the Gatekeeper to resolve the route path.

Succession 1000 Release 2.0

For a system running the Succession 3.0 software to interwork with a Succession 1000 Release 2.0 system, the following requirements must be met:

1. The ITG-Pentium 24-port and Succession Media Card 32-port trunk cards must be upgraded to IP Trunk 3.0x software. This upgrade supports MCDN features and Gatekeeper registration. Use OTM 2.1 to perform the upgrade. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on installing, upgrading, and configuring IP Trunk 3.01 parameters.

2. Configure the IP Trunk 3.x node to register with the Succession 1000 Gatekeeper, in the OTM 2.1 Gatekeeper Properties dialog window which is shown in Figure 43 on page 162. This dialog window enables the administrator to link an IP Trunk 3.x endpoint to a Gatekeeper zone (automatically providing Primary and Alternate Gatekeepers). This window is also used to manually provision a Gatekeeper for the node. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on how to configure the IP Trunk 3.x options.

Figure 43
Gatekeeper Properties dialog window

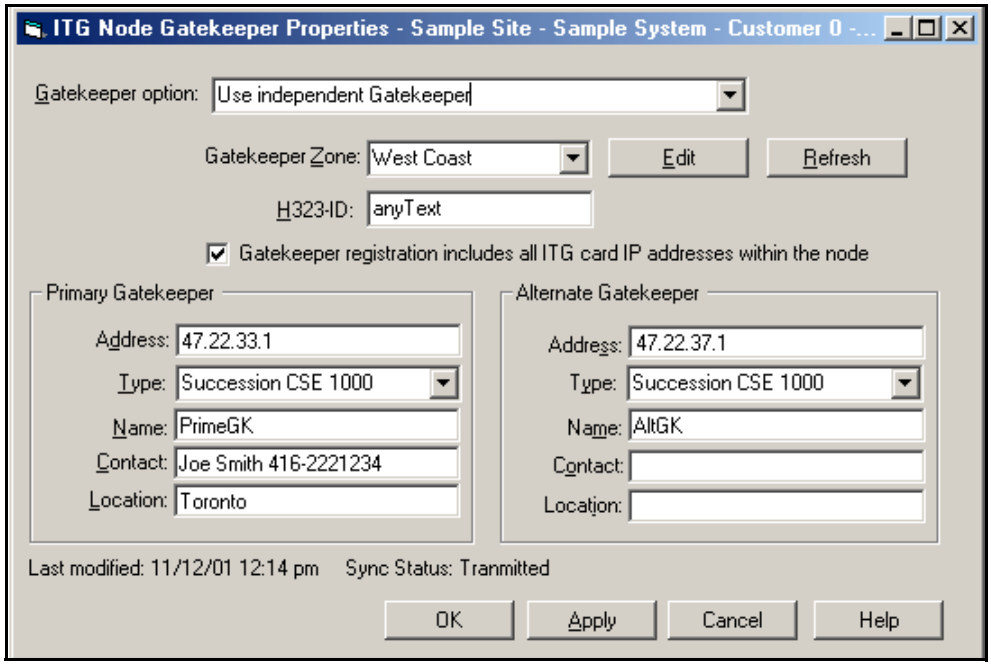
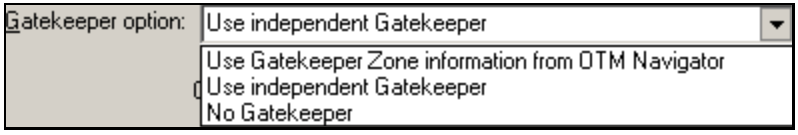


Figure 44
Gatekeeper option drop-down list



If configured properly, the IP Trunk 3.x node uses RAS messaging to register with the Gatekeeper. The IP Trunk 3.x node then processes calls by scanning its DN information and routing unresolved calls to the Gatekeeper, using the Address Translation Protocol Module (ATPM).

OTM 2.1 enables the user to configure the IP address of a Succession 3.0 node, with a capability of "CSE" in the ATPM dialing plan table. This enables the IP Trunk 3.x node to directly call the Succession 1000 Release 2.0 node.

The IP Trunk 3.01 node is subordinate to the Gatekeeper for all calls requiring the Gatekeeper. The IP Trunk 3.x node:

1 registers with the Gatekeeper, according to H.323 protocol

2 requests admission

3 accepts the reply, according to H.323 protocol

4 proceeds to handle the call as required, based on the returned message

Note: IP Trunk 3.x supports the Succession Media Card 32-port trunk card and/or the ITG-Pentium 24-port trunk card.

Refer to *IP Trunk* (553-3001-202) for information on how to install, configure, and operate IP Trunk 3.x functions, as well as information on IP Trunk 3.x signaling support (for example, MCDN, non-call associated signaling, and ESN5).

Succession Business Communication Manager (BCM)

IP Peer Networking Phase 2 interoperates with Succession Business Communication Manager (BCM) version 3.01. Succession BCM 3.01 has been enhanced with many additional MCDN features including the following:

- Network Call Transfer
- Network Call Redirection Information
- Message Waiting Indication
- ISDN Call Connection Limitation
- Trunk Route Optimization
- Trunk Anti-Tromboning
- Camp-On
- Break-In

For interworking between a Succession Business Communication Manager (BCM) and a system running the Succession 3.0 software, upgrade the Succession BCM to version 3.01 software.

A Succession BCM endpoint is configured on the Gatekeeper the same way that a Succession 1000 or Succession 1000M endpoint is configured. Configure the following on the Succession BCM so that it can interwork with the Succession 3.0 system:

- **Unified Manager: Services | IP telephony | H.323 Trunks | Call Signaling** should be set to **GatekeeperRouted** or **GatekeeperResolved**
- **Unified Manager: Services | IP telephony | H.323 Trunks | Gatekeeper IP** should be set to IP address of the Gatekeeper
- **Unified Manager: Services | IP telephony | H.323 Trunks | Alias Names** should be set to the Alias name that was used when the H.323 Endpoint for the Succession BCM was created on the Gatekeeper

To make a Succession BCM to Succession 1000 or Succession 1000M system call, ensure that Succession BCM routes and dialing plan (used to reach the Succession 1000 or Succession 1000M system) matches the numbering plan entry assigned to the Succession 1000 or Succession 1000M system through Element Manager.

Similarly, to make a Succession 1000 or Succession 1000M system call to Succession BCM call, ensure that the numbering plan entry assigned to the Succession BCM (through Element Manager) matches the dialing plan information configured on the Succession 1000 or Succession 1000M.

Voice quality

IP Peer Networking addresses voice quality by providing an End-to-End Voice Path between any Internet Telephones and/or H.323 Media Gateways. An End-to-End Voice Path is also known as IP Peer H.323 Trunk.

Scalability

The Succession 3.0 software increases IP scalability. Table 28 on page 165 summarizes the limits for each Succession Signaling Server.

Table 28
Succession Signaling Server limits

Succession Signaling Server component	Limit
Gatekeeper	2000 H.323 endpoints 10 000 number plan entries 60 000 calls per hour
Terminal Proxy Server (TPS)	5000 lines
IP Peer H.323 Trunks	382 trunks

Each Succession Signaling Server has the following new IP scalability limits:

- The number of supported H.323 endpoints increases to 2000.
- Prior to IP Peer Phase 2, each Gatekeeper could hold 512 entries for each endpoint (where a range is considered as one entry). The new limit is 10 000 number plan entries.
- Each Gatekeeper can now handle 60 000 calls per hour.
- The TPS on each Succession Signaling Server can support up to 5000 lines.
- The number of IP Peer H.323 Trunks supported by each Succession Signaling Server is 382. This reduces the number of Succession Signaling Servers that a large endpoint requires.

Talk-slot expansion allows non-blocking operation for virtual TNs. The number of supported Internet Telephones and IP Peer H.323 Trunks are increased as a result of the talk-slot expansion. The increase in the number of talk-slots guarantees a talk-slot for speech path connection for every virtual TN that is used by an Internet Telephone or a IP Peer H.323 Trunk.

The number of supported users in a system equals the maximum number of TNs supported in the system. The number of supported users increases to 10 000 per Call Server node, while the maximum number of users per network increases to 100 000.

Serviceability

This feature improves the serviceability of the IP Telephony equipment, resulting in the following benefits:

- Modified overlays provide operational consistency over IP Telephony Management equipment versus existing line equipment.
- Improved statistical gathering capabilities on the IP Telephony equipment through overlays.
- CLI commands for filtering and simplifying equipment tracing tools.
- Improved operational measurements threshold alarms and configuration CLIs for Voice Gateway (VGW) and Line Terminal Proxy Server (LTPS) Real-time Transport Protocol (RTP) packet loss, latency, and jitter.
- Hand-off CLI that gracefully switches resources from a targeted system to the connected resource, load-sharing system.

Reduction of provisioning effort

Vacant Number Routing (VNR) is improved to direct calls to the Gatekeeper that controls routing. This reduces the provisioning effort required for Branch Offices. VNR and VNR Enhancement are discussed in more detail in *IP Peer Networking* (553-3001-213).

Succession Branch Office

Contents

This section contains information on the following topics:

Introduction

This chapter describes the Succession Branch Office feature. Based on IP Peer Networking, the Branch Office feature extends Main Office features to one or more Branch Offices.

The Succession Branch Office feature already exists for Succession 1000 Release 2.0 systems, and has been enhanced in Succession 3.0 Software. Succession Branch Office customers, and users familiar with Branch Office functionality can go directly to “Succession 3.0 Software enhancements” on page 226 for more information on these enhancements.

Overview

Succession 3.0 Software introduces the Succession Branch Office feature to Meridian 1 systems equipped with the Succession Signaling Server, which make up the Succession 1000M portfolio.

The Branch Office is an H.323 WAN Gateway connected to an IP PBX at the Main Office over a WAN. The Succession Call Server at the Main Office supports call processing for Internet Telephones in the Main and Branch Offices. The Succession System Controller in the Branch Office H.323 WAN Gateway provides call processing functionality to local digital telephones and analog devices, and digital and analog trunk access to the local Public Switched Telephone Network (PSTN).

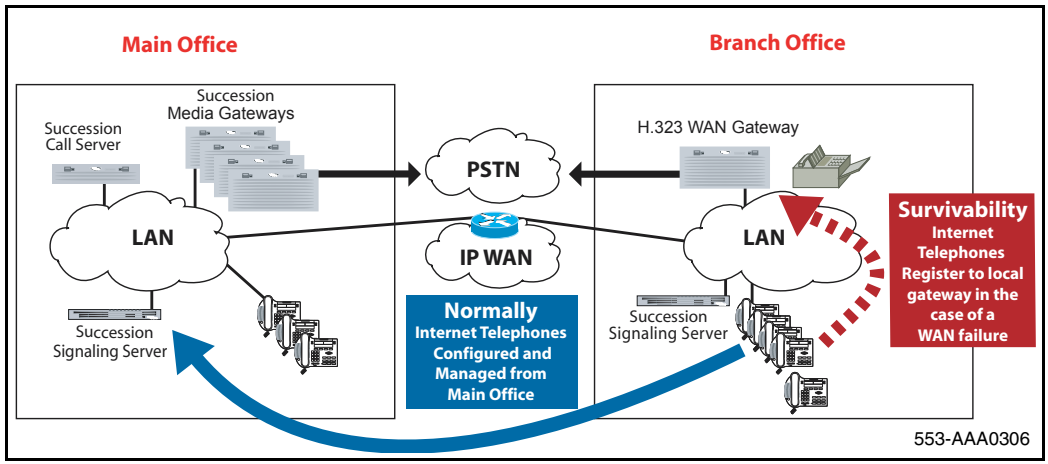
The Branch Office connects to the Main Office over Virtual Trunks on a WAN. The Main Office transmits and controls Internet Telephone calls and IP network connections. If the Main Office fails to function, or if there is a network outage, the Branch Office Succession System Controller (SSC) provides service to the telephones located in the Branch Office. This enables the Internet Telephones to survive the outage between the Branch Office and the Main Office.

The Main Office can be one of six systems (see page 183). More than one Branch Office can be associated with a single Main Office. One Branch Office can be associated with more than one Main Office.

A Branch Office is designed to work with a Main Office only if the two offices use a common dialing plan. Any other configuration is not guaranteed to work.

A Branch Office network is shown in Figure 45.

Figure 45
Branch Office network (with a Succession 1000 Main Office)



For a full description of Branch Office, refer to *Branch Office* (553-3001-214).

Network Connection Server

A Network Connection Server (NCS) is required for the Branch Office to work. Currently, the only NCS available is the Succession 1000 Gatekeeper. Therefore, Nortel Networks recommends that Virtual Trunks and Network Connection Servers both utilize the Succession 1000 Gatekeeper.

Note 1: Interoperability with Succession Communication Server for Enterprise Multimedia Xchange (MX) is supported. Virtual Trunks can utilize the MX H.323 Gatekeeper. In this case, at least one dedicated Succession Signaling Server is required to run as primary Succession 1000 NCS, where the H.323 endpoints are configured as non-RAS endpoints. However, the private numbering plan has to be configured on both the MX H.323 Gatekeeper and the Succession 1000 H.323 Gatekeeper.

Note 2: If both Branch Office and Virtual Office features are not required, then one of the following Gatekeepers is required: either a Succession 1000 H.323 Gatekeeper, or an MX H.323 Gatekeeper without a Succession 1000 H.323 Gatekeeper.

Zones and dialing plans

The Branch Office configuration enables Internet Telephones to run over a low latency WAN in many geographic locations other than that of the Main Office but controlled by the Main Office Succession Call Server. It is possible, and probably desirable, to have these Internet Telephones exhibit dialing plan behaviors that are location-specific rather than specific to the Main Office.

Branch Office zones

A zone is a collection of Internet Telephones that:

- share similar IP bandwidth restrictions
- are geographically near each other
- are all in the same time zone
- are all in the same PSTN dialing plan

A zone must be created before Branch Office properties are assigned. The Branch Office zone (or zones, if the Branch Office is to have multiple zones) must be configured at the Main Office. Each Internet Telephone in the Branch Office is then assigned to a zone during its configuration. For dialing plan purposes, all telephones in the same zone are treated identically.

Individual zones and zone features can be enabled and disabled separately. This enables the craftsperson to make the changes as a group, and activate them all at once. As soon as a feature is activated in an enabled zone, the Branch Office behavior takes effect for new calls.

Branch Office dialing plan

The Succession Branch Office is versatile enough to provide solutions for a wide variety of applications which require different dialing plans. Therefore, an effective dialing plan is critical for the successful deployment of a Succession 3.0 Branch Office.

When a number is dialed, the Succession Call Server determines whether the called number is internal or external to the Branch Office. If internal, the system terminates the call on the appropriate terminal. If external, the system routes the call in one of two ways:

- Uniform Dialing Plan (UDP) or Coordinated Dialing Plan (CDP) routes the call to the proper trunk group.
- Vacant Number Routing (VNR) routes the call to a Virtual Trunk.

Once the call is sent over the IP network, the call is routed to the Branch Office H.323 WAN Gateway, which uses the Gatekeeper to route the call. The Gatekeeper translates the address from a telephone number to an IP address, and authorizes the call in the H.323 network.

Specific dialing plan configuration is required for Internet Telephones to properly select a Main Office or Branch Office gateway that provides access to the PSTN for the originating Internet Telephone.

PSTN calls can be routed according to the point of origin (Main Office or Branch Office) and/or the desired destination, and can select trunks at the Main Office, Branch Office, or other Branch Offices as required. Therefore, the user can route calls to gateways that minimize long distance costs, minimize bandwidth usage, or meet other criteria.

The user can choose from two types of dialing plans: on-net dialing plans and off-net dialing plans.

On-net dialing plan options

Depending upon customer dialing preferences and configuration management requirements, many on-net dialing plans are available:

- Coordinated Dialing Plan (CDP) – Each location is allocated one or more Steering Codes that are unique within a CDP domain.
- Uniform Dialing Plan (UDP) – Each location is assigned a Location Code (LOC). Each telephone has a unique Directory Number (DN).

- Group Dialing Plan (GDP) – Each group has an LOC that has to be dialed from outside the group as a prefix to the group CDP. Members in the group may dial only the CDP number. Effectively, GDP is a combination of CDP and UDP.
- Transferable Directory Numbers (TNDN) – Each user is given a unique DN, that does not change even if it moves to a different Succession Call Server. The Gatekeeper keeps track of each TNDN in the network so that it knows to which H.323 endpoint (Succession Call Server or Branch Office H.323 WAN Gateway) to return when asked to resolve a TNDN address.

For more information, refer to *Dialing Plans: Description* (553-3001-183).

Nortel Networks recommends that customers use Coordinated Dialing Plan (CDP) between the Main Office and its Branch Offices since it enables all users, at the Main or Branch Office, to call each other using just an extension number. CDP enables consistent dialing between the Main Office and Branch Office Internet Telephones and devices.

Off-net dialing plan

When dialing to the PSTN, the Succession Call Server determines that the call destination is off-net by analyzing the digits that must be pre-configured at major Succession Call Servers in the network.

If routed over a Virtual Trunk, a request is sent to the Gatekeeper to determine the location of public E.164 numbers. The Gatekeeper is configured with a list of potential alternate routes that can be used to reach a certain dialed number. Each route is configured with a unique Gatekeeper Cost Factor to determine the least-cost route.

The Gatekeeper replies with the address information for E.164 numbers. It also provides a list of alternative H.323 endpoints, sorted by cost. If a terminating H.323 endpoint resource is busy when a call attempt is made, the originating H.323 endpoint tries the next alternative. If no alternative is available over the IP network, the originating H.323 endpoint steps to the next entry on its route list, which could be a TIE or PSTN alternate route.

Vacant Number Routing

Vacant Number Routing (VNR) is mandatory in a Branch Office. It enables a Branch Office to route calls through the Gatekeeper, or other alternate routes if configured, with minimal configuration. Instead of changing the numbering trees and steering codes at each location, all the routing information can be kept at one central location.

At the Branch Office, VNR is normally routed first to the H.323 IP Peer Trunk. VNR also enables data manipulation index (DMI) numbers for all trunk types so alternate routes can be configured.

If a vacant number is dialed, the number is not treated as invalid, and the call is routed to the Gatekeeper. The Gatekeeper tries to determine where the terminal is located. If the terminal is located, the call is routed to the terminating location. If the terminal cannot be located, each of the alternate routes will be tried, in the configured sequence. If all alternate routes fail, the call is blocked.

Emergency Services Access

The Branch Office allows the use of two methods to route emergency calls on a trunk at the same geographical location where the call-originating telephones are located:

- use of the Emergency Services Access (ESA) feature, which is the preferred method in North America
- use of a special dialing sequence such as a Special Number (SPN) in the the Network Alternate Route Selection (NARS) data block

Abbreviated Dialing

The Abbreviated Dialing feature allows users in the same geographic location—Main Office or Branch Office—to call one another with a DN shorter than the configured DN.

Survivability

In Normal Mode, Internet Telephones in the Branch Office are registered to, and controlled by, the Main Office Succession Call Server. If an outage

occurs at the Main Office or the WAN connecting the Main and Branch Offices, the Internet Telephones register with the SSC in the Branch Office and operate in Local Mode. The local SSC controls the telephones until the outage is resolved, at which point they are directed back to the Main Office and resume operating in Normal Mode.

In Local Mode, Branch Office Internet Telephones are under the control of the SSC in the Branch Office H.323 WAN Gateway. The local Internet Telephones can call Internet Telephones within the Branch Office. They can also call Internet Telephones at the Main Office through the local PSTN if ESN is configured correctly.

> ***Note:*** The Branch Office is not intended to be used as a peer switch or as a stand-alone system for an extended period of time. Operation of Internet Telephones in Local Mode is meant to provide survivability during conditions of network failure only. A license feature exists allowing Internet Telephones in a Branch Office to stay in Local Mode for a maximum of 30 days.

Features supported in the Branch Office

In Normal Mode, Internet Telephones in the Branch Office receive those features provisioned on the Main Office Succession Call Server. In Local Mode, Internet Telephones receive only those features and tones that are provisioned on the Branch Office SSC. The features are not necessarily the same in Normal Mode due to local configuration, or if the Branch Office and Main Office are running different software releases or service levels.

When the Branch Office is running the previous software release, the Local Mode features are limited to those available in that release. Depending on what is provisioned, this means that Normal Mode may have more features than Local Mode.

Network Bandwidth Management

Succession 1000 and Succession 1000M support bandwidth management on a network-wide basis. The Virtual Private Network Identifier (VPNI) is used to identify intrazone calls that involve Virtual Trunks. Recognizing that these calls do not use any WAN bandwidth, the calls are allowed, even though no spare WAN bandwidth is available. This provides more efficient use of bandwidth across the network. For more information, refer to *Branch Office* (553-3001-214).

H.323 WAN Gateway interoperability

H.323 WAN Gateway to H.323 WAN Gateway interoperability is fully supported between Succession 1000 and Succession Communication Server for Enterprise Multimedia Xchange (MX). A Network Connection Server (NCS) configured with H.323 endpoints is required for Branch Office and Virtual Office features to work. Currently, the only NCS available is the Succession 1000 Gatekeeper. Therefore, Nortel Networks recommends that Virtual Trunks and Network Connection Servers both utilize the Succession 1000 Gatekeeper.

Alternatively, Virtual Trunks can utilize the MX H.323 Gatekeeper. In this case, at least one dedicated Succession Signaling Server is required to run as primary Succession 1000 NCS, where the H.323 endpoints are configured as non-RAS endpoints. However, the private numbering plan has to be configured on both the MX H.323 Gatekeeper and the Succession 1000 H.323 Gatekeeper.

Hardware components

Branch Office

Overview

A Branch Office is built on an H.323 WAN Gateway platform. The BO chassis contains the Succession System Controller (SSC), a Succession Media Card, and three slots for flexible configuration of digital lines, analog lines, analog trunks, or digital trunks. An optional Expansion chassis provides

additional capacity for digital lines, analog lines, and analog trunks, but not digital trunks.

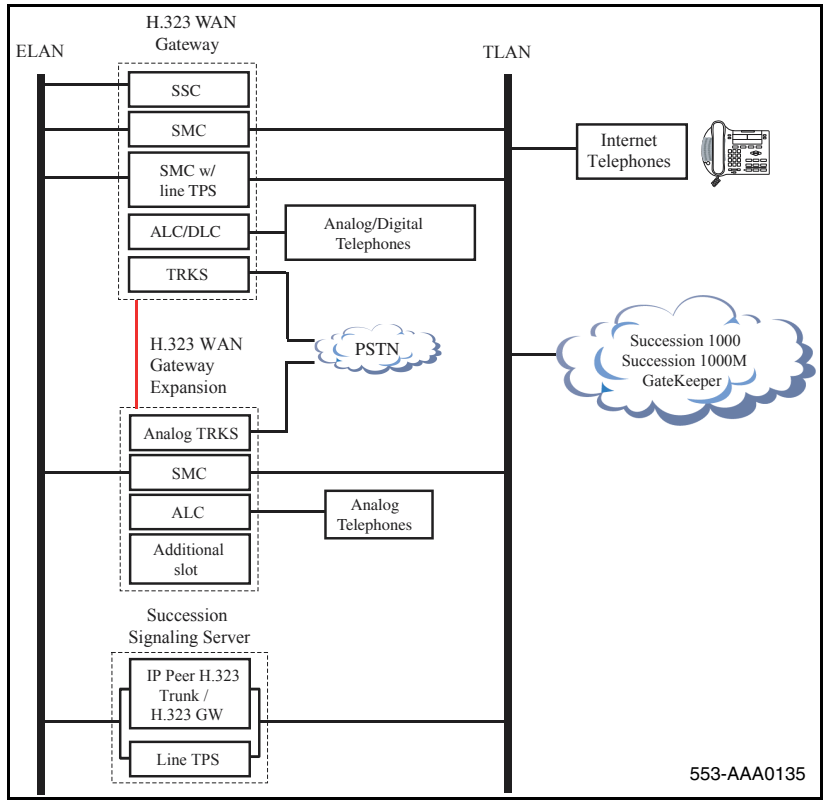
IP Peer networking and H.323 signaling between the Branch Office and the Main Office and other Branch Offices is handled by the Succession Signaling Server.

The Branch Office links to a Succession Call Server located in the Main Office. The Main Office Succession Call Server and the Branch Office Succession System Controller (SSC) are configured as ESN nodes and connected by Virtual Trunks. Access to PSTN digital or analog trunks at the Branch Office by Branch Users are tandemed through the Virtual Trunk.

Internet Telephones at the Branch Office are configured at, and registered with, the Main Office Succession Call Server. The Internet Telephones are controlled by the Main Office Succession Call Server and have access to the same feature set as other telephones at the Main Office. Internet Telephones physically located at a Branch Office are referred to as Branch Users.

Figure 46 on page 179 shows a Branch Office configured with a Branch Office H.323 WAN Gateway expansion.

Figure 46
Branch Office with H.323 Gateway Expansion



Branch Office H.323 WAN Gateway

The Branch Office H.323 WAN Gateway provides access to the local PSTN for users in the Branch Office. It also provides support for analog and digital devices such as fax machines or telephones in the Branch Office. For additional capacity, the H.323 WAN Gateway Expansion can be installed.

The Branch Office H.323 WAN Gateway has four “usable” slots, plus one (slot 0) for the mandatory Succession System Controller. The following can be installed in the other four “usable” slots:

- Succession Media Cards

- Digital Trunk Cards
- Analog Trunk Cards
- Digital Line Cards
- Analog Line Cards
- Meridian Integrated RAN (MIRAN) Card
- Meridian Integrated Conference Bridge (MICB)
- cards to support CallPilot Mini or CallPilot 201i

Succession System Controller (SSC)

The Succession System Controller is mandatory, and has a dedicated slot (slot 0) in the Branch Office H.323 WAN Gateway. In Normal Mode, the SSC acts as a telephony services controller for the Branch Office H.323 WAN Gateway elements. In Local Mode, the SSC also acts as a Succession Call Server for the Internet Telephones.

Succession Media Cards

Succession Media Cards provide echo cancellation, compression, and decompression of voice streams. They also contain a pool of Digital Signaling Processor (DSP) ports for media transcoding between IP voice packets and circuit-switched resources. Each call between an Internet Telephone and an analog telephone, digital telephone, or the PSTN uses one DSP port. Calls between two Internet Telephones do not require any DSP ports, because there is no need for IP-to-circuit-switched transcoding.

If the TPS facility on the Succession Signaling Server fails while the Branch Office is in Local Mode, the Succession Media Card provides a back-up Internet Telephone Terminal Proxy Server.

There are two types of Succession Media Cards: an 8-port and a 32-port card. Also supported is a legacy 24-port ITG-P card. If upgraded to IP Line 3.1 software, this 24-port card can be used as a Succession Media Card in place of the 8- or 32-port Media Card. However, the 24-port card is not optimal.

Analog or digital trunk cards

Trunk cards provide analog or digital interfaces to the PSTN. All analog and digital interfaces supported on Meridian are also supported in the Branch Office. The most commonly used cards are the XUT (NT8D14), the 1.5 Mb TMDI (NTRB21), the 2 Mb PRI, and the 2 Mb DTI. For information on trunk cards, refer to *Circuit Card: Description and Installation* (553-3001-211).

Analog or digital line cards

In the Branch Office, Analog and Digital Line Cards provide interfaces to analog and digital devices, respectively. When additional digital and analog telephones are located in the Branch Office, additional DSP resources are required. Refer to *Succession 1000 System: Planning and Engineering* (553-3031-120).

Succession Signaling Server

The Succession Signaling Server is mandatory in the Branch Office. It provides the following functions:

- IP Peer Networking, incorporating the Branch Office H.323 WAN Gateway and Gatekeeper
- Internet Telephone registration to the Internet Telephone Terminal Proxy Server (TPS) during Local Mode for survivability
- Web server for Element Manager

A second redundant Succession Signaling Server can be used to provide survivability in the case of a failure in the other (primary) Succession Signaling Server in the Branch Office.

IP Peer Networking

The Branch Office Succession Signaling Server provides IP Peer Networking, or H.323 signaling, from the Branch Office to the Main Office and other Branch Offices. It uses the IP Line 3.1, Gatekeeper, and Virtual Trunk applications. A Gatekeeper must be present within the network for Internet Telephones to be registered to the Main Office.

Internet Telephone Terminal Proxy Server (TPS)

The TPS is a signaling proxy software component for the Internet Telephones. When the Branch Office is in Local Mode, the Branch Office Succession Signaling Server registers Internet Telephones at the Branch Office to the Internet Telephone Terminal Proxy Server (TPS). If this functionality fails on the Branch Office Succession Signaling Server, the system uses the TPS on the Succession Media Card.

Web Server

The Element Manager Web-based interface supports the configuration of customer data blocks, Electronic Switched Networks (ESN) data, routes and trunks. It also supports Maintenance commands and other utilities.

Telephones and other devices

Internet Telephones

The Branch Office supports the i2002 and i2004 Internet Telephones, and the i2050 Software Telephone.

> ***Note:*** The term "Internet Telephones", as used in this document, includes the i2002, i2004, and i2050 devices.

Internet Telephones at the Branch Office are provisioned using Set-Based Installation, Command Line Interface (CLI) overlays, or Optivity Telephony Manager (OTM).

> ***Note 1:*** The MOTN can be configured with either two or four fields. It does not have to be the same format as the Branch Office TN.

Internet Telephones in the Branch Office must be running the minimum firmware release as stated in "Software requirements" on page 183. Refer to "Upgrading Internet Telephone firmware" on page 192 for information on upgrading firmware.

Each Succession 1000 or Succession 1000M Main Office can support up to 256 Branch Offices. Each Branch Office supports up to 400 Internet Telephone users. However, since all Internet Telephones register with the Main Office, the governing factor is the maximum number of Internet

Telephones that can be supported at the Main Office. This means the total number of Internet Telephones in all offices can be no greater than the capacity of the Main Office, as determined using *Succession 1000 System: Planning and Engineering* (553-3031-120), *Large System: Planning and Engineering* (553-3021-120), or *Small System: Planning and Engineering* (553-3011-120).

Digital and analog devices

Digital and analog telephones are supported in the Branch Office, but are managed at the Branch Office, not at the Main Office. To support a call between an Internet Telephone and an analog or digital telephone, a DSP resource is required. Therefore, when digital telephones are located in the Branch Office, configure additional voice gateway channels for IP-TDM connections.

Main Office

The Main Office must be one of the following systems:

- Succession 1000 (as shown in Figure 45 on page 171)
- Succession 1000M Cabinet
- Succession 1000M Chassis
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

Software requirements

The minimum software requirements for the Branch Office feature are as follows:

- Succession 3.0 Software (see note on page 184)
- IP Line 3.1
- Optivity Telephone Manager (OTM) 2.1

Both the Succession Call Server and Succession Signaling Server in an office must be running the same release of software. The Main Office must always be running Succession 3.0 Software on the Succession Call Server and Succession Signaling Server.

> ***Note:*** For Succession 1000 systems, existing Branch Offices running Succession 1000 Release 2.0 are still compatible with a Main Office running Succession 1000 Release 2.0. However, Nortel Networks recommends that customers upgrade these Branch Offices to Succession 3.0 Software within 30 days. Refer to "Mixed software operation between Main Office and Branch Office" on page 191.

Internet Telephones in the Branch Office must be running firmware version 1.39 or later.

Feature interactions

Call Detail Recording

There is no change to CDR record formats with the Succession Branch Office feature.

CallPilot Mini
CallPilot 201i

Succession Branch Office supports CallPilot Mini and CallPilot201i.

A Message Waiting Indication (MWI) will not survive a Mode change (Normal to Local or Local to Normal). The message itself is preserved, but the lamp indicator may not be lit after the Mode change.

Personal Call Assistant (PCA)

There is no interaction between Personal Call Assistant and the Succession Branch Office feature.

Virtual office

Succession Branch Office supports the Virtual Office feature.

When an Internet Telephone is in Local Mode, a Virtual Office Login is successful only if a Station Control Password is configured in the Branch Office.

Virtual Office Login is only permitted if the Internet Telephone is idle.

Virtual Office Login is not supported under Test Local Mode.

The system locks out a Branch Office Internet Telephone for one hour when a user enters an invalid password for the Virtual Office Login three consecutive times. The lock-out occurs whether the telephone is in Normal Mode or Local Mode.

VNR+

There is no interaction between VNR+ and the Succession Branch Office feature.

Voice Mail

Voice Mail service is provided by a Call Pilot in the Main Office or a Call Pilot Mini Call Pilot 201i in the Branch Office. In Normal Mode, both configurations are supported. In Local Mode, call treatment depends on where the call originates and where the Call Pilot Mini is deployed. Call treatments are summarized in Table 29 on page 185.

Table 29
Treatment of calls terminating to Branch Office telephones (Part 1 of 2)

	Treatment of calls to Branch Users in Local Mode	
Call origination	**Call Pilot in Main Office**	**Call Pilot Mini / CallPilot 201i in Branch Office**
Main Office CO into Main Office	Voice Mail boxes in Main Office	Ring No Answer treatment

Table 29
Treatment of calls terminating to Branch Office telephones (Part 2 of 2)

	Treatment of calls to Branch Users in Local Mode	
Call origination	**Call Pilot in Main Office**	**Call Pilot Mini / CallPilot 201i in Branch Office**
Branch Office CO into Branch Office	Telephones or Busy treatment	Telephones or Voice Mail boxes in Branch Office

Feature packaging

This feature is supported by Succession Branch Office (SBO) package 390. This package must be equipped on the Branch Office Succession System Controller (SSC).

Note: The Succession Branch Office (SBO) package 390 must not be equipped on the Succession Call Server in the Main Office.

To implement a Branch Office, the Main Office requires the following packages:

- Network Alternate Route Selection (NARS) package 58
- H323 Virtual Trunk (H323_VTRK) package 399
- Emergency Services Access (ESA) package 329. This package is optional, and is required only to get 911/ESA features in North American and some CALA markets. Refer to *Emergency Services Access: Description and Administration* (553-3001-313).
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional, and required only for Virtual Office functionality.

  Note: The Main Office must also have a Service Level of 2 or higher to interwork with the Branch Office.

At the Branch Office, the following packages are required:

- Flexible Numbering Plan (FNP) package 160
- Emergency Services Access (ESA) package 329
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387
- Succession Branch Office (SBO) package 390
- H323 Virtual Trunk (H323_VTRK) package 399

Note: These packages are automatically enabled in the Branch Office software.

The following packages are required when using set-based installation:

- Set Relocation (SR) package 53
- Flexible Feature Code (FFC) package 139
- Set-Based Installation (SET_INSTALL) package 200

The feature packages listed above are automatically included with the Branch Office software.

Note: The keycodes used to install software at the Branch Office differ from those used to install software at the Main Office.

Feature implementation

This section summarizes implementation and configuration for a Branch Office, as well as configuration for the related Main Office. It summarizes the overlays used.

Note: OTM and Element Manager can also be used to perform some steps. Refer to *Branch Office* (553-3001-214) for further information.

Implementation summary

To prepare for a Branch Office, refer to *Succession 1000 System: Planning and Engineering* (553-3031-120). This contains important electrical information and safety guidelines.

Follow these steps to implement a Succession 3.0 Branch Office.

1 At the Main Office:

- **a** Upgrade the Main Office software to Succession 3.0 Software. Refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258), *Large System: Upgrade Procedures* (553-3021-258), or *Small System: Upgrade Procedures* (553-3011-258).
- **b** If not already implemented, implement IP Peer Networking as part of a system installation or upgrade. Refer to *IP Peer Networking* (553-3001-213).
- **c** Configure the Branch Office zones. Refer to *Branch Office* (553-3001-214).
  - **i.** Configure the Customer Data Home Location Code and Virtual Private Network Identifier.
  - **ii.** Configure the Branch Office zones.
  - **iii.** Define the zone parameters for the Branch Office.
  - **iv.** Enable the features for the Branch Office zone.
- **d** Configure the Branch Office dialing plan. Refer to *Branch Office* (553-3001-214).
  - **i.** Configure the Zone Access Code Behavior (ZACB) and Zone Digit Prefix (ZDP) properties.
  - **ii.** Configure the Route List Index.
  - **iii.** Configure the ESN Special Number and Digit Manipulation.
- **e** Configure the Internet Telephone passwords. Refer to *Branch Office* (553-3001-214).
  - **i.** Configure the SCPW length in the Customer Data Block.

ii. Enable password change and set removal features.

f Use Gatekeeper Management to add the Host name of the Branch Office Succession Signaling Server to the Primary Gatekeeper H.323 Endpoint list. This enables the Succession Signaling Server at the Branch Office to register with the Gatekeeper. Refer to *IP Peer Networking* (553-3001-213).

2 At the Branch Office:

a Install the Branch Office H.323 WAN Gateway. Refer to *Branch Office* (553-3001-214).

b Install the Branch Office Succession Signaling Server. Refer to *Branch Office* (553-3001-214).

c Install the Branch Office software. Refer to *Branch Office* (553-3001-214).

Software for the Branch Office SSC comes with pre-programmed data that is selected during the installation procedure. For more information, refer to *Branch Office* (553-3001-214).

d Configure the Branch Office zone. Refer to *Branch Office* (553-3001-214).

i. Define the system date.

ii. Define the Branch Office zone properties.

iii. Configure Vacant Number Routing.

iv. Configure the Customer Data Home Location Code and Virtual Private Network Identifier.

e Configure the Branch Office dialing plan. Nortel Networks recommends that customers use CDP at the Branch Office. Refer to *Branch Office* (553-3001-214).

i. Configure the Route List Index.

ii. Configure the ESN Special Number and Digit Manipulation.

f Configure the Succession Media Cards. Refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Use the same zone for DSP physical TNs and Internet Telephone TNs. Refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

g Install and provision the local trunks (the XUT, PRI, and DTI cards). Refer to *Large System: Installation and Configuration* (553-3021-210).

h If applicable, configure Abbreviated Dialing. Refer to *Branch Office* (553-3001-214).

i Provision the Virtual Trunks. Refer to *IP Peer Networking* (553-3001-213).

j Install the Branch Office telephones and configure the Internet Telephone Passwords. Refer to *Branch Office* (553-3001-214).

Adding a Succession 3.0 Branch Office to an existing Succession 1000 Release 2.0 network

Succession 3.0 Branch Office requires a Main Office running Succession 3.0 Software. Therefore, the Main Office must be upgraded to Succession 3.0 Software before a Succession 3.0 Branch Office can be added.

Two options are available when adding a new Branch Office to an existing Succession 1000 Release 2.0 Main Office and Branch Office network. These options are:

1 Upgrade the entire network to Succession 3.0 Software, and then add the new Branch Office.

2 Upgrade only the Main Office to Succession 3.0 Software before adding the new Branch Office. This is only a temporary measure. In this case, you have two options:

a Upgrade the Internet Telephone firmware in the existing Succession 1000 Release 2.0 Branch Offices.

b Do not upgrade the Internet Telephone firmware in the existing Succession 1000 Release 2.0 Branch Offices.

Refer to *Branch Office* (553-3001-214) for detailed instructions.

Mixed software operation between Main Office and Branch Office

It is possible for the Main Office Call Server and the Branch Office to temporarily have different software releases, as long as the Main Office is running at the highest release (Succession 3.0 Software). In addition, it is possible to temporarily have Branch Offices running different software releases (Succession 1000 Release 2.0 or Succession 3.0 Software) associated with a given Succession 3.0 Main Office Call Server.

This is required to support customers who are currently running a network of Succession 1000 Release 2.0 Branch Office systems with a Succession 3.0 Main Office, and who want to add one Branch Office running Succession 3.0. It is also required for customers with a Succession 1000 Release 2.0 network who wish to upgrade to Succession 3.0 Software. By allowing this mixed software operation, customers will not have to upgrade their entire network from Succession 1000 Release 2.0 to Succession 3.0 Software at the same time. Instead, the network upgrade can be scheduled over a longer period.

This mixed software configuration between the Main Office and the Branch Office must only remain on a temporary basis. Customers must upgrade their Branch Offices to Succession 3.0 Software within 30 days. Indefinite operation with a mixed software configuration is not supported.

> ***Note 1:*** Both the Succession Call Server and Succession Signaling Server in an office must be running the same release of software.The Main Office must always be running Succession 3.0 Software on the Succession Call Server and the Succession Signaling Server.
>
> ***Note 2:*** If the Branch Office Gatekeeper is also the Alternate Gatekeeper in the network, it and the Primary Gatekeeper must be running the same release of software.

Feature operation of Internet Telephone users in Normal Mode is the feature set on the Main Office. Internet Telephone users in Local Mode use the feature set on the Branch Office. Branch Users of analog and digital devices always use the feature set on the Branch Office.

When the Branch Office is running the previous software release, the Local Mode features are limited to those available in that release. Depending on what is provisioned, this means that Normal Mode may have more features than Local Mode.

Internet Telephone Firmware

If adding a new Succession 3.0 Branch Office to a network that has Succession 1000 Release 2.0 Branch Offices, you must choose whether to upgrade Internet Telephone firmware for existing Branch Offices. You can choose not to upgrade the firmware at the existing Branch Offices only if the Internet Telephones in those Branch Offices are running at least the minimum version of firmware as specified in "Software requirements" on page 183.

If you choose to upgrade the firmware, you must upgrade the firmware at the existing Branch Offices first. The Main Office may or not require a firmware upgrade, depending on its current version.

Refer to the following section "Upgrading Internet Telephone firmware" for more information on upgrading firmware for i2002 and i2004 Internet Telephones.

Upgrading Internet Telephone firmware

Note: This section only applies to i2002 and i2004 Internet Telephones. It does not apply to i2050 Software Telephones.

When an Internet Telephone registers with a TPS, the TPS checks the firmware version in the Internet Telephone. If the firmware version differs from that required by the Succession Signaling Server (or the Succession Media Card) and the firmware upgrade policy requires an upgrade, the firmware is downloaded to the telephone. The telephone reboots after the firmware download is complete and registers with the TPS again.

When the Internet Telephone firmware in the TPS is upgraded, the Internet Telephones that registered with the Succession Call Server before the upgrade are not affected. The system administrator must execute the CLI command `umsUpgradeAll` to download firmware to all registered Internet Telephones that do not have the latest firmware. However, firmware

download is automatic for Internet Telephones that register to the TPS after the upgrade.

Firmware download does not happen when Internet Telephones register to the TPS by a Virtual Office Login or Branch Office redirection to the Main Office. Instead, Branch Office Internet Telephones are redirected back to the Branch Office TPS for firmware upgrade. This redirection occurs only if the `umsUpgradeAll` command is issued from the Main Office TPS, and the current firmware version does not match the Main Office TPS firmware policy.

If an Internet Telephone is in use when the `umsUpgradeAll` command is issued, the call is not interrupted. Its firmware version is checked against the Main Office TPS firmware policy, and if there is no match, the Internet Telephone is flagged, then redirected to the Branch Office TPS when the call is completed.

> ***Note:*** The `umsUpgradeAll` command has no immediate impact on Internet Telephones that are logged in or out by Virtual Office. However, the firmware may be upgraded, if required, when the Virtual Office session is terminated.

Each Internet Telephone that is redirected back to the Branch Office has its firmware version checked against the Branch Office TPS firmware policy. If there is no match, the firmware is upgraded automatically and the Internet Telephone is redirected back to the Main Office. If there is a match, the Internet Telephone stays in Local Mode, and displays the message "Required FW Vers xxxxxx".

This display can only be cleared by pressing the Cancel key. While this display appears, you can only receive calls; you cannot make outgoing calls.

> ***Note:*** If the Branch Office is running Succession Release 2.0, the display may clear after 30 seconds, depending on the status of the headset connection.

Software Input/Output prompts, responses, and commands

This section lists all software prompts, responses, and commands relevant to the Branch Office. For further information on overlays, refer to *Software*

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

Main Office configuration

The following overlays are used to configure a Main Office:

- LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier.
- LD 117 – Define zone properties at the Branch Office.
- LD 117 – Define zone parameters for the Branch Office.
- LD 117 – Enable features for the Branch Office zone.
- LD 15 – Configure the SCPW length in the Customer Data Block.
- LD 15 – Assign Automatic Set Relocation security code.
- LD 57 – Enable password change and set removal features.
- LD 11 – Provision Branch User and SCPW at the Main Office.

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 1 of 2)

Prompt	Response	Description
REQ:	CHG	Change existing data block
TYPE:	NET	ISDN and ESN Networking options
CUST	 0-99 0-31	Customer number For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems
...		
CLID	YES	Allow Calling Line Identification option
- ENTRY	xx	CLID entry to be configured
- - HLOC	100-9999999	Home location code (ESN) (3-7 digits)

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 2 of 2)

Prompt	Response	Description
ISDN	YES	Integrated Services Digital Network
- VPNI	(0)-16283	Virtual Private Network Identifier for Bandwidth Management Feature 0 or X = Disables feature 1-16383 = Enables feature <cr> = No Change

LD 117 – Define zone properties at the Branch Office. (Part 1 of 2)

Command	Description
NEW ZONE <xxx> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]	
	Create a new zone with the following parameters: • xxx = 0-255 zone number • intraZoneBandwidth = Intrazone available bandwidth (see Note 1 on page 197) 0-1000000 Kbps • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 197) • interZoneBandwidth = Interzone available bandwidth (see Note 1 on page 197) 0-1000000 Kbps • interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 197) • zoneResourceType = zone resource type (shared or private), where — shared = Current default zone type. The Internet Telephones configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: 1. channel from same zone as the Internet Telephone is configured 2. any available channel from the shared zones' channels — private = New zone type introduced by IPL 3.0. DSP channels configured in a private zone are only used by Internet Telephones which have also been configured for that private zone. If more DSP resources are required by these Internet Telephones than what are available in the zone, DSPs from other zones are used. However, Internet Telephones configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: 1. channel from same private zone as the Internet Telephone is configured 2. any available channel from the pool of shared zones' channels

LD 117 – Define zone properties at the Branch Office. (Part 2 of 2)

Command	Description
Note 1: If the Network Bandwidth Management feature is going to be used, the intraZoneBandwidth and interZoneBandwidth parameters must be set to the actual available bandwidth. Refer to “Network Bandwidth Management” on page 177. ***Note 2:*** If the Network Bandwidth Management feature is going to be used, and zone is going to be associated with a Virtual Trunk, the intraZoneStrategy and interZoneStrategy parameters must be set to BQ. Refer to “Network Bandwidth Management” on page 177.	

LD 117 – Define zone parameters for the Branch Office.

Command	Description
CHG ZBRN <zone> <yes no>	
	Define a zone as a Branch Office zone.
CHG ZDST <Zone> <yes/no> <StartMonth> <StartWeek> <StartDay> <StartHour> <EndMonth> <EndWeek> <EndDay> <EndHour>	
	If the Branch Office observes Daylight Savings Time (DST), these parameters specify the start and end of DST. During DST, the clock automatically advances one hour forward.
CHG ZTDF <Zone> <TimeDifferencefromMainOffice>	
	Specified in minutes, the time difference between Main Office and Branch Office when both are not in DST.
CHG ZDES <Zone> <ZoneDescription>	
	A name to render data display more meaningful.

LD 117 – Enable features for the Branch Office zone.

Command	Description
ENL ZBR <zone> ALL	Enable features for Branch Office <zone>.

LD 15 – Configure the SCPW length in the Customer Data Block.

Prompt	Response	Description
REQ:	CHG	Change existing data block
TYPE:	FFC	Flexible Feature Code
SCPL	0-8	Length of SCPW, minimum recommended is 4 digits.

LD 15 – Assign Automatic Set Relocation security code.

Prompt	Response	Description
REQ:	CHG	Change existing data block
TYPE:	FTR	Customer Features and options
CUST	 0-99 0-31	Customer number For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems
SRCD	(0000)-9999	Automatic Set Relocation security code. X removes security code.

LD 57 – Enable password change and set removal features. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create a new data block
TYPE	FFC	Flexible Feature Code
CUST	xx	Customer number, as defined in LD 15
FFCT	YES	Flexible Feature Confirmation Tone
CODE	AREM	Automatic Set Removal
- AREM	xxxx	Code to invoke Automatic Set Removal

LD 57 – Enable password change and set removal features. (Part 2 of 2)

Prompt	Response	Description
CODE	SCPC	Station Control Password Change
- SCPC	xxxx	Code to invoke password change

LD 11 – Provision Branch User and SCPW at the Main Office.

Prompt	Response	Description
REQ:	NEW CHG	Add or Change
TYPE:	 i2002 i2004 i2050	Terminal type. i2002 Internet Telephones i2004 Internet Telephones i2050 Softphone
CUST	xx	Customer number, as defined in LD 15
ZONE	0-255	Zone Number to which the Internet Telephone belongs. The zone prompt applies only when the type is i2002, i2004, or i2050. Zone number is not checked against LD 117.
...		
SCPW	xxxx	Station Control Password Must equal Station Control Password Length (SCPL) as defined in LD 15. Not prompted if SCPL = 0. Precede with X to delete.

Branch Office configuration

The following overlays are required to configure a Branch Office:

- LD 2 – Define system date.
- LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier.

- LD 15 – Configure Vacant Number Routing.
- LD 117 – Define zone properties at the Branch Office.

LD 2 – Define system date.

Command	Description
STAD dd mm yyyy hh nn ss	
	Set the time and date: STAD DAY MONTH YEAR HOUR MINUTE SECOND

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier.

Prompt	Response	Description
REQ:	NEW CHG	Add or Change existing data block
TYPE:	NET	ISDN and ESN Networking options
CUST ...	 0-99 0-31	Customer number For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems
CLID	YES	Allow Calling Line Identification Option
- ENTRY	xx	CLID entry to be configured
- - HLOC	100-9999999	Home location code (ESN) (3-7 digits)
ISDN	YES	Integrated Services Digital Network
- VPNI	(0)-16283	Virtual Private Network Identifier for Bandwidth Management Feature 0 or X = disables feature 1-16383 = enables feature <cr> = no change

LD 15 – Configure Vacant Number Routing.

Prompt	Response	Description
REQ:	NEW CHG	Add or Change existing data block
TYPE:	NET	Configure networking
VNR	YES	Vacant Number Routing
- RLI	0-999	Route List Index as defined in LD 86
- FLEN	1-(16)	Flexible length of digits expected
- CDPL	1-(10)	Flexible length of VNR CDP
- UDPL	1-(19)	Flexible length of VNR LOC

LD 117 – Define zone properties at the Branch Office.

Command	Description
NEW ZONE <xxx> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType>]	Create a new zone with the following parameters: • xxx = 0-255 zone number • intraZoneBandwidth = Intrazone available bandwidth (see Note) 0-100000 Kbps • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) • interZoneBandwidth = Interzone available bandwidth (see Note) 0-100000 Kbps • interzoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) • zoneResourceType = zone resource type (shared or private), where — shared = Current default zone type. The Internet Telephones configured in shared zones use DSP resources configured in shared zones. If all of the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. The order of channel selection for the gateway channels is: 1. channel from same zone as the Internet Telephone is configured 2. any available channel from the shared zones' channels — private = New zone type introduced by IPL 3.0. DSP channels configured in a private zone are only used by Internet Telephones which have also been configured for that private zone. If more DSP resources are required by these Internet Telephones than what are available in the zone, DSPs from other zones are used. However, Internet Telephones configured in shared zones cannot use the private zones' channels. The order of selection for the gateway channels is: 1. channel from same private zone as the Internet Telephone is configured 2. any available channel from the pool of shared zones' channels

Note: If the Network Bandwidth Management feature is going to be used, parameters intraZoneBandwidth and interZoneBandwidth must be set to the maximum configurable value. See "Network Bandwidth Management" on page 177.

Branch Office Internet Telephones installation

The following overlays are required to install Internet Telephones in the Branch Office:

- LD 11 – Provision Branch User and SCPW at the Branch Office.
- LD 11 – Enable/disable Virtual Office (optional).

Internet Telephones can also be installed using OTM or Set-Based Installation. Refer to *Branch Office* (553-3001-214) for details.

LD 11 – Provision Branch User and SCPW at the Branch Office. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add or Change
TYPE:	 i2002 i2004 i2050	Terminal type i2002 Internet Telephones i2004 Internet Telephones i2050 Softphone
CUST	xx	Customer number, as defined in LD 15
BUID	x...x	Branch User ID A dialable DN to call the telephone in Normal Mode from the Branch Office. Enter X to delete.
MOTN	 <cr> l s c u c u	Main Office TN Main Office TN is the same as the Branch Office TN For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems
ZONE	0-255	Zone Number to which the Internet Telephone belongs. The zone prompt applies only when the type is i2002, i2004, or i2050. Zone number is not checked against LD 117.

LD 11 – Provision Branch User and SCPW at the Branch Office. (Part 2 of 2)

Prompt	Response	Description
...		
SCPW	xxxx	Station Control Password Must equal Station Control Password Length (SCPL) as defined in LD 15. Not prompted if SCPL = 0. Precede with X to delete.

LD 11 – Enable/disable Virtual Office (optional).

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
TYPE:	a...a	Telephone type
CLS	(VOLA)	Allow Virtual Office operation from this TN
	VOLD	Deny Virtual Office operation from this TN
CLS	(VOUA)	Allow Virtual Office login onto this TN using other telephone (destination of Virtual Office login)
	VOUD	Deny Virtual Office login onto this TN using other telephone (destination of Virtual Office login)

Dialing Plan configuration

The following overlays are required to configure the dialing plan in the Main and Branch Offices:

- LD 117 – Define zone Access Code handling for the Branch Office zone at the Main Office.
- LD 117 – Define zone digit manipulation for the Branch Office zone at the Main Office.
- LD 86 – Configure Digit Manipulation Index at the Main Office.
- LD 86 – Configure Route List Index.

- LD 90 – Configure ESN Special Number and Digit Manipulation.
- LD 86 – Configure Digit Manipulation Index at the Branch Office.
- LD 90 – Configure ESN Special Number and Digit Manipulation.

LD 117 – Define zone Access Code handling for the Branch Office zone at the Main Office.

Command	Description
CHG ZACB <zone> [ALL]|[<AC1|AC2> <AC1|AC2>]	
	Define the Access Codes used to modify local or long distance calls in the Branch Office to force all Branch Office calls to be routed to the Branch Office PSTN.

LD 117 – Define zone digit manipulation for the Branch Office zone at the Main Office.

Command	Description
CHG ZDP <zone> <DialingCode1> <DialingCode2> <DialingCode3>	
	Define the dialing plan for the Branch Office zone, where DialingCode1, DialingCode2, and DialingCode3 are inserted into the dialed digits between the Access Code and the remainder of the dialed number.

LD 86 – Configure Digit Manipulation Index at the Main Office. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block.
CUST	xx	Customer number, as defined in LD 15.
FEAT	DGT	Digit manipulation data block
DMI	1-999	Digit Manipulation Index numbers The maximum number of Digit Manipulation tables is defined by prompt MXDM in LD 86.

LD 86 – Configure Digit Manipulation Index at the Main Office. (Part 2 of 2)

Prompt	Response	Description
DEL	(0)-19	Number of leading digits to be deleted, usually 0 at the Main Office.
INST	x...x	Insert. Up to 31 leading digits can be inserted, usually none at the Main Office. Default is none.
CTYP		Call Type to be used by the call. This call type must be recognized by the Gatekeeper and far-end switch. This is critical for correct CLID behavior.
	INTL	For off-net North American calls
	UKWN	For off-net non-North American calls
	LOC	For on-net calls

LD 86 – Configure Route List Index. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	RLB	Route List data block
RLI		Route List Index to be accessed
	0-127	CDP and BARS
	0-255	NARS
	0-999	FNP
ENTR	0-63	Entry number for NARS/BARS Route List
	X	Precede with X to remove
LTER	NO	Local Termination entry
ROUT		Route number of the Virtual Trunk, as provisioned in LD 16.
	0-511	For Succession 1000M Large Systems
	0-127	For Succession 1000M Small Systems and Succession 1000 systems

LD 86 – Configure Route List Index. (Part 2 of 2)

Prompt	Response	Description
...		
DMI	1-999	Digit Manipulation Index number as defined in LD 86, FEAT = DGT.

LD 90 – Configure ESN Special Number and Digit Manipulation.

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	NET	Network translation tables
TRAN	AC1	Translator – Access Code 1 (NARS/BARS) Because the call is incoming to the Branch Office, AC1 will be triggered. (Ensure that INAC = YES in the Route Block for the Virtual Trunk in LD 16).
TYPE	SPN	Special code translation data block
SPN	x...x	Special Number translation Enter the SPN digits in groups of 3 or 4 digits, separated by a space (for example, xxxx xxx xxxx). The SPN can be up to 19 digits long. The maximum number of groups allowed is 5.
- FLEN	(0)-24	Flexible Length The number of digits the system expects to receive before accessing a trunk and outpulsing these digits.
...		
- RLI	0-999	Route List Index configured in LD 86

LD 86 – Configure Digit Manipulation Index at the Branch Office.

Prompt	Response	Description
REQ	NEW	Create new data block.
CUST	xx	Customer number, as defined in LD 15.
FEAT	DGT	Digit manipulation data block
DMI	1-999	Digit Manipulation Index numbers The maximum number of Digit Manipulation tables is defined by prompt MXDM in LD 86.
DEL	(0)-19	Number of leading digits to be deleted. This would normally be configured to remove the unique non-dialable number that identifies the Branch Office, configured in the ZDP property of the Branch Office zone in LD 117 at the Main Office.
INST	x...x	Insert. Up to 31 leading digits can be inserted.
CTYP	<cr>	Call Type to be used by the call. This call type must be recognized by the far-end switch. <cr> = Incoming call type will not be changed.

LD 86 – Configure Route List Index. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	RLB	Route List data block
...		
RLI	 0-127 0-255 0-999	Route List Index to be accessed CDP and BARS NARS FNP

LD 86 – Configure Route List Index. (Part 2 of 2)

Prompt	Response	Description
ENTR	0-63 X	Entry number for NARS/BARS Route List Precede with x to remove
LTER	NO	Local Termination entry
ROUT ...	 0-511 0-127	Route number of the Virtual Trunk, as provisioned in LD 16. For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems
DMI	1-999	Digit Manipulation Index number, as defined in LD 86, FEAT = DGT.

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	NET	Network translation tables
TRAN	AC1	Translator – Access Code 1 (NARS/BARS) Because the call is incoming to the Branch Office, AC1 is triggered. (Ensure that INAC = YES in the Route Block for the Virtual Trunk in LD 16).
TYPE	SPN	Special code translation data block
SPN	x...x	Special Number translation Enter the SPN digits in groups of 3 or 4 digits, separated by a space (for example, xxxx xxx xxxx). The SPN can be up to 19 digits long. The maximum number of groups allowed is 5.

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 2 of 2)

Prompt	Response	Description
- FLEN	(0)-24	Flexible Length The number of digits the system expects to receive before accessing a trunk and outpulsing these digits.
...		
- RLI	0-999	Route List Index configured in LD 86

Emergency services configuration

The following overlays are required to configure Emergency Services Access (ESA):

- LD 24 – Configure Emergency Services Access.
- LD 117 – Configure Branch Office zone ESA route.
- LD 86 – Configure Digit Manipulation Index.
- LD 86 – Configure Route List Index.
- LD 90 – Configure ESN Special Number and Digit Manipulation.

LD 24 – Configure Emergency Services Access. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	New or Change
TYPE	ESA	Emergency Services Access data block
CUST	xx	Customer number, as defined in LD 15
ESDN	xxxx	Emergency Services DN (for example, 911). Up to four digits are accepted.
ESRT	 0-511 0-127	ESA route number For Succession 1000M Large Systems For Succession 1000M Small Systems and Succession 1000 systems

LD 24 – Configure Emergency Services Access. (Part 2 of 2)

Prompt	Response	Description
DDGT	x...x	Directing Digits (for example, 1, 11, or 911). Up to four digits are accepted.
DFCL	x...x	Default ESA Calling Number. The input must be the following lengths: • On a system that is not FNP equipped, 8 or 11 digits are accepted if the first digit of the input is '1'; otherwise the input must be 7 or 10 digits. • On a system that is FNP equipped, up to 16 digits are allowed.
OSDN	x...x	On-Site Notification station DN. The input must be a valid single appearance internal DN.

LD 117 – Configure Branch Office zone ESA route.

Command	Description
CHG ZESA <Zone><ESA Route #><AC><ESA Prefix><ESA Locator>	
	Defines the ESA parameters for the Branch Office zone, where: • Zone = Zone number for the Branch Office. • ESA Route # = Virtual Trunk route to Branch Office Gateway. • AC = Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2. • ESA Prefix = Digit string added to start of ESDN. This is a unique prefix in the Gatekeeper. Nortel Networks recommends that users use "0" + ESN location code of the Branch node. An example for location code 725 would be: 0725. • ESA Locator = Direct-inward-dial telephone number to be sent as part of ANI for use by the PSAP to locate the source of the call.

LD 86 – Configure Digit Manipulation Index.

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	DGT	Digit manipulation data block
DMI	 (0) (0)-31 (0)-255 (0)-999	Digit Manipulation Index numbers No digit manipulation required CDP NARS and BARS NARS and BARS with FNP DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID. The maximum number of Digit Manipulation tables is defined by prompt MXDM. DMI is not prompted if route TKTP = ADM.
DEL	(0)-19	Number of leading digits to be deleted
INST	x...x	Insert. Up to 31 leading digits can be inserted.
CTYP	<cr>	Call Type to be used by the manipulated digits. This call type must be recognized by the far-end switch.

LD 86 – Configure Route List Index. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	RLB	Route List data block
...		

LD 86 – Configure Route List Index. (Part 2 of 2)

Prompt	Response	Description
RLI		Route List Index to be accessed
	0-127	CDP and BARS
	0-255	NARS
	0-999	FNP
ENTR	0-63	Entry number for NARS/BARS Route List
	0-6	Route List entry number for CDP
	X	Precede with X to remove
LTER	NO	Local Termination entry
ROUT		Route number
	0-511	For Succession 1000M Large Systems
	0-127	For Succession 1000M Small Systems and Succession 1000 systems
DMI	(0)-999	Digit Manipulation Index number as previously defined in LD 86, FEAT = DGT.

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	NET	Network translation tables
TRAN		Translator
	AC1	Access Code 1 (NARS/BARS)
	AC2	Access Code 2 (NARS)
TYPE	SPN	Special code translation data block

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 2 of 2)

Prompt	Response	Description
SPN	x...x	Special Number translation Enter the SPN digits in groups of 3 or 4 digits, separated by a space (for example, xxxx xxx xxxx). The SPN can be up to 19 digits long. The maximum number of groups allowed is 5.
- FLEN	(0)-24	Flexible Length The number of digits the system expects to receive before accessing a trunk and outpulsing these digits.
...		
- RLI		Route List Index to be accessed
	0-127	CDP and BARS
	0-255	NARS
	0-999	FNP
...		
- SDRR		Supplemental Digit Restriction or Recognition
	ALOW	Allowed codes
	ARRN	Alternate Routing Remote Number
	DDD	Recognized remote Direct Distance Dial codes
	DENY	Restricted codes
	DID	Recognized remote Direct Inward Dial codes
	ITED	Incoming Trunk group Exclusion Digits
	LDDD	Recognized Local Direct Distance Dial codes
	LDID	Recognized Local Direct Inward Dial codes
	STRK	For ADM/MDM trunk groups
	<cr>	Return to SPN
- - DMI	1-255	Digit Manipulation Index
	1-999	Digit Manipulation Index with FNP DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID.

Abbreviated Dialing configuration

Abbreviated Dialing must be configured in both the Main Office and the Branch Office. The following overlays are required to configure Abbreviated Dialing:

- LD 18 – Configure Speed Call Lists (SCL) for each zone.
- LD 18 – Configure default Speed Call List.
- LD 18 – Configure Pretranslation Group for each zone.
- LD 18 – Configure default Pretranslation Group.
- LD 15 – Activate Pretranslation feature.
- LD 11 – Assign Pretranslation Group to telephones.
- LD 15 – Configure Flexible Code Restriction (FCR) for Incoming DID Digit Conversion.
- LD 49 – Configure Incoming DID Digit Conversion (IDC).
- LD 49 – Configure Flexible Code Restriction (FCR).
- LD 16 – Configure Route Data Block.

LD 18 – Configure Speed Call Lists (SCL) for each zone. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	New
TYPE	SCL	Speed Call List
LSNO	0-8190	List Number
DNSZ	4-(16)-31	Maximum number of DNs allowed for Speed Call Lists.
SIZE	0-1000	Maximum number of DNs in Speed Call List.
WRT	(YES) NO	Data is correct and can be updated in the data store.
STOR	0-999 yyy...y	Entry number and the digits stored with it.

LD 18 – Configure Speed Call Lists (SCL) for each zone. (Part 2 of 2)

Prompt	Response	Description
WRT	(YES) NO	Data is correct and can be updated in the data store.
Note: The STOR and WRT prompts are repeated in sequence for each number in the SCL.		

LD 18 – Configure default Speed Call List.

Prompt	Response	Description
REQ	NEW	New
TYPE	SCL	Speed Call List
LSNO	0	Default SCL
DNSZ	4-(16)-31	Maximum number of DNs allowed for Speed Call Lists.
SIZE	0-1000	Maximum number of DNs in Speed Call List.
WRT	(YES) NO	Data is correct and can be updated in the data store.
STOR	<cr>	Accept default
WRT	(YES) NO	Data is correct and can be updated in the data store.

LD 18 – Configure Pretranslation Group for each zone.

Prompt	Response	Description
REQ	NEW	New
TYPE	PRE	Pretranslation Group
XLAT	0-8191	Zone number. Correlates Pretranslation Group to Speed Call List.
- PRE	0-8190	Pretranslation Speed Call List Number. Corresponds to LSNO defined in LD 18, TYPE=SCL.

LD 18 – Configure default Pretranslation Group.

Prompt	Response	Description
REQ	NEW	New
TYPE	PRE	Pretranslation Group
XLAT	0	Default Zone number
- PRE	0	Default Pretranslation Speed Call List Number

LD 15 – Activate Pretranslation feature.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	FTR	Features and options
...		
PREO	1	Activate Pretranslation feature
...		

LD 11 – Assign Pretranslation Group to telephones.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	a...a	Telephone type
...		
XLST	(0)-254	Pretranslation Group associated with this station.
...		

LD 15 – Configure Flexible Code Restriction (FCR) for Incoming DID Digit Conversion.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	FCR	Flexible Code Restriction
...		
NFCR	YES	Enable new Flexible Code Restriction.
...		
IDCA	YES	Incoming DID Digit Conversion allowed.
- DCMX	1-255	Maximum number of IDC conversion tables.
...		

LD 49 – Configure Incoming DID Digit Conversion (IDC).

Prompt	Response	Description
REQ	NEW	New
TYPE	IDC	Incoming Digit Conversion
DCNO	0-254	Digit Conversion tree number (IDC tree number).
...		
IDGT <0-9999>	0-9999 0-9999	Incoming Digits (DN or range of DNs to be converted).The external DN to be converted is output and the users enter the internal DN. For example, to convert the external DN 3440 to 510, enter: Prompt: Response IDGT: 3440 3440: 510
...		

LD 49 – Configure Flexible Code Restriction (FCR).

Prompt	Response	Description
REQ	NEW	New
TYPE	FCR	Flexible Code Restriction
CRNO	(0)-254	Code Restriction tree number
INIT	ALOW	Allow all codes
...		

LD 16 – Configure Route Data Block.

Prompt	Response	Description
REQ	CHG	Change
TYPE	RDB	Route Data Block
...		
IDC	YES	Incoming DID Digit Conversion on this route.
- DCNO	(0)-254	Day IDC tree number
- NDNO	0-254	Night IDC tree number
...		

Maintenance

The following overlays are required to perform system maintenance:

- LD 117 – Print zone information.
- LD 117 – Enable/Disable Branch Office zone features.
- LD 117 – Display zone status.
- LD 117 – Display inventory.
- LD 22 – Print Branch Office software and system information.

LD 117 – Print zone information.

Command	Description
PRT ZACB [<Zone>]	
	Print a table of Branch Office zone dialing plan entries.
PRT ZBW [<Zone>]	
	Print a table of zone bandwidth utilization.
PRT ZDES [<DESMatchString>]	
	Print a table of the zone description entries.
PRT ZDP [<Zone>]	
	Print a table of Branch Office zone dialing plan entries.
PRT ZDST [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.
PRT ZESA [<Zone>]	
	Print a table of Branch Zone Emergency Services Access parameters.
PRT ZONE ALL	Print zone information for all zones.
PRT ZONE 0-255	Print zone information for a specific zone.
PRT ZTDF [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.
PRT ZTP [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.

LD 117 – Enable/Disable Branch Office zone features.

Command	Description
ENL ZBR [<Zone>] [ALL] [LOC] [ESA] [TIM]	
	Enable features for the Branch Office zone. If no specific features are specified, ALL is assumed.
DIS ZBR [<Zone>] [ALL] [LOC] [ESA] [TIM]	
	Disable features of the Branch Office zone. If no specific features are specified, ALL is assumed.

LD 117 – Display zone status.

Command	Description
STAT ZONE [<Zone>]	
	Display zone status table
STAT ZBR [<Zone>]	
	Display status of Branch Office zones (displays which local dialing)

LD 117 – Display inventory.

Command	Description
INV PRT	Print STATUS, CARDS, SETS or ALL
INV GENERATE	Generate inventory CARDS, SETS, ALL or ABORT
INV MIDNIGHT	Generate inventory CARDS, SETS, ALL, OFF or STATUS

LD 22 – Print Branch Office software and system information.

Prompt	Response	Description
REQ	ISS	Print issue and release
REQ	ISSP	Print system and patch information
Note: If Branch Office (SBO) package 390 is equipped, these commands output the relevant information for the Branch Office. If package 390 is not equipped, the output is the information for the Succession Call Server.		

System Messages

This section lists all system messages relevant to the Branch Office. They are described in Table 30.

Table 30
System messages (Part 1 of 2)

Message Mnemonic	Severity	Event	Action
BUG0103	Info	Internet Telephones have been serviced at the Branch Office in survival mode beyond the licensed period.	Use Branch User Config to redirect the sets to the Main Office, restore the IP link between the Main Office and the Branch Office, or do a software installation.
ITS4012	Info	User entered the wrong Branch Office Internet Telephone password three times during Branch User Config. The set is locked out from doing Branch User Config for one hour.	Action: Wait for the set to unlock in one hour, or use the IPL CLI command *clearLockout* to unlock the set.

Table 30
System messages (Part 2 of 2)

Message Mnemonic	Severity	Event	Action
SRPT0108	Minor	VO login Password retry failed 3 times. Tried to login as TN: 0x%x on the set TN: 0x%x.	Let the login lock expire in one hour, or disable/enable the set to login through LD 32.
SYS0116	Severe	The zone database is corrupt. One or more entries have not been loaded.	Verify zones in Overlay 117. Zones that did not load could be out-of-service. If the problem persists, re-enter the zone configuration or restore the zone table from back-ups.

For further information on System Messages, refer to *Software Input/Output: System Messages* (553-3001-411)

Feature operation

A Branch Office Internet Telephone is operational immediately after configuration. A few operations are given in this section. Refer to *Internet Terminals: Description* (553-3001-368) for additional information.

Changing the Station Control Password (SCPW)

You can change the SCPW of a telephone at any time by following this procedure.

Procedure 12
Changing the SCPW

1. Dial the SCPC code followed by the current station control password. An FFC tone is given.
2. Enter the new password (the new password must have the same length as SCPL).

3 Wait for the FFC tone and enter the new password again. If the new password is accepted, another FFC tone is given; otherwise, an overflow tone is given.

End of Procedure

Telephone Option

See *Internet Terminals: Description* (553-3001-368) for details on the Telephone Option feature.

Procedure 13
Using the Option feature

This procedure explains how to use Internet Telephone Option features. The Internet Telephone has been configured using Branch User Config and is operating in Normal Mode.

1 Press the Services key (the key with the Globe icon) to bring up the Options menu on the display. The menu contains the following items:

- Telephone Options
- Virtual Office Login
- Test Local Mode

Note: The i2002 telephone has a one-line display, so scroll to view all menu items.

2 Use the Down key to highlight **Telephone Option**.

3 Press the **Select** softkey to activate the feature.

4 Scroll through the options and select one.

5 Follow the screen prompts to enter data if necessary.

6 Press the Services key or the **Cancel** softkey to exit the Services menu.

End of Procedure

Virtual Office login on the Branch

Details of the Virtual Office Login feature are described in *Internet Terminals: Description* (553-3001-368).

Procedure 14
Using the Virtual Office Login feature

This procedure explains how to log into and out of Virtual Office. The Internet Telephone has been configured using Branch User Config and is operating in Normal Mode.

1. Press the Services key (the key with the Globe icon) to display the Options menu.
2. Use the Down key to highlight the Virtual Office Login.
3. Press the **Select** softkey. The screen prompts for the User ID.
4. Enter the User ID, the user's dialable DN with the Access Code.

   Note: The User ID must be an ESN number.
5. Enter the Station Control Password for the Main Office Internet Telephone.

   A "Locating Remote Server" appears on the display.
6. To log out, use the arrow key to highlight **Virtual Office Logout**, and press **Select**.

End of Procedure

Test Local Mode

Test Local Mode is used to test the survivability of the Internet Telephone. Refer to "Survivability" on page 175.

Procedure 15
Using the Options feature

This procedure explains how to test the Internet Telephone in Local Mode. The Internet Telephone has been configured using Branch User Config and is operating in Normal Mode.

1 Press the Services key (the key with the Globe icon) to bring up the Options menu. The menu contains the following items:

- Telephone Options
- Virtual Office Login
- Test Local Mode

Note: The i2002 telephone has a one-line display, so scroll to display all menu items.

2 Use the Down key to highlight **Test Local Mode**.

3 Press the **Select** softkey to activate the feature.

4 Make and receive a call to the telephone.

5 Use the Resume Normal Mode command (under the Services key, Options menu) to redirect the telephone to the Main Office TPS node (which reregisters the telephone at the Main Office).

End of Procedure

Succession 3.0 Software enhancements

Note: This section identifies Succession Branch Office enhancements implemented in Succession 3.0 Software. Details of these enhancements have already been given throughout this chapter. They are repeated here for concise reference by users already familiar with Branch Office concepts and functionality.

Succession Branch Office enhancements implemented in Succession 3.0 Software include the following:

- Abbreviated Dialing feature
- mixed software operation between Main Office and Branch Office
- automatic redirection to Main Office following MOTN or BUID configuration change for Branch User in Local Mode
- Main Office TN can differ from Branch Office TN for a given Branch User with a small system at the Main Office
- support for media redirection by Network Bandwidth Management

- configuration of alternate routes and support for international calls in Vacant Number Routing
- new and modified ISM parameters
- enhanced CHG ZACB command in LD 117
- expanded isetShow output
- new print zone information commands in LD 117
- enhanced ISS and ISSP prompts in LD 22 for Branch Office

Abbreviated Dialing

The Abbreviated Dialing feature allows users in the same geographic location—Main Office or Branch Office—to call one another with a DN shorter than the configured DN.

To configure Abbreviated Dialing:

1 Configure Speed Call Lists.

2 Configure Pretranslation Groups.

3 Assign Pretranslation Groups to the telephones.

4 Configure Incoming DID Digit Conversion.

Refer to *Branch Office* (553-3001-214) for detailed information on implementing this feature.

Mixed software operation between Main Office and Branch Office

It is possible for the Main Office Call Server and the Branch Office to temporarily have different software releases, as long as the Main Office is running at the highest release (Succession 3.0 Software). In addition, it is possible to temporarily have Branch Offices running different software releases (Succession 1000 Release 2.0 or Succession 3.0 Software) associated with a given Succession 3.0 Main Office Call Server.

This is required to support customers who are currently running a network of Succession 1000 Release 2.0 Branch Office systems with a Succession 3.0

Main Office, and who want to add one Branch Office running Succession 3.0. It is also required for customers with a Succession 1000 Release 2.0 network who wish to upgrade to Succession 3.0 Software. By allowing this mixed software operation, customers will not have to upgrade their entire network from Succession 1000 Release 2.0 to Succession 3.0 Software at the same time. Instead, the network upgrade can be scheduled over a longer period.

This mixed software configuration between the Main Office and the Branch Office must only remain on a temporary basis. Customers must upgrade their Branch Offices to Succession 3.0 Software within 30 days. Indefinite operation with a mixed software configuration is not supported.

> ***Note 1:*** Both the Succession Call Server and Succession Signaling Server in an office must be running the same release of software.The Main Office must always be running Succession 3.0 Software on the Succession Call Server and the Succession Signaling Server.
>
> ***Note 2:*** If the Branch Office Gatekeeper is also the Alternate Gatekeeper in the network, it and the Primary Gatekeeper must be running the same release of software.

Feature operation of Internet Telephone users in Normal Mode is the feature set on the Main Office. Internet Telephone users in Local Mode use the feature set on the Branch Office. Branch Users of analog and digital devices always use the feature set on the Branch Office.

When the Branch Office is running the previous software release, the Local Mode features are limited to those available in that release. Depending on what is provisioned, this means that Normal Mode may have more features than Local Mode.

Internet Telephone Firmware

If adding a new Succession 3.0 Branch Office to a network that has Succession 1000 Release 2.0 Branch Offices, you must choose whether to upgrade Internet Telephone firmware for existing Branch Offices. You can choose not to upgrade the firmware at the existing Branch Offices only if the Internet Telephones in those Branch Offices are running at least the minimum version of firmware as specified in “Software requirements” on page 183.

If you choose to upgrade the firmware, you must upgrade the firmware at the existing Branch Offices first. The Main Office may or not require a firmware upgrade, depending on its current version.

Refer to "Upgrading Internet Telephone firmware" on page 192 for more information on upgrading firmware for i2002 and i2004 Internet Telephones.

Automatic redirection to Main Office

If the MOTN or BUID for a Branch User in Local Mode is reconfigured, the Internet Telephone is automatically redirected to the Main Office. No manual intervention, such as the `Resume Normal Mode` command or a reset is required to redirect the Internet Telephone to the Main Office.

Terminal numbers (TN)

Main Office TNs can be entered in either large system format (four fields) or small system format (two fields). For new TNs, the default is Branch Office format (small system, or two fields).

For any given Branch User, the Main Office TN can differ from the Branch Office TN, even if the Main Office is a Succession 1000 or a Succession 1000M Small System.

Network Bandwidth Management

The Network Bandwidth Management feature has been enhanced to support media redirection, in addition to basic call scenarios. The zone table is updated accordingly.

Vacant Number Routing

Vacant Number Routing (VNR) has been enhanced to enable the configuration of alternate routes. These alternate routes can be used for the VNR route, providing more flexibility to the user.

The flexible length of UDP digits has been increased from 10 to 19 to enable international calls. The prompt 'LOCL' in LD 15 has also been renamed 'UDPL' to reflect this.

LD 15 – Enhanced prompt for Vacant Number Routing

Prompt	Response	Description
- UDPL	**1-(19)**	**Flexible length of VNR LOC** **Formerly known as "LOCL"**

ISM parameters

The ISM parameter PCA, with a default value of 0, has been added.

The ISM parameter VIRTUAL TRUNKS has been renamed IP PEER H.323 TRUNKS, and is used in place of the ITG_ISDN TRUNKS parameter.

The default values of the following ISM parameters have been modified:

- AST (400)
- ANALOGUE TELEPHONES (0)
- CLASS TELEPHONES (0)
- INTERNET TELEPHONES (400)
- PHANTOM PORTS (400)
- WIRELESS TELEPHONES (0)
- WIRELESS VISITORS (0)
- ITG_ISDN TRUNKS (0) – This parameter is no longer applicable to the Branch Office, and its default value has been changed to zero. The IP PEER H.323 TRUNKS parameter is used in its place.

The ANALOGUE TELEPHONES and CLASS TELEPHONES parameters are now set to zero for Succession 3.0, allowing customers to order them in increments of eight.

Expanded isetShow report

Two fields have been added to the report produced by the isetShow command:

- `RegdTN`
- `UNIStimVsn`

Two fields have been renamed:

- `Reg` changed to `RegType`
- `TN` changed to `Set-TN`

Refer to *Branch Office* (553-3001-214) for more information on this command.

Enhanced CHG ZACB command in LD 117

In the CHG ZACB command in LD 117, the new value ALL indicates that both Access Codes are to receive digit manipulation to force all Branch Office calls to be routed to the Branch Office PSTN.

LD 117 – Updated CHG ZACB command.

Command	Description
CHG ZACB <Zone> [ALL]|[<AC1|AC2> <AC1|AC2>]	
	Define the Access Codes used to modify local calls in the Branch Office zone, where: • ALL = both AC1 and AC2 receive digit manipulation to force all Branch Office calls to be routed to the Branch Office PSTN. • <AC1|AC2> <AC1|AC2> = Access Codes — The first Access Code parameter specifies the NARS Access Code to which the feature should be applied. All digit strings in the zone that start with digits matching the specified access code will be processed. — The second Access Code parameter defines the replacement NARS Access Code after processing. — If the values of the two Access Code parameters are identical (for example, AC1), the other Access Code (for example, AC2) does not receive digit manipulation. If no Access Code parameters are specified, neither Access Code is considered for digit manipulation. In the typical case of PSTN, long distance is AC1 and local calls is AC2. For example, CHG ZACB <zone> AC2 AC1.

New print zone information commands in LD 117

Five commands have been added to LD 117 to print information about a zone.

LD 117 – New print zone information commands. (Part 1 of 2)

Command	Description
PRT ZACB [<Zone>]	
	Print a table of Branch Office zone dialing plan entries.
PRT ZDST [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.

LD 117 – New print zone information commands. (Part 2 of 2)

Command	Description
PRT ZESA [<Zone>]	
	Print a table of Branch Zone Emergency Services Access parameters.
PRT ZTDF [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.
PRT ZTP [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.

Enhanced ISS and ISSP prompts in LD 22

If Branch Office package 390 is equipped on the Branch Office Succession System Controller (SSC), the ISS and ISSP prompts in LD 22 return status information about the Branch Office, not the Main Office Succession Call Server. The output is clearly headed with the term “Branch Office” instead of “Call Server”. Refer to *Software Input/Output: Administration* (553-3001-311) for more information.

End of Procedure

Meridian 1 Option 61C CP PII enhancements

Contents

This section contains information on the following topics:

Introduction

The Meridian 1 Option 61C CP PII is a dual Pentium II Processor system with standby processing capability, fully redundant memory, and a full network group. Two Core/Net modules and one IPE module are the minimum installation requirements. Additional IPE modules and application modules can be used.

Succession 3.0 introduces enhancements to the Meridian 1 Option 61C CP PII system. This chapter describes these enhancements.

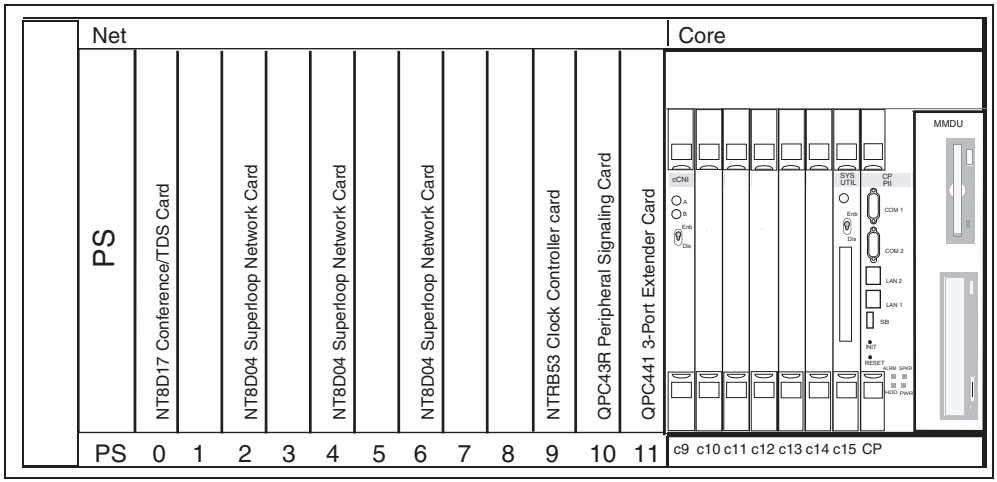
Hardware modifications

The Meridian 1 Option 61C CP PII and Meridian 1 Option 81C CP PII feature an updated NT4N41 Core/Net module (see Figure 47 below), allowing Succession 3.0 Software to support a unified hardware platform for

both single-group and multi-group configurations for CP PII systems. This platform allows:

- one generic CD-ROM for all CP PII systems
- upgrades from single-group to multi-group configurations (requiring a new keycode file and any additional hardware necessary for a multi-group system)

Figure 47
NT4N41 Core/Net module (Meridian 1 Option 61C CP PII example)

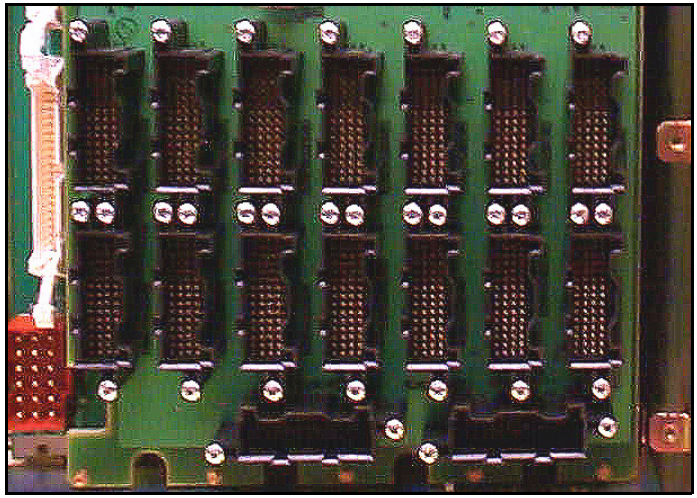


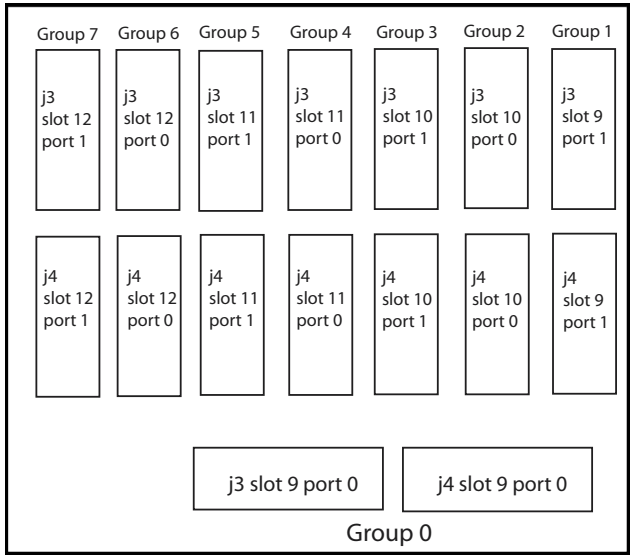
553-9123r26revised

The NT4N41 Core/Net module is updated as follows:

- The cPCI shelf is integrated into the Core/Net module.
- The NT4N48AA System Utility card incorporates the functionality of the System Utility Transition card, LCD display, and the security device holder.
- The LCD display is located on the System Utility card (formerly located on the front chassis).
- A fanout panel (see Figure 48 on page 237) replaces the Transition cards (cCNI Transition card and System Utility Transition card) and provides connectivity to the network shelf.

Figure 48
Fanout panel (backplane)





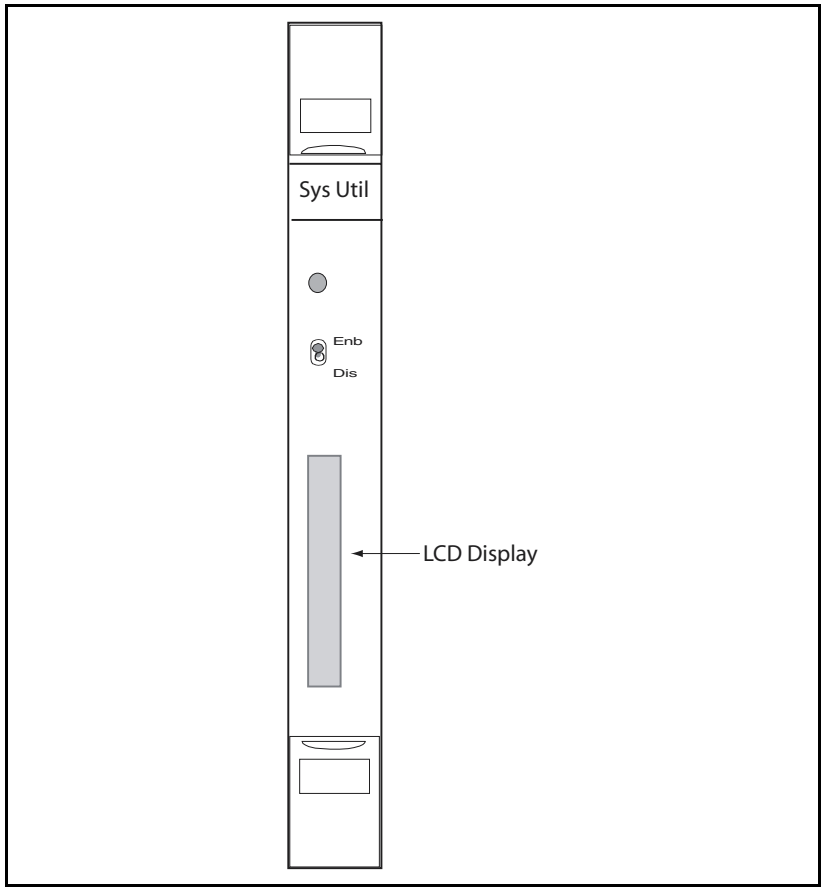
The NT4N41 Core/Net module is identical for Meridian 1 Option 61C CP PII and Meridian 1 Option 81C CP PII, with the following exceptions for Meridian 1 Option 61C CP PII:

- Only one cCNI card is required. This card must be installed in slot c9 in the Core/Net module and configured as group 0.
- Only one connection is required between the cCNI and the 3PE for group 0 using cable NT4N29.
- IGS/FNF cards and associated cables are not required.
- The Clock Controller card occupies card slot 9 in group 0.

System Utility card

Both Large Systems include an NT4N48AA System Utility card, located in slot c15 of the Core/Net module (see Figure 49 on page 239).

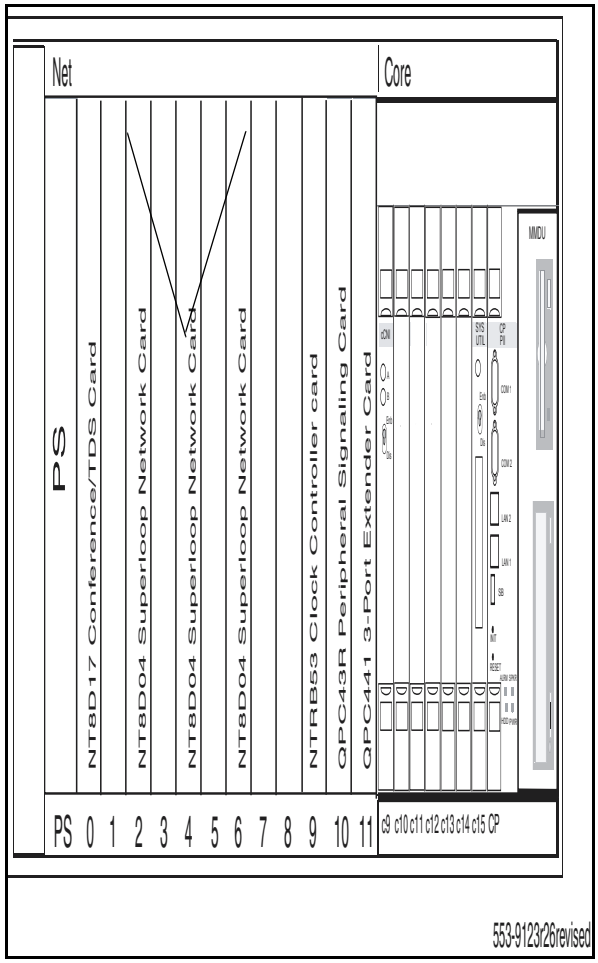
Figure 49
NT4N48AA System Utility card



Security Device

The Security Device Holder has been replaced. The Security Device now fits into the NT4N48AA System Utility card (see Figure 50 on page 240).

Figure 50
System Utility card Security Device



Software modifications

Keycodes

The keycode generation procedure includes system version 3211 for Meridian 1 Option 61C CP PII.

Sysload

Sysload recognizes and stores system version 3211 for Meridian 1 Option 61C CP PII.

CD-ROM Media

The installation CD-ROM is generic for Large Systems and includes an additional subdirectory for system version 3211.

Install Disks

Two separate Install Disks (floppy) are used for individual system version 3211 (Meridian 1 Option 61C CP PII) or 3311 (Meridian 1 Option 81C CP PII).

Patches Utility

The patches utility differentiates between Meridian 1 Option 61C CP PII and Meridian 1 Option 81C CP PII.

Mixed Disk Drive Sizes CP PII

Contents

This section contains information on the following topics:

Overview

This feature provides disk redundancy for Mixed Disk Drive Units (MMDUs) of different sizes on the same switch. This feature configures the MMDUs to be exactly 6GB, thus preserving disk redundancy.

This feature is automatically enabled during sysload (bootup). Manual intervention is not required.

This feature is not applicable for MMDU sizes less than 6GB.

Inventory feature

Since no pack ID is available, there is no data provided to the Inventory Reporting Feature.

Option 61C CPP

The Option 61C CP PII and Option 81C CP P11 systems use the install disk, which is modified to support the Mixed Disk Drive feature.

CPP Health State Monitoring Enhancement

Contents

This section contains information on the following topics:

Feature description

Currently the status of the Embedded Local Area Network (ELAN) port, and the state of the ELAN connections to platforms running Application Module Link (AML) applications, are not considered for the CPP health count. As such, if the ELAN port fails, or the connections to applications such as Call Pilot and Symposium drop, the CPP will not attempt to switch cores.

Health State Monitoring only applies to Meridian 1 systems with Pentium processors (Option 61C CP PII and Option 81C CP PII).

Health State Monitoring is enhanced by incorporating the ELAN port physical layer status and the status of ELAN connections to AML and IP Line

(IPL) applications into the overall system health count. Health count now uses a two-tier approach to determine which core is active.

- The first tier considers the ELAN port as part of the hardware operating system status in addition to existing hardware components in the health count of both cores.
- The second tier considers the ELAN ethernet connections to the applications (AML) health weight as part of the system's operating status, in addition to the existing IPL connectivity health weight.

The new **STAT HEALTH** command in LD 135 displays the contents, status, and values of tier 1 and tier 2 health counts (see Table : "LD 135: Core Common Equipment Diagnostic" on page 246). The health comparison is first done on tier 1. For example, if core 0 has a higher tier 1 health count than core 1, core 0 will be the active CPU regardless of the tier 2 count. If tier 1 health counts are identical in both cores, the tier 2 health count will be used to decide the active core.

Each time the system detects a change in an ELAN connection health, the system sends a message to the other core. This ensures that one core always knows the health of ELAN connections of the other core. Also, when a change in health is detected on either core, the system logs a report.

HEALTH commands

Using the command **STAT HEALTH** in LD 135, an administrator can display tier1 and 2 health counts.

LD 135:
Core Common Equipment Diagnostic (Part 1 of 2)

New Command Syntax	Description
STAT HEALTH	Displays tier 1 and 2 health counts together with the status of the hardware components that do not have a health weight.
STAT HEALTH HW	Displays tier 1 health count together with the status of the hardware components that do not have a health weight.

LD 135:
Core Common Equipment Diagnostic (Part 2 of 2)

New Command Syntax	Description
STAT HEALTH ELAN	Displays tier 2 health count.
STAT HEALTH AML	Displays the health count of the configured ELAN connections to AML applications.
STAT HEALTH IPL	Displays the health count of the IPL connections.
STAT HEALTH HELP	Displays the meaning of the mnemonics used for the hardware components.

The command to display tier 1 health count and status is:

mnemonic <side><slot>[port]: [health][status]

Where:

- mnemonic = hardware component name abbreviation (see Table 31 on page 248.)
- <side> = [0/1] - the side number of the core
- <slot> = [9... 16] - the slot in which the hardware component resides
- <port> = [0/1] - if the component is a port on a card

- <health> = the health weight of the component if InService. If OutOfService, health weight is 0. For the components that do not contribute to health count, this field is omitted.
- <status> = InService/OutOfService. If the component has a health weight and it is InService, this field is omitted.

Table 31:
Hardware components mnemonics

Mnemonic	Meaning
sio8	Serial Input-Output on the CPU card (COM)
sio2	Serial Input-Output on the SUTL card (DONGLE) (see note below)
sutl	System UTiLities card
disp	DISPlay Panel (see note below)
strn	Transition card at the back of SUTL card
xsmp	eXtended System Monitor
ipb	Inter Processor Bus (see note below)
cp	CPu card (see note below)
cmdu	Multimedia Device Unit
eth	ETHernet port on CPU card
cnib	CNI Board
cnip	CNI Port
Note: This item is reportable, but not part of the overall health count.	

The command to display tier 2 health count and status is:

ELAN<n>IP:<ipAddress>Health:<health>

Where:

- <n> = the connection number as configured in Overlay 48 [16...32]

- <ipAddress> = the IP address of the platform that runs the AML application.
- <health> = the health weight of the connection: 2 if the connection PINGs, or 0 if the connection does not PING.

Note 1: The IPL health weight is not fixed and depends on how many IPL cards are configured.

Note 2: For the active side, besides the current health weight of the IPL connections, the command displays the connection history.

Note 3: If the system is in redundant mode, the command shows information for both sides.

Note 4: If the system is in split mode, the information only displays for the local side.

PE/EPE Blocking

Contents

This section contains information on the following topics:

Overview

This feature introduces a blocking facility that disables all cards, loops, and Terminal Numbers (TNs) configured on the PE/EPE shelves. This feature is active immediately after an installation or upgrade.

The feature includes:

- a warning message during installation or upgrade, which the user must acknowledge to complete the process
- a reporting facility in LD 81 to list blocked hardware components
- a post-blocking message to indicate when a user attempts to modify a TN or create a new TN on PE/EPE shelves

Operating parameters

If a TN is in a call, the call is dropped after the terminal is upgraded.

A loop that is disabled before an upgrade remains disabled after the upgrade and cannot be enabled. Meridian Mail TNs configured on this loop cannot be enabled.

This feature does not affect Meridian Mail TNs, DTI loops, or PRI loops configured on PE/EPE shelves. Once the hardware is disabled, no further handling on PE/EPE shelves is possible.

Loop numbers on PE/EPE shelves cannot be reused until the blocks are manually removed.

Even background loop tests and audits cannot enable the disabled units and cards.

The user can **OUT** existing TNs configured on PE/EPE shelves.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

No new software packages are introduced for this feature.

Feature implementation

The system automatically implements this feature during an installation or upgrade to Succession 3.0 Software.

Software install/upgrade

The following warning message displays during Succession 3.0 software installation or upgrade:

```
WARNING:

This S/W release does not support TNs configured on
PE/EPE shelves.

Upgrading to this software release will permanently
disable all TN's configured on PE/EPE and will not
allow new TN's to be configured.

Proceed with the upgrade (Y/N)?
```

If the user enters YES, the upgrade main menu displays, enabling the user to continue the process. If the user enters NO, the upgrade is cancelled and the system is restored to the previous version of the software.

Station administration

The FEAT prompt in LD 81 accepts **PEPE**, which prints all the TNs, loops, and cards configured on PE/EPE shelves. An error message displays when the user attempts to change an existing TN or create a new TN on PE/EPE shelves.

Maintenance

OTM retrieves and displays the status of loops, cards, or units configured on the system. After feature implementation, the loops, cards, or units configured on PE/EPE shelves show a status of **PE/EPE disabled**. The affected components are: network loops, PE shelves, PE cards, and PE units.

An error message displays when the user attempts to change an existing TN or create a new TN on PE/EPE shelves.

Feature operation

There are no specific operating procedures required to use this feature.

Call Center Transfer Connect (UUI)

Contents

This section contains information on the following topics:

Feature description

The Call Center Transfer Connect User-to-User information (UUI) enables the transport of UUI from the AT&T Toll Free Transfer Connect Service over ISDN to the Succession 1000M, Succession 1000, and Meridian 1 PBXs.

Note: UUI and User-to-User Signaling (UUS) are used interchangeably.

Call Center Transfer Connect is an AT&T service, which enables AT&T Toll Free subscribers to transfer or redirect a Calling Party to another location.

Note: This service is described in AT&T TR50075.

The party that receives the incoming call (the Toll Free subscriber) and wants to transfer the call is designated as the Redirecting Party. The party that is the recipient of the transferred call is referred to as the Target Party. In addition to call redirection, the service supports data forwarding from the Redirecting Party to the Target Party. Data Forwarding allows the Redirecting Party to

send data to the Target Party using the Message-Associated User-to-User Information (MA UUI) signaling procedure that is described in AT&T TR41459.

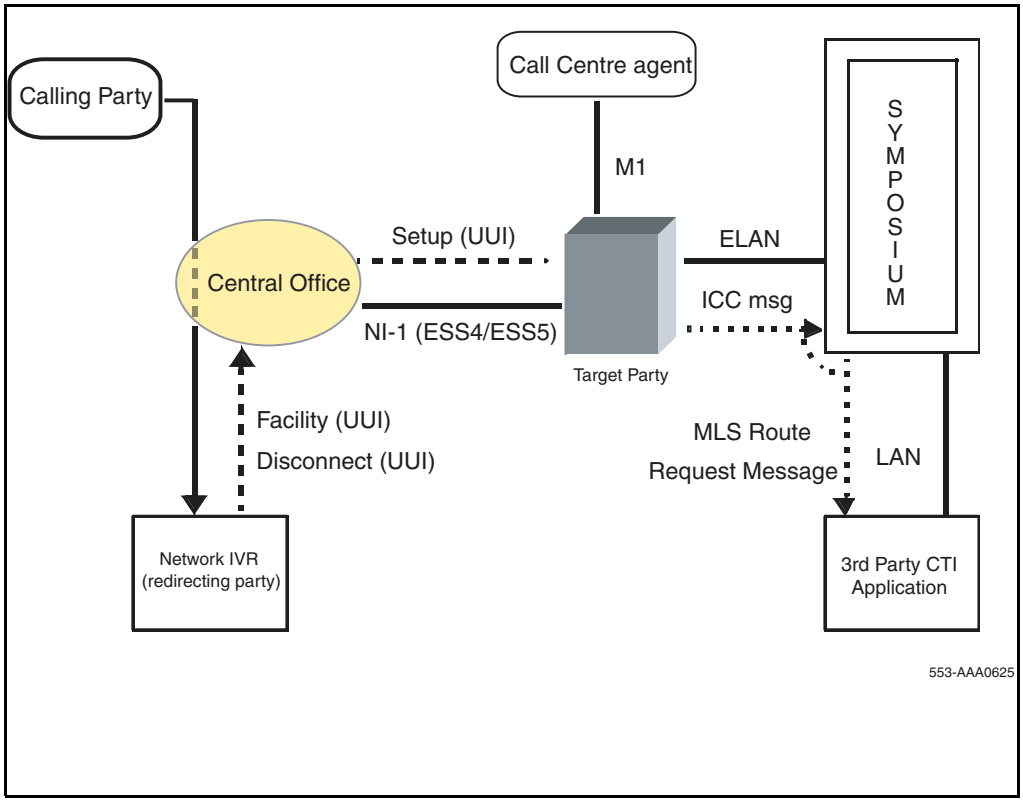
This feature supports the User-to-User Signaling (UUS) information exchange between Succession 1000M, Succession 1000, and Meridian 1 PBXs and an AT&T Electronic Switching System No 4/5 (ESS4/ESS5) over the Primary Rate Interface (PRI) trunks signaling channel.

> ***Note:*** This feature only supports the Target party functionality of the AT&T toll-free Call Center Transfer Connect service feature.

The system transports the UUS information by Ethernet LAN (ELAN) to the Symposium Call Center Server (SCCS).

Figure 51 on page 257 shows the UUI data flow from the Calling Party to the third-party application. In Figure 51, connectivity is shown with bold lines and message flow is shown with dotted lines.

Figure 51
User-to-User data flow from Calling Party to third-party application



The network prompts a user who calls a 1-800 number to enter a credit card number, home phone number, or other essential information. The network then directs the user to a human agent based on the user's profile. The system makes the essential information available to the human agent.

The following is a UUS call scenario:

1 A customer dials a 1-800 number to a network-based Interactive Voice Response (IVR) unit.

2 An IVR collects the necessary information (credit card information, home phone number, and so on) from the user and passes it to the Central Office (CO).

3 The CO inserts the data into the UUI field within the ISDN call SETUP message and passes it on to the target party's PBX.

4 The call, with the associated UUI data, arrives at a system Control Directory Number (CDN).

5 The system extracts the UUI data from the SETUP message and passes it to SCCS over ELAN in the Incoming Call (ICC) message.

6 The SCCS passes the UUI data to the third-party CTI application over MLS.

When User-to-User Information Elements (IEs) are sent over ISDN NI-1 (ESS4 & ESS5) interfaces and received in call establishment messages, they are stored without processing. This information is sent to Symposium through ELAN in an Incoming Call Message (ICC).

The UUS information passes over the ISDN network without modification. The system extracts the UUS information from the ISDN message and sends the UUS information over the ELAN interface to the SCCS. The SCCS passes the UUS information to the third-party Computer Telephony Integration (CTI) application using Meridian Link Service (MLS). A CTI application notifies the agent. For this feature to work, calls from the ISDN network that contain the UUS information must terminate on a Control Directory Number (CDN). This CDN must be acquired by SCCS and have its UUI prompt set to YES in LD 23.

UUI transport over PRI

This feature supports the transport of UUI over ISDN NI-1 (ESS4 & ESS5). This feature only supports Message Associated User-to-User Information (MA UUI).

The Message Associated User-to-User Information (MA UUI) is the information that comes in the following ISDN messages from the MA UUI to the Succession 1000M, Succession 1000, and Meridian 1 PBXs:

- SETUP: UUI comes in the SETUP message in either Codeset 0, or Codeset 7, or both. The length of Codeset 0 or Codeset 7 User-User Information Element cannot exceed 103 octets (100 octets of data).The combined length of Codeset 0 and Codeset 7 User-User Information Element cannot exceed 106 octets (100 octets of data).

- ALERTING: UUI IE comes in the ALERT message in Codeset 0.
- CONNECT: UUI IE comes in the CONNECT message in Codeset 0.
- DISCONNECT: UUI IE comes in the DISCONNECT message in Codeset 0.

UUI transport over ELAN

This feature supports the transport of MA UUI over the ELAN from Succession 1000M, Succession 1000, and Meridian 1 PBXs to Succession Call Center Server only in an ICC message.

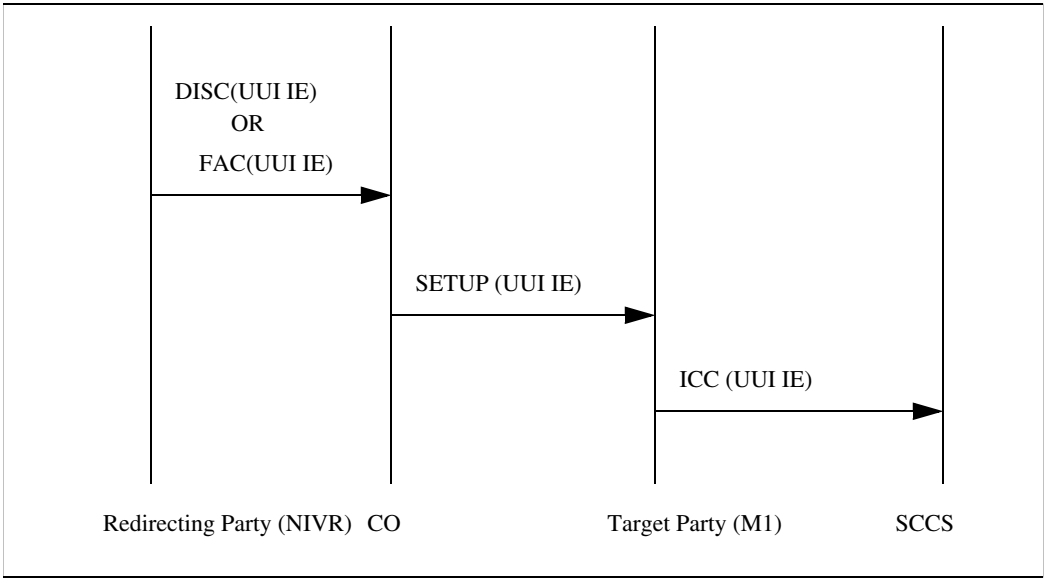
The MA UUI information is not sent in any ELAN message to SCCS during call ALERT, call CONNECT, and call DISCONNECT phases.

A new IE in an ICC message is implemented for UUS data. The ICC message is sent during the SETUP phase on an incoming call to the CDN.

The UUI data is embedded in the F9 IE (UUI IE) in the ICC message. The incoming SETUP message from the CO to the system can contain the UUI data in either Codeset 0 or Codeset 7 or both.

Figure 52 on page 260 shows the message flow for the UUS call scenario.

Figure 52
Message flow for UUS call scenario



New and modified Information Elements

Call Center Transfer Connect introduces a User-to-User Information Element (IE). Table 32 shows the IE format*:*

Table 32
User to User IE Format (CO to the system)

Octet	Field	Bits	Value	Meaning
1	Identifier	1-8	01111110	User-User Information Element
2	Length	1-8	Binary	Length of UUI contents
3	Protocol Discriminator	1-8	Binary	Protocol Disclaimer
4-103	User Data	1-8	Binary	User Data

Protocol Discriminator is not a part of the User data that is sent to Symposium. User data starts with the User-User Application ID as its first octet.

Maintenance and security

This feature supports monitoring of the UUS information in LD 96. Maintenance overlays 96 and 48 allow the craftsperson to monitor (print) the messages on the TTY console. This enables the craftperson to capture the UUI data in both SETUP and ICC messages. The User-to-User information contains sensitive data such as user credit card number and account number. Therefore, the system restricts printing UUI data to the TTY console. The content is replaced by phantom characters (XX) before it is output to TTY console. The UUI IE ID and length are printed. For example: 7E 04 XX XX XX XX.

Operating parameters

Call Center Transfer Connect does not support the following:

- Redirecting Party functionality
- Call Associated Temporary Signaling Connection (CA TSC) and Non-Call Associated Temporary Signaling Connection (NCA TSC)

- Sending of the UUI information to Meridian Link / MAX / CCR
- Presentation of UUI data on telset displays.
- UUI in ISDN Facility message
- Transfer of UUI data to a network Symposium Call Center Server (first node in the Meridian Customer Defined Network cannot be a Symposium Network Call Center node.)

Call Center Transfer Connect supports the following:

- MA-UUI on NI-1 custom AT&T interfaces in the North America and CALA markets.
- Only Target Party functionality of AT&T Transfer Connect service.
- Transfer of UUI data into Symposium Meridian Link Services to enable screen notifications through Nortel Networks, or a 3rd party CTI application.

  Note: This feature is implemented in the Symposium Meridian Link Services only. It is not implemented in Meridian Link 5 C.

Feature interactions

There are no feature interactions with this feature.

Feature packaging

Call Center Transfer Connect (UUI) is package 393. The following packages are also required:

- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package B (ACDB) package 41
- Command Status Link (CSL) package 77
- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146
- Next Generation Connectivity (NGEN) package 324

Feature implementation

Task summary list

The following is a summary of the tasks in this section.

1 LD 17 – Set the RCAP value.

2 LD 23 – Configure a CDN with UUI = YES.

LD 17 – Set the RCAP value.

PROMPT	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device And Number
ADAN		Action Device And Number, where
	NEW aaa x	Add I/O device
	CHG aaa x	Change I/O device
IFC		Interface Type for D-Channel
	ESS4	AT&T ESS#4
	ESS5	AT&T ESS#5
...		
RCAP		Remote capability
	UUI	User-to-User Signaling Supported
	XUUI	User-to-User Signaling Denied

LD 23 – Configure a CDN with UUI = YES. (Part 1 of 2)

PROMPT	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CDN	Control DN

LD 23 – Configure a CDN with UUI = YES. (Part 2 of 2)

CUST	xx	Customer number, as defined in LD 15
CDN	xxxx	Control Directory Number
... ...		
DFDN	xxxx	Default DN (Must be an ACD DN)
... ...		
UUI	(NO)YES	This field is prompted only when the UUI package is enabled.

Feature operation

There are no specific operating procedures required by this feature.

Call Detail Recording Enhancement

Contents

This section contains information on the following topics:

Feature description

Call Detail Recording

Call Detail Recording (CDR) records information about selected calls for accounting purposes. For each call, CDR captures the identity of the calling party, the identity of the called party, and the call time and duration. When the call terminates, the system generates a CDR record. Five recording options are available for each trunk route and can be specified in any combination:

- all outgoing calls
- all outgoing toll calls
- answered outgoing calls

- answered outgoing toll calls
- all incoming calls

For a detailed description of the Call Detail Recording feature, refer to *Call Detail Recording: Description and Formats* (553-3001-350).

Call Detail Recording Enhancement

The CDR Enhancement (CDRX) feature enables customers to bill telephone users for their participation in call segments. Affected calls include outgoing trunk calls transferred one or more times, and CO outgoing calls extended to another party by an attendant. CDR charges users connected to the call who originate and control each transfer. Billing is facilitated through a new CDR "X" record and through enhancements to the "S" (Start) and "E" (End) records.

The CDR Enhancement feature provides the following enhancements:

- Ensures local attendant-originated calls are allocated to the proper chargee.
- Generates CDR "X" records for stand-alone multiple Call Transfers on outgoing non-PPM CO trunks.
- Generates CDR "X" records for network multiple transfers on outgoing PPM and non-PPM CO trunks. Call Detail Recording Enhancement introduces the Billing Line Identification (BLID) CDR field to indicate the remote responsible party for the particular call duration specified in the Call Duration field in cases of network multiple Call Transfers.

Operating parameters

No special hardware is required for CDRX in stand-alone and network non-Periodic Pulse Metering (PPM) CO trunk scenarios. On network PPM trunks, PPM trunk cards are required.

Feature interactions

Conference/No-hold Conference

CDR Enhancement only contains enhancements to Call Transfer records. The following table explains the interaction between Conference/No-hold Conference and the CDR Enhancement.

Table 33
CDR Enhancement – Conference interaction (Part 1 of 2)

Scenario	Description
A calls an outgoing CO trunk and conferences B. ***Note:*** A, B and the CO trunk are on the same node.	An “S” record is generated against A at conference completion time. An “E” record is generated against the party that disconnects last (either A or B).
A calls an outgoing CO trunk; A transfers to B; B conferences C; C conferences D; B disconnects and C disconnects; D transfers to F. ***Note:*** All sets and CO trunks are on the same node.	An “S” record is generated against A at transfer time. An “X” record is generated against B when B completes the conference with C. No record is generated when C conferences D. No record is generated when either B or C disconnect. An “X” record is generated against D when D completes the Call Transfer to F. An “E” record is generated against F when F disconnects. Stand-alone PPM maintains its existing operation.
A calls an outgoing CO trunk; A transfers to B; B conferences C; C conferences D; B disconnects and C disconnects. D transfers to F. ***Note:*** Set A and the CO trunk are in Node 1. Sets B, C, D, and F are in Node 2. Nodes 1 and 2 are connected by an ISDN TIE trunk.	An “S” record is generated against A at transfer time. No record is generated for B’s conference to C or C’s conference D. No record is generated when B disconnects. When C disconnects, an “X” record is generated against B. An “X” is generated against D when D completes the Call Transfer to F. An “E” record is generated against F when F disconnects.

Table 33
CDR Enhancement – Conference interaction (Part 2 of 2)

Scenario	Description
Use the conference key for Call Transfer. A calls outgoing CO, A conferences to B, A disconnects, B conferences C, B disconnects, C conferences D, C disconnects and D transfers to F. ***Note:*** All sets and CO trunk are in the same node.	An "S" record is generated against A at transfer completion time. All the succeeding transfers and conferences do not generate any CDR record. An "E" record is generated when F disconnects.
Use conference key for call transferring. A calls outgoing CO and transfers to B. B conferences C, B disconnects, C conferences D, C disconnects. D transfers to F. ***Note:*** Set A and CO trunks are on node 1. Set B, C, D and F are in node 2. Node 1 and node 2 are connected with an ISDN TIE trunk.	An "S" record is generated against A when the transfer completes. All succeeding transfers and conferences do not generate a CDR record. An "E" record is generated.

Stand-alone PPM Call Transfer

The CDR Enhancement feature ensures that CDR "S", "X", and "E" records do not operate as they do for stand-alone PPM. In an existing stand-alone PPM, an "S" or "X" record is generated when the originating party completes the Call Transfer and the third party answers.

In a non-PPM stand-alone environment, with the CDR enhancement, the "S" and "X" records are generated at transfer completion time. As soon as the originating party completes the Call Transfer, whether the third party answers or not, the CDR "S" or "X" record is printed. A CDR "E" record can be generated against an unanswered DN for its ringing time until the far-end trunk disconnects.

Override

When one station overrides another established station on a CDR trunk call, a Start record is generated for the trunk against the overridden party and a conference is established (however, if there was a previous Start or "X" record, the override generates "X" record). An "E" record is generated against the last party to disconnect, whether they are the overridden or overriding party. However, if the far-end disconnects first while the override is in progress, the "E" record is generated against the conference DN.

Barge-in

When an attendant barges in on a CDR trunk connected to A, a CDR "S" record is generated against A and a conference is established. An "E" record is generated against A when A disconnects. However, if A disconnects before the attendant, an "E" is generated against the attendant when the attendant disconnects to show the barge-in duration and the attendant's duration on the call after A disconnects.

Call Forward

Call Forward All Calls

The following table explains the interaction between Call Forward All Calls and the CDR Enhancement feature.

Table 34
CDR Enhancement – Call Forward All Calls interaction (Part 1 of 2)

Scenario	Description
A calls an outgoing CO trunk, and transfers to B. B call forwards (all calls) to C, and C call forwards (all calls) to D. ***Note:*** All sets and the CO trunk are on the same node.	An "S" record is generated against A when the transfer completes, whether D answers or not. When D disconnects, an "E" record is generated against D.

Table 34
CDR Enhancement – Call Forward All Calls interaction (Part 2 of 2)

Scenario	Description
A calls an outgoing CO trunk, and transfers to B. B call forwards (all calls) to C, and C call forwards (all calls) to D. ***Note:*** A and the CO trunk are on Node 1. B, C, and D are on Node 2. Nodes 1 and 2 are connected by ISDN.	An "S" record is generated against A when the transfer completes, whether D answers or not. When D disconnects, an "E" record is generated against D.
A calls an outgoing CO trunk, and transfers to B. B call forwards (all calls) to C, and C call forwards (all calls) to D. D transfers to E. ***Note:*** A and the trunk are on Node 1. B, C, D, and E are on Node 2. Nodes 1 and 2 are connected by ISDN.	An "S" record is generated against A when the transfer completes, whether or not D answers. When D transfers to E, an "X" record is generated against D. When E disconnects, an "E" record is generated against E.

Call Forward No Answer

Table 35 on page 270 explains the interaction between Call Forward No Answer and the CDR Enhancement.

Table 35
CDR Enhancement – Call Forward No Answer interaction (Part 1 of 2)

Scenario	Description
A calls an outgoing CO trunk, and transfers to B. B call forwards (no answer) to C, and C call forwards (no answer) to D. ***Note:*** All sets and the CO trunk are on the same node.	An "S" record is generated against A when the transfer completes whether D answers or not. When D disconnects, an "E" record is generated against D.

Table 35
CDR Enhancement – Call Forward No Answer interaction (Part 2 of 2)

Scenario	Description
A calls an outgoing CO trunk, and unguarded transfers to B. B call forwards (no answer) to C and C call forwards (no answer) to D. ***Note:*** A and the CO trunk are on Node 1. B, C, and D are on Node 2. Nodes 1 and 2 are connected by ISDN.	An "S" record is generated against A when the transfer completes, whether or not D answers. When D disconnects, an "E" record is generated against B.
A calls an outgoing CO trunk, and unguarded transfers to B. B call forwards (no answer) to C, and C call forwards (no answer) to D. D transfers to E. ***Note:*** A and the CO trunk are on Node 1. B, C, D, and E are on Node 2. Nodes 1 and 2 are connected by ISDN.	An "S" record is generated against A at transfer completion, whether or not D answers. When D transfers to E, an "X" record is generated against B. When E disconnects, an "E" record is generated against E.
A calls an outgoing CO trunk, and guarded transfers to B. B call forwards (no answer) to C, and C call forwards (no answer) to D. D answers and A completes the transfer. D disconnects. ***Note:*** A and the CO trunk are on Node 1. B, C, and D are on Node 2. Nodes 1 and 2 are connected by ISDN.	An "S" record is generated against A when the transfer completes. When D disconnects, an "E" record is generated against D.

Call Forward Busy

See Call Forward All Calls.

Internal Call Detail Recording (ICDR)

CDR Enhancement generates a CDR "X" record when the Call Transfer completes if an outgoing CO trunk participates in the call. There are no changes to the ICDR feature. The two features are independent.

Call Waiting

In a Call Transfer on busy station A with Call Waiting Allowed, a CDR "S" or CDR "X" record is generated when the transferring station disconnects. An "E" record is generated when either A or the far-end/trunk disconnects. The CDR record includes the wait time.

Initialize

If the system initializes, CDR information is lost.

Attendant Recall

Table 36 explains the interaction between Attendant Recall and the CDR Enhancement feature.

Table 36
CDR Enhancement – Attendant Recall interactions (Part 1 of 2)

Scenario	Description
The attendant calls an outgoing CO trunk, and extends the call to A. A presses the Attendant Recall (ARC) key to recall the attendant and a three-party conference is established ***Note:*** The trunk is not a CDRX trunk.	An "S" record is generated against the attendant when the attendant presses the Release key. An "E" record is generated at the end of the call against the party that disconnects last. Stand-alone PPM maintains existing operation.
The attendant makes an outgoing CO call, and extends the call to A. A presses the Attendant Recall (ARC) key to recall the attendant and a three-party conference is established. ***Note:*** The trunk is a CDRX trunk.	An "S" record is generated against the attendant when the attendant presses the Release key. An "X" record is generated against A when the attendant presses the LOOP key to respond to the call. If A disconnects first, then the attendant releases, and an "E" record is generated against the attendant. If the attendant releases first, an "X" record is generated against the attendant. An "E" record is generated against A when A disconnects.

Table 36
CDR Enhancement – Attendant Recall interactions (Part 2 of 2)

Scenario	Description
The attendant makes an outgoing CO call, and extends the call to A. A presses the Attendant Recall (ARC) key twice to recall the attendant, which is also treated as a transfer complete. ***Note:*** The CO trunk is a CDRX trunk.	An “S” record is generated against the attendant when the attendant presses the Release key. An “X” record is generated against A when A presses the ARC key twice to complete the transfer. An “E” record is generated against the attendant when the attendant releases.

Meridian Mail

Stand-alone Non-PPM

During Call Transfer, if the outgoing CDRX trunk terminates at Meridian Mail due to call redirection, the CDR “E” record is generated against the Meridian Mail virtual agent DN when the far-end disconnects.

If an outgoing CDRX trunk transfers to Meridian Mail, and the far-end caller uses “through dial” to call the attendant, an “X” record is generated against the Meridian Mail virtual agent DN. If the attendant extends the call to A, an “X” record is generated against the attendant. When A disconnects, an “E” record is generated against A.

Network PPM and Non-PPM

During network Call Transfer, if the outgoing CDRX trunk is transferred through ISDN directly to Meridian Mail, the CDR record is generated against the Meridian Mail virtual agent DN.

During network Call Transfer, if the outgoing CDRX trunk is transferred though ISDN to a remote DN that is Call Forwarded (All Calls) to Meridian Mail, the CDR record is generated against the Meridian Mail virtual agent DN.

During network Call Transfer, if the outgoing CDRX trunk is unguarded transferred through ISDN to a remote DN that is Call Forward (No Answer) to Meridian Mail, the CDR record is generated against the remote DN instead of the Meridian Mail virtual agent DN.

During network Call Transfer, if the outgoing CDRX trunk is guarded transferred through ISDN to a remote DN which is Call Forwarded (No Answer) to Meridian Mail, the CDR record is generated against the Meridian Mail virtual agent DN.

Hunting

See Call Forward All Calls.

Call Park

Table 37 explains the interaction between Call Park and the CDR Enhancement feature.

Table 37
CDR Enhancement – Call Park interaction

Scenario	Description
A calls an outgoing CO trunk, and presses the Call Park key twice. Later, the CO recalls A. A disconnects.	An “S” record is generated against A when A presses the call park key twice. An “E” record is generated against A when either A or trunk disconnects.
A calls an outgoing CO, and transfers to B. B presses the Call Park key twice. The CO recalls B. B disconnects.	An “S” record is generated against A when the transfer completes. When B presses the Call Park key twice, an “X” record is generated against B. The CO later recalls B. An “E” record is generated against B when either B or the trunk disconnects.
A calls an outgoing CO trunk, and presses the Call Park key twice. B dials Special Service Prefix (SPRE) + Parked Call Access code (72) + the identification number assigned to the parked call to access the parked call later. B transfers to C. C disconnects.	An “S” record is generated against A when A presses the Call Park key twice. An “X” record is generated against B when the transfer completes, whether or not C answers. An “E” record is generated against C when either C or the CO trunk disconnects.

Call Pickup

The following table explains the interaction between Call Pickup and the CDR Enhancement feature.

Table 38
CDR Enhancement – Call Pickup interaction

Scenario	Description
A makes an outgoing CO call, and transfers to B. B unguarded transfers to C and C does not answer. D picks up the call by pressing the DN key and the RNP key. ***Note:*** All sets are on the same node.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the transfer completes. An “E” record is generated against C when D picks up the call. An “N” record is generated against D when either D or the far-end disconnects. If D does not disconnect, and instead transfers to E, an “S” record is generated against D when the transfer completes. An “E” record is generated against E when E or the far end disconnects.
A makes an outgoing CO call, and transfers to B. B transfers to C and C does not answer. D picks up the call by pressing the DN key and the RNP key. ***Note:*** A and the CO are on Node 1. B, C, and D are on Node 2. Nodes 1 and 2 are connected by ISDN.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the transfer completes. An “E” record is generated against C when D disconnects.
A makes an outgoing CO call, and transfers to B. B guarded transfers to C and C does not answer. D picks up the call by pressing the DN key and the RNP key. ***Note:*** All sets are on the same node.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the transfer completes and D picks up the call. An “E” record is generated against D when D or the far end disconnects. If D does not disconnect, and instead transfers to E, an “X” record is generated against D when the transfer completes. An “E” record is generated against E when E or the far end disconnects.

Automatic Call Distribution

For ACD Call Transfer, ACD Conference, and Network ACD, CDR records are generated as if these features are functioning in a non-ACD environment. For the Agent Observe subfeature, CDR records are generated as they do in a non-ACD conference call.

Disconnect Supervision

The Central Office can notify the system trunk card that the office has released when the trunk has disconnect supervision. The far end or near end can control trunk disconnect. The CDR records are generated when the trunk disconnects.

Network Attendant Service

When a remote attendant at Node 1 is involved in an outgoing CDRX trunk at Node 2 through the ISDN network, the CDR at Node 2 treats it as if it were a Call Transfer.

Table 39
CDR Enhancement – Network Attendant Service

Scenario	Description
The set calls the attendant and the attendant extends out.	An “S” record is generated against the remote attendant DN (for example: 0000 or 0) and an “E” record is generated against the set when the set disconnects.
The attendant calls out and extends to a local set.	An “S” record is generated against the remote attendant DN and another “E” record is generated against the set when the set disconnects.
The attendant calls the set first, then extends out.	An “S record is generated against the remote attendant DN and another “E” record is generated against the set when the set disconnects.

Break-in

The following table explains the interaction between Break-in and the CDR Enhancement feature.

Table 40
CDR Enhancement – Break-in Interaction

Scenario	Description
A makes an outgoing CO call and then transfers to B. B is talking to the outgoing CO. C calls the attendant and the attendant Breaks-in to B. B disconnects.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the attendant Breaks-in. An “E” record is generated against the conference DN when B disconnects.

Break-in to Enquiry Calls

The following table explains the interaction between Break-in to Enquiry Calls and the CDR Enhancement feature.

Table 41
CDR Enhancement – Break-in to Enquiry Calls Interaction

Scenario	Description
A makes an outgoing CO call, and transfers to B. B transfers to C, and is talking to C without completing the transfer. D calls the attendant, and the attendant Breaks-in to B. B disconnects. C is connected to the outgoing CO.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when B disconnects. An “E” record is generated against C when C disconnects.

Attendant Metering Recall

This feature does not support Attendant Metering Recall.

Virtual Network Service

If “Trunk on Hold for Reuse” is not configured, the COT trunk is released when the VNS call is released. If the COT trunk is a PPM trunk, the different sets involved in the call will be charged as for a regular non-VNS call. CDR “N”, “S”, “X”, and “E” records will generate according to the call modifications. CDRX/PPM operation should be transparent to the VNS feature.

If “Trunk on Hold for Reuse” is configured, the COT trunk remains established after the VNS call is released and a CDR “S” record is produced with no charge information. If a new VNS call uses the same trunk, a CDR “X” record is printed, once again containing no charge information.

Multi-party Operations

“Recovery of Misoperation on Call Transfer” interacts with the CDR Enhancement feature as follows.

Table 42
CDR Enhancement – Multi-party Operations Interaction

Scenario	Description
A calls outgoing CO and transfers to B. B transfers to C and C does not answer. After a pre-defined number of rings, the call is recalled to B. If B does not answer after a predefined number of rings the call is dropped.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the transfer completes. An “E” record is generated against C when C does not answer after a pre-defined number of rings and the call is recalled to B. An “N” record is generated against B when the call is dropped.

Busy Verification

The following table explains the interaction between Busy Verification and the CDR Enhancement feature.

Table 43
CDR Enhancement – Busy Verification Interaction

Scenario	Description
A calls an outgoing CO trunk and transfers to B. B is talking to the outgoing CO. The attendant performs a Busy Verification on B.	An “S” record is generated against A when the transfer completes. An “X” record is generated against B when the attendant presses the Busy Verify key and dials B’s DN. An “E” record is generated against B if the attendant disconnects before B. An “E” record is generated against the conference DN if B disconnects before the attendant. An “E” record is generated against the conference DN if the far-end trunk disconnects first.

Feature packaging

For stand-alone and network non-PPM environments, the following software package is required:

- Call Detail Recording Enhancement (CDRX) package 259, which requires the following packages:
  - — Call Detail Recording (CDR) package 4
  - — Call Detail Recording Teletype Terminal (CTY) package 5
  - — New Format Call Detail Recording (FCDR) package 234

CDR for the attendant is included as part of Call Detail Recording (CDR) package 4 and is applicable to outgoing trunks.

Network PPM CDRX is included as part of Periodic Pulse Metering/Message Registration (MR) package 101.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. LD 17 – Change the Configuration Record for CDR Enhancement.
2. LD 16 – Configure the Route Data Block to print CDR "X" records.
3. LD 15 – Configure the Customer Data Block for CDR Enhancement.

LD 17 – Change the Configuration Record for CDR Enhancement.

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	PARM	Change system parameters
...		
- FCDR	NEW	Format for Call Detail Recording
- MTRO	PPM	Periodic Pulse Metering

LD 16 – Configure the Route Data Block to print CDR "X" records. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	RDB	Route data block
CUST	xx	Customer number, as defined in LD 15.
ROUT	 0-511 0-127	Route number For Large Systems For Small Systems and Succession 1000 systems
...		

LD 16 – Configure the Route Data Block to print CDR "X" records. (Part 2 of 2)

Prompt	Response	Description
TKTP	COT DID WAT FEX	Central Office Trunk data block Direct Inward Dialing trunk data block Wide Area Telephone Service trunk data block Foreign Exchange trunk data block
...	...	
CDR	YES	CDR provided
- INC	(NO) YES	CDR records generated for incoming calls
- OAL	YES	CDR records generated for outgoing calls
- - OTL	(NO) YES	CDR on Outgoing Toll calls
- - OPD	(NO) YES	Outpulsed digits recorded in CDR
- CDRX	(NO) YES	Print CDRX records on multiple Call Transfer for non-PPM (Digital Trunk) outgoing calls. This prompt appears if CDRX package 259 is equipped, and "MR" is not "PPM", "XLD" "ENDC", "DURC", or "IFC" is not equal to 1TR6. NI2 does not support Advice of Charge (AOC) so MR is not prompted.

LD 15 – Configure the Customer Data Block for CDR Enhancement.

Prompt	Response	Description
REQ:	CHG	Change existing data
TYPE:	CDR	CDR and Charge Account options
CUST	 0-99 0-31	Customer number For Large Systems For Small Systems and Succession 1000 systems

LD 15 – Configure the Customer Data Block for CDR Enhancement.

...		
CDR	YES	Call Detail Recording

Feature operation

No specific operating procedures are required to use this feature.

CTI Enhancements - DTMF Tone Generation

Contents

This section contains information on the following topics:

Feature description

Currently, Computer Telephony Interface (CTI) applications, such as network routing applications and Symposium agent, must connect directly to individual telephones to control the generation of dual-tone multiple frequency (DTMF) digits. These connections enable the installation of Meridian Communication Adaptors (MCA) at each telephone.

The CTI Enhancements - DTMF Tone Generation feature enables host-based applications (such as Windows TAPI applications) to invoke DTMF tones on behalf of any acquired telephone, as if a user pressed digits on the telephone dialpad during an active call. This DTMF tone invocation is accomplished by sending a new Set Feature Invocation (SFI) message from the application.

The SFI message is sent on behalf of the acquired telephone. The message includes DTMF digits and optional fields such as inter-digit delay, tone duration, and pause duration. An SFI response message is sent back to the application to acknowledge receipt of an incoming SFI message (DTMF generation request). A Set Feature Notification (SFN) message is sent from the system to the application only after successfully generating DTMF tones that correspond to digits sent in the SFI message. To support this feature, the acquired telephone must be established on a call.

The application sends a Set Feature Invocation (SFI) DTMF message on behalf of an acquired telephone to the system that contains the digits and the duration (that is, the length of the DTMF tone). On receipt of this message, the system validates the message and the call state of the telephone that requests tone generation. An SFI response message returns indicating whether the request has been accepted or rejected.

Tone duration is constant for all digits in each SFI message. Actual duration depends on the value of the duration IE tag in the SFI DTMF message. The duration value is set in multiples of 56 ms. Therefore, if the value is 10, the duration is 560 ms. The value of the duration IE tag can range from 1 to 100, resulting in a maximum tone duration of 5.6 seconds.

The inter-digit timer is constant for all digits in the SFI message. The inter-digit timer depends on the value set in the inter-digit duration IE tag of the SFI message. The duration value is set in multiples of 56 ms. Therefore, if the value is 10, the duration is 560 ms. The value of the inter-digit duration IE tag can range from 1 to 100, resulting in a maximum timer value of 5.6 seconds.

When the system receives a message to generate DTMF tones, it checks for an established connection and then generates tones for DTMF digits. The DTMF tones are sent only if there is an End-to-End Signaling (EES) connection (established speechpath) between the two parties. The application can send multiple SFI DTMF messages for the same call. However, a subsequent SFI DTMF message can be sent only after the previous SFI DTMF message has been received and acknowledged.

After successful generation of all DTMF tones corresponding to the digits sent in the SFI message, an SFN message is sent to the requesting application. The requesting application awaits this message for a time period based on the number of digits that were sent and for which the system generated tones, multiplied by the tone generation time, plus the inter-digit delay. If a pause generation has also been requested, it is factored into the wait time.

The acquired telephone receives feedback tone when the system generates the DTMF tones requested by the application. Administrators can configure the feedback tones in LD 15.

The system does not process a new SFI DTMF message while it generates DTMF tones for the same telephone. If such a request is made, an SFI DTMF response message is issued, which indicates and explains the request failure.

Operating parameters

This feature applies to the following systems:

- Succession 1000M Cabinet
- Succession 1000M Chassis
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81C CP PII
- Meridian 1 Option 11C Cabinet
- Meridian 1 Option 11C Chassis

Only acquired telephones support this feature. Phantom PBX telephones and attendant consoles do not support this feature. The DTMF tones are not generated if the telephone is undergoing treatment (for example, if the telephone is receiving Music or a Recorded Announcement (RAN). The application can send up to 31 digits to the telephone. DTMF digits appear in CDR reports only if the DTMF-generating telephone is the originating telephone.

This feature supports:

- ten digits: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0
- two characters: # and *
- a maximum of 31 digits (sent from the application)
- pause capabilities sent from the application

Pause is implemented by sending the character ",". Pause duration depends on the value specified in the pause duration IE tag of the SFI DTMF message from the application.

This feature functions differently when the acquired telephone is digital than when it is analog (500/2500-type). For a digital telephone, the End-to-End Signaling (EES) feature generates the DTMF tones by conferencing a TDS with the connected parties. Pause is implemented by sending the character ",". Pause duration depends on the value specified in the pause duration IE tag of the SFI DTMF message from the application.

The TDS generates DTMF tones for the terminating device while the originator of the EES receives feedback tone. Since analog (500/2500-type) telephones have the native capability to generate DTMF tones, analog (500/2500-type) telephones do not use the EES feature to generate tones.

This feature depends on End-to-End Signaling (EES). Therefore, it supports only EES-compatible trunk types, such as CO, FEX, WATS, TIE, CCSA, DID, and CAMA trunks.

Feature interactions

Call Detail Recording

The DTMF digits are printed in the Call Detail Recording (CDR) record if the telephone is the originating party and if the ECDR prompt in LD 15 is set to YES. DTMF digits print in the CDR record even if tone generation has not completed due to abnormal operation.

Call Modifications

All call modifications are blocked if DTMF tone generation is in progress. The telephone that generates DTMF tones cannot initiate call modifications such as transfer and conference.

Conference

All parties in an established conference hear DTMF tones generated for the acquired telephone. The acquired telephone hears single feedback tones or no tone at all, depending on the EEST setting in LD 15.

Display

Digits received in the SFI DTMF message display on the telephone even if tone generation cannot complete due to abnormal operation. Digits display on the telephone only if the EESD prompt in LD 15 is set to YES.

Multiple Appearance Directory Number

Only one telephone can be associated with a Multiple Appearance Directory Number (MADN). DTMF tones are generated only for the acquired telephone if it is active on the speechpath. Other telephones receive neither the DTMF tones nor the feedback tones. The display of other telephones is not affected.

No Hold Conference

When a call is placed on No Hold Conference (NHC), DTMF tones cannot be generated. Tones generate after the NHC concludes.

Observe

If the OBTN option is set to NO and tones generate on behalf of (a) the agent under silent observe or (b) the connected telephone, the supervisor does not hear DTMF tones between the agent and the customer. The supervisor does hear a click as tones are generated. This click is caused by idling of the path between the agent and the far end.

If the OBTN option is set to AGT or ALL, the supervisor is in a conference loop with the agent and the customer, and thus hear DTMF tones as the agent and the caller hear them. Tones are provided for conferenced parties by attaching a TDS to the existing conference loop.

Phantom telephones

DTMF tones can be generated on behalf of the phantom telephone from the application if the telephone is active on a call and is associated (AST). Since phantom telephones do not have a physical appearance, display and feedback tones do not apply.

Since a PBX phantom telephone cannot be associated (AST), tones cannot be generated on behalf of the PBX phantom telephone from the application.

Recorded Announcement and Music

If the acquired telephone is listening to a Recorded Announcement (RAN) or Music, the application cannot generate DTMF tones on behalf of the telephone. An SFI DTMF response message is sent to indicate that the failure resulted from RAN or Music.

Feature packaging

This feature requires the following packages:

- End-to-End Signaling (EES) package 10
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package B (ACDB) package 41
- Command Status Link (CSL) package 77
- Meridian Link Module Server (MLM) package 209

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1 LD 17 - Configure ELAN and define associated VAS ID.

2 LD 48 - Enable ELAN messages.

3 LD 10 - Configure analog (500/2500-type) telephones.

4 LD 11 - Configure digital telephones.

5 LD 15 - Configure End-to-End Signaling.

LD 17 - Configure ELAN and define associated VAS ID.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration Record
ADAN	NEW ELAN xx	Add I/O device type ELAN, where xx = 16 to 31.
CTYP	ELAN	Enable the AML messages in LD 48; card type = ELAN.
LCTL	(NO) YES	Modify link control system parameters.
-N1	128 (512)	Maximum octets per one frame (128 or 512 is recommended for ELAN).
...	....	...
VAS	NEW	New Value Added Server
	CHG	Change Value Added Server
VSID	xx	Associate link and VASID so messages can be sent.
ELAN	xx	Associate VASID xx with ELAN xx.
SECU	(NO) YES	YES if Meridian link is connected to ICCM, otherwise NO.
INTL	1 to 12	Time interval for checking Meridian Link for overload for five second increments.
MCNT	5 to 100 000	Message count threshold for number of Meridian Link messages per time interval.

LD 48 - Enable ELAN messages.

Command	Description
ENL MSGI xx	Enable incoming messages on ELAN xx.
ENL MSGO xx	Enable outgoing messages on ELAN xx.
ENXP MSGI xx 1	Disable all incoming polling messages on ELAN xx.
ENXP MSGO xx 1	Disable all outgoing polling messages on ELAN xx.

LD 10 - Configure analog (500/2500-type) telephones.

Prompt	Response	Description
REQ:	CHG NEW	Change or Add
TYPE:	500	Telephone type
TN		Terminal number
	l s c u c u	For Large Systems For Small Systems and Succession 1000 systems
CUST	xx	Customer number, as defined in LD 15
DN	2022	Directory Number
AST	YES	Associate set assignment
IAPG	(0)-15	Status Change Group, where: 0 = No Status Change Message 1 = All Status Change Message 2-15 must be defined in LD 15

LD 11 - Configure digital telephones.

Prompt	Response	Description
REQ:	CHG NEW	Create new data or change existing data.
TYPE:	aaaa	Telephone types, where aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 3000, 390x
TN		Terminal Number
	l s c u c u	For Large Systems For Small Systems and Succession 1000 systems
AST	xx yy	Associate set assignment, where xx, yy = DN key numbers, Incalls key.
IAPG	(0)-15	Status Change Group, where: 0 = No Status Change Message 1 = All Status Change Message 2 - 15 must be defined in LD 15
KEY	xx SCR yy	Single Call Ringing DN key, where yyyy = DN

LD 15 - Configure End-to-End Signaling. (Part 1 of 2)

Prompt	Response	Description
REQ:	CHG	Change existing data.
TYPE:	FTR	Features and options
CUST	 0-99 0-31	Customer number For Large Systems For Small Systems and Succession 1000 systems
EEST	(NO) YES	End-to-End Signaling, where: NO = Disabled (Do not send feedback tone to the originator) YES = Enabled (Send single feedback tone to the originator)

LD 15 - Configure End-to-End Signaling. (Part 2 of 2)

Prompt	Response	Description
EESD	(NO) YES	End-to-End Signaling display, where: NO = Disabled (DTMF digits do not display) YES = Enabled (DTMF digits display) For YES and NO, Application Request DTMF generation for PBX does not apply.
ECDR	YES	Print End-to-End Signaling digits in CDR record.

Feature operation

No specific operating procedures are required for this feature.

Emergency Services for Virtual Office

Contents

This section contains information on the following topics:

Feature description

The Emergency Services for Virtual Office feature allows Virtual Office users to place an emergency (E911) call to the correct Public Safety Answering Point (PSAP) for their geographical location. It recognizes when a user dials an Emergency Services Directory Number (ESDN) and forces the Virtual Office Internet Telephone to log out of the Remote Succession Call Server and redirect to the Home Succession Call Server. Although this adds a small delay to call processing, the delay is almost imperceptible to the user.

No overlay changes are required since there are no configuration options.

> ***Note:*** Unless stated otherwise, all ESA functions (for example OSN, non-DID mapping to DID, and internetworking with partner solutions) continue to operate as previously described.

Virtual Office operation with feature not enabled

Upon Virtual Office login, without the Emergency Services for Virtual Office feature enabled, the Internet Telephone de-registers with the Home Succession Call Server and registers with the Succession Call Server associated with the given User ID. This can be the same Succession Call Server or another Succession Call Server within the network. If it is another Succession Call Server, then it might be in a different geographic area and use a different PSAP to handle emergency calls. Therefore, if a user places an emergency call using an Internet Telephone that is geographically distant from its registered Succession Call Server, the emergency call is sent to the wrong PSAP and help might be delayed, go to the wrong location, or not arrive at all.

> ***Note:*** The basic ESA feature uses the premise that all the telephones connected to the Succession Call Server are served by the same PSTN and the same PSAP. This assumption is acceptable for TDM telephones where the maximum length of the cable from the Succession Call Server to the telephone is restricted to approximately 1000 feet. With Internet Telephones, it is possible for a telephone to be at a great distance from the Succession Call Server.

Without the Emergency Services for Virtual Office feature configured, ESA operates the same on a Virtual Office Internet Telephone as it operates on any other Succession Call Server telephone, and the wrong PSAP may be used. This is considered fall back mode, which is compatible with older versions of the software or firmware.

Virtual Office operation with feature enabled

Upon Virtual Office login on a Remote Succession Call Server with the Emergency Services for Virtual Office feature enabled, the Home TPS stores the ESA configuration in the DRAM of the Internet Telephone before redirecting it to the Remote Succession Call Server. This information tells the Remote Succession Call Server that the Home Succession Call Server is enabled and configured for ESA. The Remote Succession Call Server uses this information to redirect the Internet Telephone to the Home Succession Call Server to handle ESA calls.

> ***Note:*** The ESA configuration stored in the DRAM includes the Emergency Services DN (ESDN). This is implemented for future use, when the ESDN could differ on Succession Call Servers.

When the redirected Internet Telephone starts the registration and Virtual Office login procedure at the Remote Succession Call Server, the Remote TPS reads its DRAM and passes the ESA configuration to the Succession Call Server. This lets the Succession Call Server know that if the Internet Telephone user makes an ESA call, it must use the Emergency Services for Virtual Office feature.

When the Virtual Office user dials the ESDN, then the Emergency Services for Virtual Office feature is invoked on the Remote Succession Call Server. The feature checks for a flag that indicates that the originating Internet Telephone can be redirected to the Home Succession Call Server to process the ESA call. If this is the case, then the Remote Succession Call Server sends a message to the Remote TPS to write the request into the DRAM of the Internet Telephone and redirect it to the Home TPS.

> ***Note:*** The request to redirect the set to the Home TPS for the ESA call includes the dialed ESDN. This is implemented for future use, when the ESDN could differ on Succession Call Servers.

A message is sent to the Internet Telephone's display alerting the user that the emergency call is in progress. Then, another message is sent to the Internet Telephone's display indicating an emergency call is in progress. A final message causes the Internet Telephone to return to its Home TPS without the visible flashing of the light or clearing of the display.

When the Internet Telephone re-registers with the Home TPS, the Home TPS retrieves the DRAM and acts on the request for an ESA call. The Home TPS simultaneously refreshes the Internet Telephone's display with the correct keymap and sends a message to the Succession Call Server indicating that an emergency call must be originated on the Internet Telephone's TN.

After the emergency call ends, the Internet Telephone remains registered to the Home TPS as a normal telephone, in case the PSAP makes a call back to the originator of the emergency call.

To prevent interworking problems with external On Site Notification (OSN) data processing devices, OSN is not changed on the Home Succession Call Server. If OSN is changed on the Remote Succession Call Server, then care must be taken to not confuse external OSN data processing devices.

After the Internet Telephone is redirected to its Home Site, it is not allowed to initiate a new operation for five minutes. This prevents the user from accidentally dialing the emergency DN and hanging up. In this case, the emergency response personnel might call back to confirm the accidental call (and thus confirm that there is no emergency). If the phone is allowed to immediately resume a Virtual Office login to another site, it cannot receive the call back.

Operating parameters

The following are the minimum software and firmware requirements for the Emergency Services for Virtual Office feature:

- Internet Telephone firmware 1.5x
- Succession 3.0 software

The ESA package must be enabled on the Home and Remote Succession Call Servers. If either site does not have ESA enabled, the E911 feature operates the same with or without the feature enabled, and calls are placed to the PSAP of the user's home location.

The resources required to originate an emergency call should be blocked from use by normal call processing, and reserved for emergency calls. Since the Emergency Services for Virtual Office feature overrides access restrictions, it is possible to have resources that cannot be normally accessed, but can be accessed for an emergency call. In particular, the outbound trunks and DSP resources should be reserved in this manner.

The Internet Telephone may have a "red sticker" indicating the number to dial for emergency calls. This is only applicable when connected to the Local Succession Call Server. A Virtual Office user, connected to a Remote Succession Call Server, must dial the ESDN associated with the Remote Succession Call Server (not necessarily the number indicated on the "red sticker"). It is up to the site to come up with a policy for this situation.

If the Internet Telephone does not have the correct firmware, the Emergency Services for Virtual Office feature still redirects the Internet Telephone to the Home Site. However, the Internet Telephone appears to visually reset, which may cause the user to panic.

If the Home Succession Call Server does not have ESA configured, ESA is not configured correctly, or the TPS does not have the correct software, then the feature operates in fallback mode.

If network problems prevent a redirected Internet Telephone from registering with the Home TPS (the Home TPS or Home Succession Call Server might be out-of-service), the Internet Telephone goes into a server unreachable mode and resets. The Internet Telephone is out-of-service until it can connect to the Home TPS, and the data in the DRAM is lost and no emergency call originates.

If the maximum number of Internet Telephones is registered with the Home TPS, then no new telephones can register. Therefore, the Virtual Office Internet Telephone returning to the Home TPS cannot initiate an emergency call. The system should be engineered such that there are enough resources for additional Internet Telephones to register.

If the TN of the redirected Internet Telephone is used by another Virtual Office session, the Internet Telephone occupying the TN is preempted so the redirected Internet Telephone can access the TN to make an emergency call.

The IP network cannot be used to directly reach the PSAP, so the Succession Call Server must have a TDM trunk to the PSTN for each PSAP. ESA does not support more than one PSAP for a given Succession Call Server. The solution is to have a Succession Call Server in each PSAP jurisdiction and to route the call to the appropriate Succession Call Server based on the location of the originator of the emergency call.

If a user dials the ESDN on an Internet Telephone while logged onto a Remote Succession Call Server using Virtual Office, it is not appropriate to have the Remote Succession Call Server connect the call to its PSAP. It is better for the Remote Succession Call Server to send the Internet Telephone to its Home Succession Call Server (simulating a Virtual Office log out) along with a flag to let the Home Succession Call Server know the reason the phone came home is to place an ESA call.

If the user changes between headset, handset, or handsfree operation between the time the final digit for the ESDN is pressed and the call is connected to the PSAP, that change will not be recognized by the Succession Call Server. The call will be completed in all cases, but the user might not hear the PSAP if they expected the change to take effect and listened to the wrong device.

The Emergency Services for Virtual Office feature introduces error messages for the following situations:

- A remote Internet Telephone, that does not function with the feature, connects to the Succession Call Server.
- A remote Internet Telephone, after generating the previous message, dials the emergency DN and is routed to the wrong PSAP.
- A TN without an active call is preempted due to an emergency call by a remote Internet Telephone.
- A TN with an active call is preempted due to an emergency call by a remote Internet Telephone.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The Emergency Services for Virtual Office feature requires the following packages:

- Emergency Services Access (ESA) package 329
- Virtual Office (VO) package 382
- Virtual Office Enhancement (VOE) package 387

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

Group Hunt

Contents

This section contains information on the following topics:

Feature description

Group Hunting is similar to the Hunting feature. If a call encounters a busy DN and a Group Hunting Pilot DN is specified, the call is routed to the next idle DN in a prearranged group. Unlike the existing Hunting feature, Group Hunting allows a customer to:

- Configure all members of a hunt group in one block instead of many different station data blocks.
- Prevent Group Hunt termination on any idle member through a Group Hunt Deactivate Flexible Feature Code (FFC) or through a GHD (Group Hunt Deactivate) key.
- Limit the hunting steps to the total number of DNs in the list.
- Initiate hunting by dialing or accessing a Group Hunt Pilot DN directly.
- Configure a DN to be a member of more than one hunt group.

Pilot DN

Pilot DNs are defined as PLDN Flexible Feature Codes (FFC) in LD 57. Pilot DNs are used in two ways:

1 If the USE prompt is set to GPHT, then the Pilot DN is defined to activate Group Hunting.

2 If the USE prompt is set to Speed Call List Controller (SCLC) or Speed Call List User (SCLU), then the Pilot DN is defined to access the Speed Call or System Speed Call lists that are associated with the Pilot DN.

Termination conditions

When a Group Hunt Pilot DN is dialed, Group Hunting searches the list associated with the Pilot DN, according to the hunt type specified, until one of the following conditions is met:

1 idle DN is encountered

2 Automatic Call Distribution (ACD) DN,
Integrated Voice Messaging Service (VMS) DN,
Message Center (MC) DN,
Listed Directory Number (LDN),
or attendant DN is encountered

3 route access code is encountered

4 ESN access code is encountered

5 Group Hunt Pilot DN is encountered

6 all DNs in the group are hunted to, or
the maximum number of hunting groups is reached

If condition 1 or 2 is met, then incoming calls are completed to that DN. All DNs listed in condition 2 are associated with a queue. Remember the following when configuring these Group Hunt lists:

- These DNs always appear idle to a hunt cycle, regardless of their actual status. The hunt always redirects to the indicated destination, and never comes back into the Group Hunt list, therefore these calls are never queued against the Pilot DN.

- It is recommended that if these DNs must be used in a Group Hunt list, only one such DN be used. This DN must always be the last entry in the list.
- Also, linear hunting must be used. In this configuration, any redirected call is subject to the call processing treatment of the destination.
- Listed DNs can be configured as a last entry in a hunt group list, if linear hunting is used. The redirected call is presented to the associated LDN Incoming Call Indicator (ICI) key on the Attendant Console. The call can be transferred back to the Hunt Group Pilot DN; once transferred, it cannot be recalled to the attendant.
- Attendant DNs can be configured as a last entry in a hunt group list, if linear hunting is used. The call can be transferred back to the Hunt Group Pilot DN; once transferred, it cannot be recalled to the attendant.
- Automatic Call Distribution (ACD) DNs can be configured as a last entry in a hunt group list, if linear hunting is used. The call can be transferred back to the Hunt Group Pilot DN. If the ACD queue has the Hunt Group Pilot DN defined as the night DN, the call is transferred back into the hunt group list.

If termination condition 3 or 4 is met, that call termination depends on either the access code or the number that followed. Therefore, remember the following when configuring Group Hunt lists:

- Use only one access code for each Group Hunt list. The access code must always be the last entry in the list.
- Use linear hunting. In this configuration, any redirected call is subject to the call processing treatment of the destination.
- If an access code is used as a Group Hunt member, it must be entered as “access code and complete destination number” to ensure proper routing to the destination, not just the access code alone.
- Trunk optimization does not apply.

If termination condition 5 is met, the search ends for the current list and begins for the list associated with the new Pilot DN. A Pilot DN cannot be a member of its own Hunting Group.

If termination condition 6 is met, then incoming calls are placed in a queue in the order of arrival. They are then presented to the next DNs in the group as the members become available.

Direct Inward Dialing (DID) calls are placed in a Group Hunting queue only if the group is still in service. If the group is not in service (if all of its members have deactivated Group Hunting), DID calls are routed directly to the attendant.

Calls are removed from a Group Hunting queue when they are abandoned, when they are presented to an available member, or when they are attendant-extended calls and the slow answer recall timer has expired.

Ringback tone is heard by callers who wait in Group Hunting queues for service.

If the attempted DN for termination by Group Hunting is not a valid member or number, an error message (ERR 8985) prints, hunting terminates, and calls route to overflow tone as specified by the intercept treatment.

Hunt types

Two types of Group Hunt are provided: linear and round robin. Only one hunt type is allowed per Group Hunt List.

- Linear: Hunting starts at the first DN in the list and ends when one of the conditions mentioned in "Termination conditions" on page 302 is met.
- Round Robin: Hunting starts at the DN next in the list to the last DN that was hunted to. Hunting ends when one of the conditions mentioned in "Termination conditions" on page 302 is met.

Group Hunt Lists

Group Hunt lists are defined and modified in LD 18. The Pilot DN entered for each list must have been previously defined as a Group Hunt FFC in LD 57. When a Group Hunt list is defined, the members are assigned a member number as in configuring a Speed Call List. The maximum DN size of each member is 31 digits. The list members can have one of the following DN types:

1 Single or Multiple Appearance DN

2 Listed Directory Number

3 Attendant DN

4 Automatic Call Distribution (ACD-DN), VMS-DN, MC-DN

5 Route access code (route access code + number)

6 Electronic Switch Network (ESN) number (for example, access code + number)

7 Group Hunt Pilot DN

8 Radio Paging access code followed by a complete DN

Note: A Group Hunt list can also be modified through a Speed Call or System Speed Call Controller key, through an analog (500/2500 type) telephone feature Speed Call Controller, or through Group Hunting Speed Call or System Speed Call Controller Flexible Feature Codes (FFC).

Composition of Group Hunt lists

Authorized Group Hunt list members belong to one of the following categories:

- Set-associated DNs (DN type 1) — These DNs are associated with sets and/or keys in a stand-alone system. They are any of the following:
  - — Single-appearance DNs
  - — Multiple-appearance, single-call arrangement DNs
  - — Multiple-appearance, multiple-call arrangement DNs
    - – If MADNs with multiple-call arrangement are to be used in Group Hunt lists, they must have only one Prime DN appearance.
    - – MADNs on analog (500/2500-type) sets with the MCRA class of service (Multiple-call arrangement) are not supported in Group Hunt lists. If one appearance of this MADN is busy, all other appearances are also considered busy by the Group Hunt Cycle.
    - – A set-associated DN can only be defined 96 times as a Group Hunt list member in the system.

- System-associated DNs (DN types 2, 3, 4, 7, 8) — These DNs are associated with other destinations than extensions in a stand-alone system.
- Routing-associated DNs (DN types 5, 6) — These DNs are associated with destinations outside the stand-alone system.

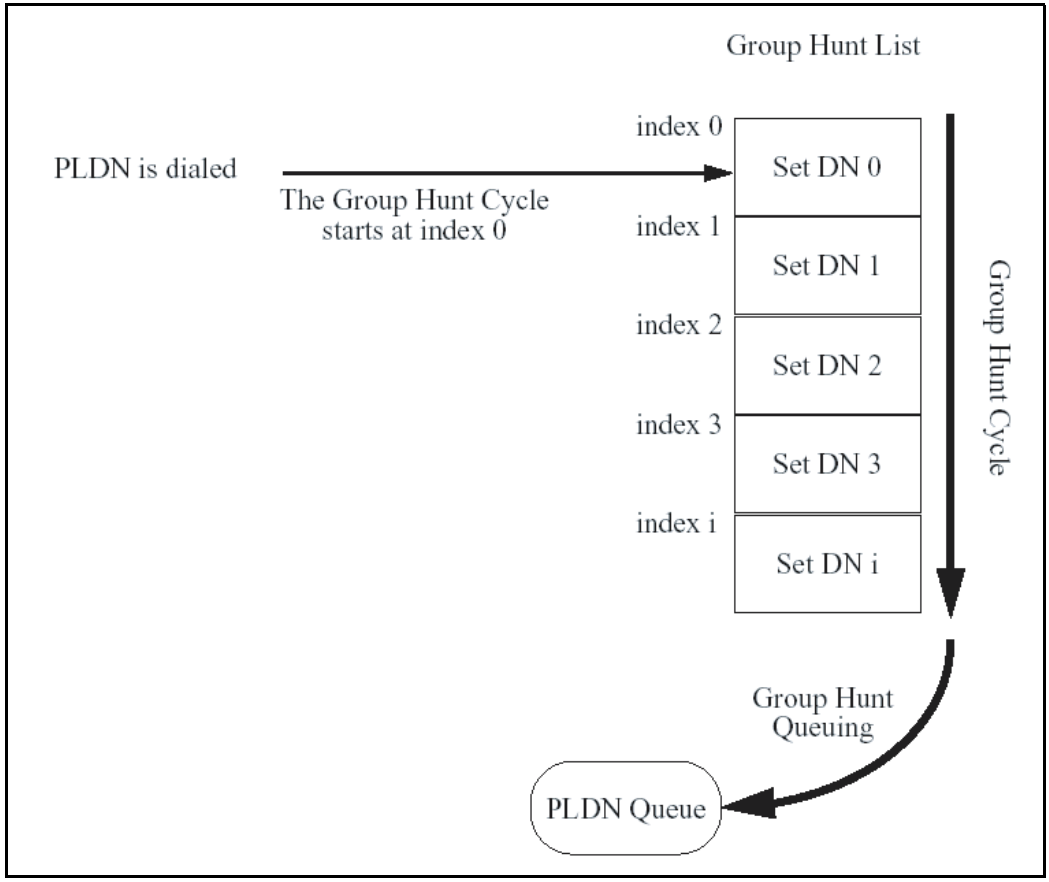
System- or routing-associated DNs always appear available during a Group Hunt cycle. Set-associated DNs do not appear available. Therefore, the Group Hunt cycle always redirects to system-associated and routing-associated DNs when they are met in the list, and the call is never queued against the Pilot DN.

If Linear Hunt is configured for a Group Hunt list that has system- or routing-associated DNs, make these DNs the last entries in the list. List members entered with a higher index are never reached because the system- or routing- associated DNs always route the call.

There are four supported Group Hunt lists:

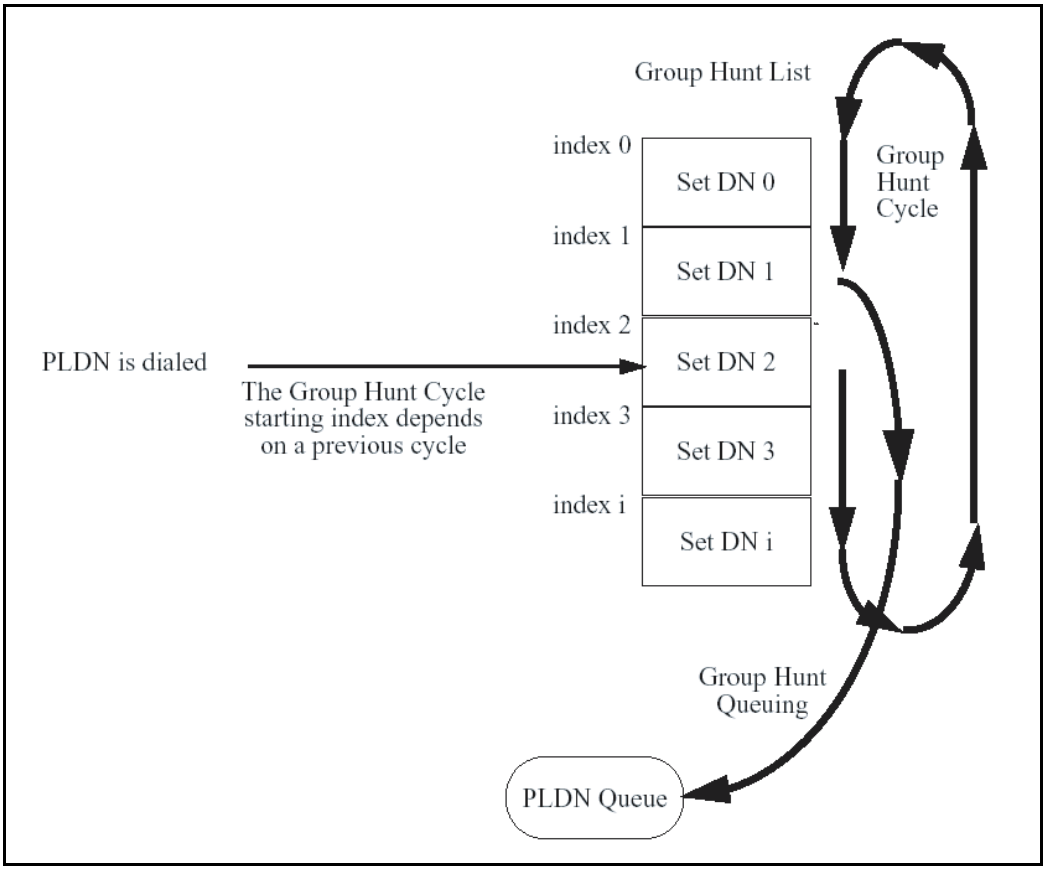
- Type I Group Hunt lists set-associated DNs — These use Linear Hunt type. When the user dials the PLDN, the Group Hunt Cycle offers the call to the first list member. If this member is not eligible, the next member is tried. This process continues until one is found, or until the complete list is searched. Figure 53 on page 307 describes the Group Hunt cycle for Type I Group Hunt lists.

Figure 53
Group Hunt cycle for Type 1 Group Hunt lists



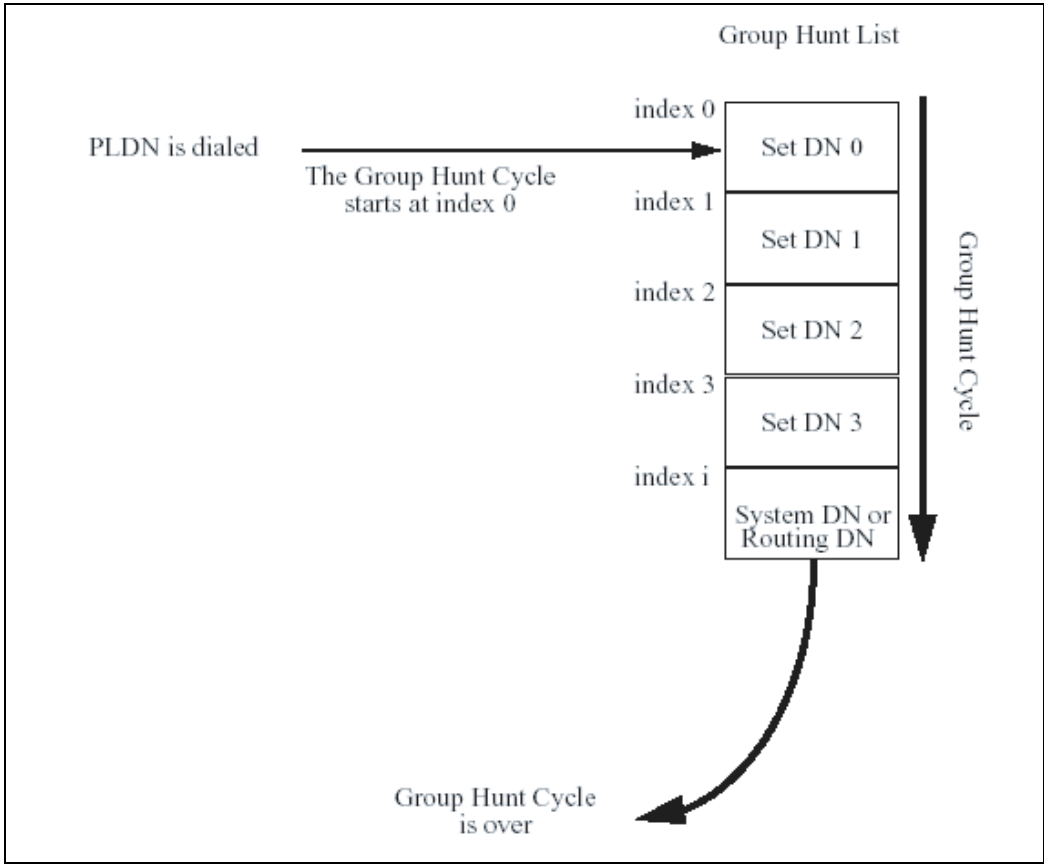
- Type II Group Hunt lists set-associated DNs — These use Round Robin Hunt type. When the user dials the PLDN, the Group Hunt Cycle offers the call to the index next to the last index that was hunted to in the previous cycle. If this member is not eligible, the next DN member is tried. This process continues until one is found, or until the whole list is searched. Figure 54 on page 308 describes the Group Hunt cycle for Type II Group Hunt lists.

Figure 54
Group Hunt cycle for Type II Group Hunt lists



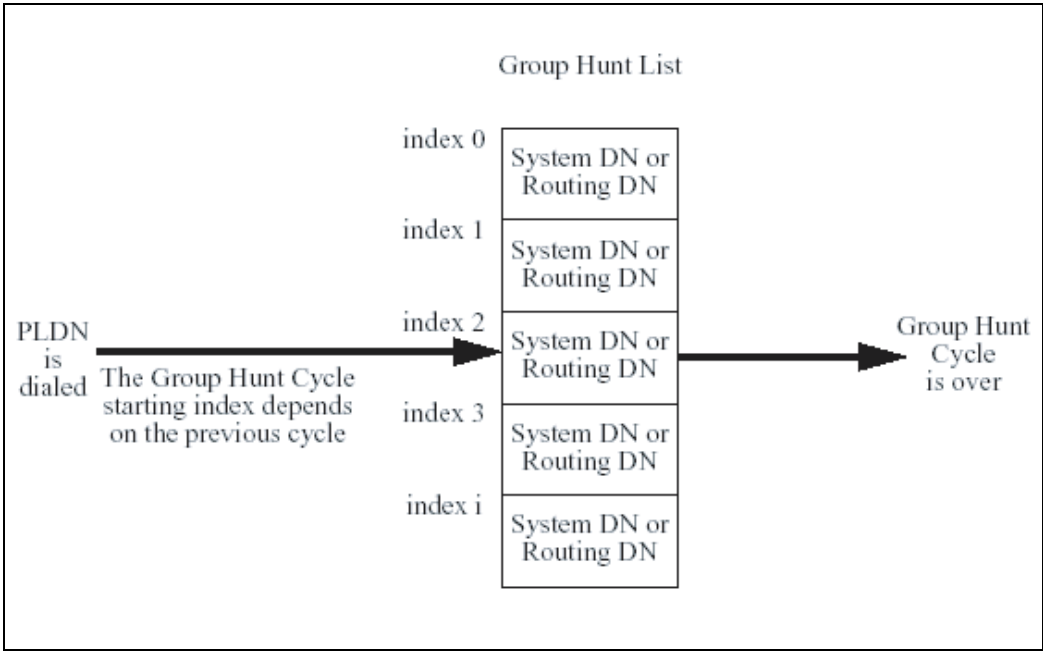
- Type III Group Hunt lists set-associated DNs except for the highest index position, which is filled with a system- or routing-associated DN — These use Linear hunt type. When the user dials the PLDN, the Group Hunt Cycle offers the call to the first list member. If this member is not eligible, the next member is tried. This process continues until one is found. If no member is found, the call is offered to the highest index position (System- or Routing-associated DN). There is no queuing. Figure 55 on page 309 describes the Group Hunt cycle for Type III Group Hunt lists.

Figure 55
Group Hunt cycle for Type III Group Hunt lists



- Type IV Group Hunt lists system- or routing-associated DNs of the same DN type — These use Round Robin hunt type. Once the PLDN has been dialed, the Group Hunt Cycle offers the call to the index next to the last index that was hunted to during the previous cycle. There is no further search in the list nor is there any queuing. Figure 56 on page 310 describes the Group Hunt cycle for Type IV Group Hunt lists.

Figure 56
Group Hunt cycle for Type IV Group Hunt lists



Note: The user must define the Group Hunt list to match one of the four list types.

Queuing

If all members of a Group Hunt list are busy, calls are queued against the Pilot DN of that Group Hunt list. Ring-back tone is provided. There are several options available to control the number of calls allowed to be queued against any given Pilot DN. These options are:

- Group Hunt Queuing Limitation allows the system administrator to select, through service change, the number of calls allowed to queue against the Pilot DN. The selection is made by responding to the Maximum Queue (MQUE) prompt in LD 57. The valid responses to this prompt are:

  — **0**: No calls allowed to queue.

— **1**: One call allowed to queue.

— **ALL**: No limit to the number of calls allowed to queue.

— **ACTM**: The number of calls allowed to queue must be less than or equal to the number of active Group Hunt list members.

Group Hunt Deactivate and Activate

Group Hunt Deactivate allows an idle Set-associated DN to be made non-eligible to Group Hunt calls. A Group Hunt Deactivate FFC code (GHTD) is available to both analog (500/2500-type) and digital sets. The Group Hunt Deactivate key (GHD) can be configured on digital sets.

1 Digital sets

a If the station user activates the DN key, dials the GHTD code and then dials PLDN, the DN is deactivated from the Group Hunt list associated with PLDN. An overflow tone is given if the operation is not successful.

b If the station user activates the DN key and dials the GHTD code, the DN is deactivated from all Group Hunt lists to which this DN belongs. An overflow tone is given if the operation is not successful.

c If the station user activates the GHD key (key lamp is dark), the Prime DN (defined on key 0) is deactivated from all Group Hunt lists to which this Prime DN belongs. The GHD key lamp is lit if the operation is successful. The GHTD code must be used to deactivate non-Prime DNs.

2 Analog (500/2500-type) sets

a If the station user goes offhook, dials the GHTD code, and then dials PLDN, the DN is deactivated from the Group Hunt list associated with PLDN. An overflow tone is given if the operation is not successful.

b If the station user goes offhook and dials the GHTD code, the DN is deactivated from all Group Hunt lists to which this DN belongs. An overflow tone is given if the operation is not successful.

If the DN is a Multiple-Appearance DN, all appearances of the DN are deactivated when a DN member executes one of the deactivation processes.

Group Hunt Activate allows an idle Set-associated DN to return to the active state from the Group Hunt Deactivate state. A Group Hunt Activate FFC code (GHTA) is available to both analog (500/2500-type) and digital sets. A Group Hunt Deactivate key (GHD) can be configured on digital sets.

1 Digital sets

a If the station user activates the DN key, dials the GHTA code and then dials PLDN, the DN is activated again in the Group Hunt list associated with PLDN. Overflow tone is given if the operation is not successful.

b If the station user activates the DN key and dials the GHTA code, the DN is activated again for all Group Hunt lists to which this DN belongs. Overflow tone is given if the operation is not successful.

c If the station user activates the GHD key (key lamp is lit), the Prime DN (defined on key 0) is activated again for all Group Hunt lists to which this Prime DN belongs. The GHD key lamp is darkened if the operation is successful.

2 Analog (500/2500-type) sets

a If the user goes offhook and dials the GHTA code, and then dials PLDN, the DN is activated again for the Group Hunt list associated with PLDN. An overflow tone is given if the operation is not successful.

b If the station user goes offhook and dials the GHTA code, the DN is activated again for all Group Hunt lists to which this DN belongs. An overflow tone is given if the operation is not successful. The GHTA code must be used to activate non-Prime DNs.

If the DN is a Multiple-Appearance DN, all appearances of the DN are activated again when a DN member executes an activation processes.

Access to Group Hunt lists

A Group Hunt list can be accessed by dialing the associated Pilot DN, through:

- manual dialing
- automatic dialing (such as Autodial, Hotline, Speed Call)
- redirection (such as Call Transfer, Call Forward, Hunt)
- ACD Night Service
- ACD interflow/overflow
- trunk access

A Pilot DN can be accessed like any other DN in the network. Any network user can access all Group Hunt lists defined for a network from anywhere in the network. This allows a centralized Group Hunt list to be set up for all network users.

However, Group Hunting is not possible across the network because calls encountering access code entries are always directed to the destination and never return to the hunt queue.

Operating parameters

The Group Hunting feature does not support data calls.

Hunting is limited to the following:

- the total number of DNs in the group
- a maximum of 30 hunting groups for each hunting sequence (for multi-group systems)
- a maximum of 18 hunting groups for each hunting sequence (for all other systems)

Hunting can be limited to the total number of DNs in the group, to 30 hunting groups per hunting sequence for multi-group systems, or to 18 hunting groups per hunting sequence for all other systems.

A maximum of 31 digits can be entered in each list entry.

A maximum of 96 entries can be placed in each list.

A specific station can be defined within a group, among different groups, or a combination thereof a maximum of 96 times.

A maximum of 8000 Group Hunt lists can be defined on a system (programmable through the existing MSCL prompt in LD 17 and reduced by the number of defined Speed Call and System Speed Call lists.)

For larger applications, the ACD package must be equipped to optimize call control and call distribution.

It is recommended that the Group Hunt feature be primarily used with set-associated DNs.

A Group Hunt pilot DN cannot be a member of its own list.

Round Robin hunting should only be used if all entries in the Group Hunt list are the same type (for example, all set-associated DNs or system-associated DNs).

A Pilot DN can be accessed from a network TIE trunk. Also, members of the Group Hunt list can be located at remote nodes.

Feature interactions

Attendant Timed Recalls

Attendant-extended calls to a PLDN will recall to the attendant when the recall timer expires.

- If the call extends to an eligible member in the Group Hunt list, the Slow Answer Recall Timer of the customer applies.
- If the attendant-extended call is queued to the PLDN, the Call Waiting Timer of the customer applies.
- If the attendant-extended call is queued to the PLDN, the Call Waiting Recall Timer is started as explained above; when a list member becomes eligible and is offered the call, the timer re-starts with its Slow Answer Recall value.

If the call is extended to an eligible member that has Call Forward No Answer configured, the Flexible Call Forward No Answer Timer applies instead of the Slow Answer Recall Timer. Ringing in the Group Hunt list continues as long as allowed by CFNA.

Access Restrictions

If a routing-associated DN is programmed in a Group Hunt list, access restrictions apply, based on the Class of Service of the calling station or route, the TGAR of the calling station or route, or both.

Attendant Alternative Answering

A Pilot DN can be defined as an alternative DN. Calls forwarded to a Pilot DN as an alternative DN are directed to the next DN in the group.

Attendant Blocking of Directory Number

It is not possible to activate the Attendant Blocking of DN feature for a Pilot DN. If an attempt is made to block a PLDN, the attempt will be canceled and overflow tone will be returned. If a DN that is a member in a Group Hunt (or Hunt) list is blocked by the Attendant Blocking of DN feature, the DN is considered to be busy.

Attendant Break-in and Toll Operator Break-in

Attendant Break-in and Toll Operator Break-in will not be supported when dialing a Pilot DN directly.

Attendant Busy Verify

An attendant is not allowed to busy-verify when dialing a Pilot DN directly.

Attendant Overflow Position

A PLDN cannot be configured as an Attendant Overflow DN (AODN).

Call Forward All Calls

When Group Hunt attempts to terminate on a DN, which has Call Forward All Calls active, it will continue with the next DN in the group if the attempted DN is busy, or if the DN is idle and the response to the Call Forward Ignore (CFWI) prompt in LD 57 is NO. If the attempted DN is idle and the response to the CFWI prompt in LD 57 is YES, then the system terminates Group Hunt and ring stations associated with the DN.

Call Forward Busy

Group Hunting has priority over the Call Forward Busy feature.

If the DNto be terminate has FBA (Forward Busy Allowed) Class of Service is busy, then Group Hunting continues with the next DN in the group.

Call Forward by Call Type

A Pilot DN can be configured as the redirection DN (HUNT, FDN, EHT, EFD) for the CFCT feature. The interaction is the same as for the Call Forward No Answer feature.

Call Forward External Deny

A Pilot DN cannot be configured as the Call Forward All Calls redirection DN if the set has the CFXD capability allowed.

Call Forward/Hunt Override through Flexible Feature Code

Primary Line Directory Numbers (PLDNs) are not overridden by the Call Forward/Hunt Override Via FFC feature. Any attempt will be ignored and access denied treatment will result.

Call Forward No Answer

Call Forward No Answer (CFNA) can optionally be configured to use a Pilot DN. This option is available when the HUNT DN or the FDN is defined as a Pilot DN.

If an idle station attempted for termination has CFNA defined, then the station will be rung. If the station does not answer within the customer specified number of ring cycles, then Group Hunting will continue with the next DN in the group. The calling party will continue to hear ringback tone until one of the conditions mentioned in "Termination conditions" on page 12 (the last condition is not applicable in this case) is met, or until they release the call.

Call Forward No Answer, Second Level

Second Level Call Forward No Answer will not be applied to calls that are using Group Hunt.

Call Forward No Answer by Call Type

CFNA by Call Type can be configured to use a Pilot DN. This option is available when the EFD or EHT DN is defined as a Pilot DN.

When Group Hunting terminates on an idle station with Call Forward No Answer by Call Type active, treatment will be the same as in the case of CFNA.

Call Forward No Answer, Second Level

Second Level CFNA will not be applied to calls with Group Hunting active.

Call Detail Recording on Redirected Incoming Calls

For the Call Detail Recording on Redirected Incoming Calls feature, in the case of Group Hunt, the Pilot DN is the one before the last set in the redirection chain.

Call Transfer

Any call can be transferred to a Group Hunt Pilot DN. If there are no idle sets available for the call transfer, the call is queued to the Pilot DN and the caller receives ringback tone. If the call cannot be queued because the queue threshold has been reached, the caller receives busy tone.

Call Waiting

Call Waiting to a Pilot DN is not be supported.

Camp-on

Camping an incoming call on to a Pilot DN is not be supported.

Digit Display and Name Display

Until a call is answered, the calling party sees the dialed DN. When the call is answered, the caller sees the dialed DN appended with the DN and name of the calling party, if Calling Party Name Display (CPND) is equipped. The terminating set will always see the originating DN appended with a Pilot DN.

Digital Private Network Signaling System (DPNSS1)/Digital Access Signaling System (DASS2) Uniform Dialing Plan (UDP) Interworking

Only basic DPNSS1 UDP calls are supported with Group Hunting. Interactions between DPNSS1 Supplementary Services and Group Hunting are not supported.

DPNSS1 Diversion

Only simple DPNSS1 calls support Group Hunting. All DPNSS1 supplementary services do not support Group Hunting.

Do Not Disturb

Do Not Disturb (DND) has priority over Group Hunting. Group Hunting will skip over sets with DND active.

Enhanced Night Service

If a Pilot DN is defined as one of the NITE DNs from the list associated with the Trunk Night Group, then incoming calls directed to the Pilot DN will be presented to the next idle DN in the hunt group.

Electronic Switched Network

Group Hunting can be applied to Network calls. An Electronic Switched Network (ESN) access code (trunk steering code), if encountered during Group Hunting, will terminate the hunting sequence.

Hunting

Group Hunting has priority over Hunting. If the DN attempted for termination by Group Hunting has HTA COS, and if it is busy, Group Hunting continues with the next DN in the group instead of following the DN's hunting configuration.

ISDN QSIG/EuroISDN Call Completion

Call Completion to Busy Subscriber cannot be applied to Pilot DN when no idle set is located during a Group Hunt call.

Last Number Redial
Stored Number Redial

A Pilot DN will be stored as a Last Number Redial (LNR) and Stored Number Redial (SNR) number when it is dialed directly.

Make Set Busy

Make Set Busy (MSB) has priority over Group Hunting. Group Hunting will skip over sets with MSB active.

Multiple Appearance Directory Number

While Multiple Appearance DNs (MADN) single call arrangements are treated the same as Single Appearance DNs (SADN), MADN multiple call arrangements must be avoided in a Group Hunt list.

With MADN multiple call arrangement, the idle or busy status of the MADN is determined by the Terminal Number (TN) data block of the prime appearance of the called DN. If there is more than one prime appearance of the called DN, the idle or busy status is then selected from the last TN in the DN block for the MADN (DNB prompt in LD 22). This means that there can be idle appearances of the MADN, while the hunt cycle regards them as busy and attempts to terminate on the next idle member of the Group Hunt list.

If an MADN multiple call arrangement must be used, a supervisor set must be assigned to the hunt group. This supervisor set must be given the one and only prime appearance of the MADN. Any other appearance must have the MADN programmed as a secondary DN (any DN key other than 0). In this way, the supervisor set controls the status of the MADN and thus the Group Hunt treatment. If the supervisor set is busy, the hunt does not terminate on the MADN.

Multi-Party Operations

As per the existing Multi-Party Operations (MPO) feature, recovery of misoperation of Call Transfer will not be applied to incoming calls which are transferred on ringing to a Pilot DN by transferring parties who are waiting in GPHT queues for service.

Night Answer by Time of Day

If a Pilot DN is defined as one of the NITE DNs in LD 15, then incoming calls directed to the Pilot DN will be presented to the next idle DN in the group. At the instant of changeover (change from one night DN to another), Group Hunting, if still active, will keep on hunting for the next idle DN in the group.

Night Service

If a Pilot DN is defined as a NITE DN or trunk NITE DN, then incoming calls directed to the NITE DN or trunk NITE DN will be presented to the next idle station in the hunt group.

On Hold on Loudspeaker

Group Hunt to a loudspeaker DN can be programmed, but will be ignored if configured as Make Set Busy (MSB) by call processing.

Override
Ring Again

Override and Ring Again will not be supported.

Recall to Same Attendant

Calls redirected from a Group Hunt list through the listed DN or flexible attendant DN, and transferred back to the Pilot DN, are recalled if the Slow Answer Recall Timer expires. However, in practical configurations, the hunt terminates on the entry with the listed DN or attendant DN before the Slow Answer Recall Timer expires; consequently, the call is not redirected to that DN and presented on the applicable ICI key on the console. Therefore, the call is never presented as a recall, so that Recall to the Same Attendant does not apply.

Recorded Announcement

Calls which are queued against the Group Hunt Pilot DN cannot receive Recorded Announcement.

Remote Call Forward

If Call Forward All Calls is activated remotely, the interaction with Group Hunting is the same as Call Forward All Calls.

Ring Again on No Answer

Ring Again on No Answer cannot be applied if the DN dialed was a Pilot DN.

Slow Answer Recall

Calls extended by the attendant to the Group Hunt Pilot DN are recalled to the same attendant, after the Slow Answer Recall timer expires. This only applies to a standalone configuration; Network Attendant Service (NAS) is not supported.

Tenant Service

If a Pilot DN is defined as a Tenant NITE DN, then incoming calls directed to the Pilot DN will be presented to the next idle DN in the hunt group.

Total Redirection Count

Group Hunt takes precedence over the Total Redirection Count feature, in that the TRCNT limit is not applied to a Group Hunt call.

Warning Tone

Warning Tone is not applied to queued calls, if the French Type Approval package (197) is not equipped. If the French Type Approval package (197) is equipped, a warning tone of Camp-on can be provided to the first active member of a Group Hunt list that has Warning Tone Allowed (WTA) Class of Service (COS). Any new call in the queue is announced to the next set in the hunt chain that has WTA COS.

16-Button Digitone/Multifrequency Operation

Group Hunt Pilot DN (GRHP) function will not be supported. Group Hunting and Speed Call DN Access can be accessed through the Autodial function.

Feature packaging

Group Hunt requires the following packages:

For markets other than France:

- Group Hunt/DN Access to SCL (PLDN) package 120, which has the following dependencies:
  - System Speed Call (SSC) package 34
  - International Supplementary Features (SUPP) package 131 where applicable
  - Flexible Feature Codes (FFC) package 139

For the French market only:

- French Type Approval (FRTA) package 197 and Group Hunt/DN Access to SCL (PLDN) package 120, which has the following dependencies:
  - System Speed Call (SSC) package 34
  - International Supplementary Features (SUPP) package 131
  - Flexible Feature Codes (FFC) package 139

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1 LD 17 – Enter the number of Group Hunt lists allowed in the system.

2 LD 15 – Enter a Group Hunt PLDN.

3 LD 10 – Enter a Group Hunt Pilot DN (PLDN).

4 LD 11 – Enter a Group Hunting Denied (GHD) key and enter a Group Hunt PLDN. LD 11 is modified to disallow the removal of the last appearance of a Single Call Non-ringing (SCN), Single Call Ringing (SCR), Multiple Call Non-ringing (MCN), or Multiple Call Ringing (MCR) DN which is part of a Group Hunt list. This ensures the DN is removed from all Group Hunt lists prior to being removed from a set.

5 LD 12 – Enter a Group Hunt PLDN.

6 LD 14 – Enter a Group Hunt PLDN.

7 LD 18 – Create or modify Group Hunt lists. Responses are required to the following prompts when a Group Hunt list is modified, created, or removed. This overlay disallows the removal of a Group Hunt list if it is still associated with a PLDN that exists in LD 57. This ensures the PLDN is removed prior to removing the Group Hunt list.

8 LD 57 – Define or change data associated with FFC.

9 LD 57 – Configure Flexible Feature Codes data block for Group Hunt Termination.

LD 17 – Enter the number of Group Hunt lists allowed in the system.

Prompt	Response	Description
REQ	CHG	Change the Configuration Record.
TYPE	PARM	System Parameters
...	...	
MSCL	0-8191	Number of Group Hunt lists allowed in the system.

LD 15 – Enter a Group Hunt PLDN. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW	Add new data.
TYPE:	NIT	Night Service Options
...		
- NIT1	x...x	First Night service by time of day DN **can be defined as a PLDN.**
- TIM1	...	Hour and Minute for First Night Service DN.
- NIT2	x...x	Second Night service by time of day DN **can be defined as a PLDN.**
- TIM2	...	Time for Second Night Service DN.
- NIT3	x...x	Third Night service by time of day DN **can be defined as a PLDN.**
- TIM3	...	Time for Third Night Service DN.

LD 15 – Enter a Group Hunt PLDN. (Part 2 of 2)

- NIT4	x...x	Fourth Night service by time of day DN **can be defined as a PLDN.**
- TIM4	...	Hour and Minute for Fourth Night Service DN.

LD 10 – Enter a Group Hunt Pilot DN (PLDN).

Prompt	**Response**	**Description**
REQ:	NEW CHG	Add new data, or change existing data.
...		
IAPG	0-15	Meridian Link Unsolicited Status Message (USM) group
HUNT	x...x	Hunt DN of the next station in the Hunt chain. Hunt DN can be defined as a PLDN.
...		
AACD	(NO) YES	Associate set (AST) telephone
FTR	FTR	Enter the feature name and related data.
	EFD x...x	External Flexible call forward DN (a Group Hunt pilot can be entered.) External Call Forward No Answer DN can be defined as a PLDN.
	EHT x...x	External Hunt DN External Hunt DN can be defined as a PLDN.
	FDN x...x	Flexible Call Forward No Answer Call Forward No Answer DN can be defined as a PLDN.

LD 11 – Enter a Group Hunting Denied (GHD) key and enter a Group Hunt PLDN.
(Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
...		
AOM	0-2	Number of Add-on Modules. AOM appears if TYPE = M2216 and M2616
FDN	x...x	Flexible CFNA DN Call Forward No Answer DN can be defined as a PLDN.
...		
ICT	0-<NIPN>	Intercept Computer Terminal or printer number Number of Intercept Positions (NIPN) is defined in LD 15.
EFD	x...x	Flexible CFNA DN for External calls External Call Forward No Answer DN can be defined as a PLDN.
HUNT	x...x	Hunt DN of next station in hunt chain Hunt DN can be defined as a PLDN.
EHT	x...x	External Hunt DN External Hunt DN can be defined as a PLDN.
...		
LANG	(0)-5 X	Language choice for Automatic Wakeup (AWU) calls. Prompted with Multi-language Wakeup (MLWU) package 206.
KEY	xx aaa yyyy	Telephone key assignments.

LD 11 – Enter a Group Hunting Denied (GHD) key and enter a Group Hunt PLDN. **(Part 2 of 2)**

	xx CFW yy z...z	Call Forward key Key number (xx), Call Forward function (CFW), length (yy), Call Forward target DN (z...z) can be defined as a PLDN.
	xx GHD	Key number (xx), Group Hunting Denied function (GHD). The GHD key is added to allow a station user to toggle the Primary (key 0) Directory Number (PDN) in and out of all groups of which that PDN is a member.

LD 12 – Enter a Group Hunt PLDN.

Prompt	Response	Description
REQ	NEW CHG	Add new data, or change existing data.
...		
ICP	(NO) YES	Intercept Computer available.
AADN	x...x	Attendant Alternate Answering DN. Alternate Answering DN can be defined as a PLDN.

LD 14 – Enter a Group Hunt PLDN. **(Part 1 of 2)**

Prompt	Response	Description
REQ	NEW CHG	Add new data, or change existing data
...		
NGRP	(0)-9	Night Service Group number
NITE	x...x	Night Service directory number Night service DN can be defined as a PLDN.

LD 14 – Enter a Group Hunt PLDN. **(Part 2 of 2)**

ATDN	x...x	Auto-terminate DN Auto-terminate DN can be defined as a PLDN.
MNDN	x...x	Manual Directory Number Manual DN can be defined as a PLDN.

LD 18 – Create or modify Group Hunt lists. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG MOV NEW OUT	Change, move, create, or remove a data block.
TYPE	GHT	Group Hunt data block
LSNO	 1-8190 <CR>	List Number Group Hunt lists Use only when REQ = CHG and TYPE = GHT
CUST	 0-99 0-31	Customer number, as defined in LD 15. For Large Systems For Small Systems and Succession 1000 systems
PLDN	x...x	Pilot DN: Prompted when REQ = NEW or CHG and LSNO = <CR>.
DNSZ	4-(16)-31	Directory Number Size Maximum length of DN allowed for Group Hunt list. Prompted when REQ = NEW or CHG and LSNO = <CR>. After DNSZ is defined, it should not be changed. Print the list in LD 20, remove it with REQ = OUT, and rebuild the list with the new DNSZ.
SIZE	 1-96 1-1000	Size of list Maximum DNs in Group Hunt list Range is 1 to 96 entries if response to TYPE is GHT. Range is 1 to 1000 if response to TYPE is SCL or SSC.

LD 18 – Create or modify Group Hunt lists. (Part 2 of 2)

STOR	...	Store: Enter entry (member) number (x...x) and Group Hunt target DN (y...y). For TYPE = GHT the input format is Group Hunt entry and digits stored against it: Where:
	x...x	x...x = GHT entry number from 0 to 95
	y...y	y...y = digits stored
	<CR>	Stop STOR prompt In Group Hunting the member number must conform with the SIZE; the number of digits must conform with DNSZ.
	xx<space><CR>	Remove entry
WRT	(YES) NO	Write Write information to data store.

LD 57 – Define or change data associated with FFC. (Part 1 of 2)

Prompt	**Response**	**Description**
REQ	CHG NEW	Add new data, or change existing data.
TYPE	FFC	Flexible Feature Codes data block.
CUST		Customer number, as defined in LD 15
	0-99	For Large Systems
	0-31	For Small Systems and Succession 1000 systems
FFCT	<CR>	Flexible Feature Confirmation Tone.
CODE	PLDN	Code to be modified or created: Pilot DN.
- PLDN	xxxx	Pilot DN: enter Pilot DN to be modified or created.
	<CR>	Enter a carriage return to proceed to next prompt.
-- USE	GPHT	USE: enter USE for Pilot DN Group Hunting.
-- LSNO	xxxx	List Number: enter Group Hunt list number. Group Hunt list must exist in LD 18.

LD 57 – Define or change data associated with FFC. (Part 2 of 2)

-- HTYP	(LIN) RRB	Hunting Type: enter either (Linear) or Round Robin as the type of hunting to be used for the Group Hunt list.
-- CFWI	(NO) YES	Call Forward All Calls Idle: Where: enter NO if Group Hunting is to skip idle stations with Call Forward All Calls active, or enter YES if Group Hunting is to terminate on idle stations with Call Forward All Calls active.
MQUE	 0 1 (ALL) ACTM	Maximum Queue (maximum number of calls allowed to queue against the Pilot DN. Where: Enter 0 to deny all calls from queuing Enter 1 to allow only one no call to queue Enter ALL, the default, to allow all calls to queue or Enter ACTM to limit the number of calls allowed to queue to be less than or equal to the number of active members of the Group Hunt list.

LD 57 – Configure Flexible Feature Codes data block for Group Hunt Termination. (Part 1 of 2)

Prompt	**Response**	**Description**
REQ	CHG NEW	Add new data, or change existing data.
TYPE	FFC	Flexible Feature Codes data block.
CUST	 0-99 0-31	Customer number, as defined in LD 15. For Large Systems For Small Systems and Succession 1000 systems
FFCT	<CR>	Flexible Feature Confirmation Tone.
CODE	GHTA	Code to be modified or created: Group Hunt Termination Allowed.
- GHTA	x...x	Enter code to be dialed to allow Group Hunt termination on a set.

LD 57 – Configure Flexible Feature Codes data block for Group Hunt Termination. (Part 2 of 2)

CODE	GHTD	Code to be modified or created: Group Hunt Termination Denied.
- GHTD	x...x	Enter code to be dialed to deny Group Hunt termination on a set.

Feature operation

No specific operating procedures are required to use this feature.

Internet Telephone Enhancements

Contents

This section contains information on the following topics:

Feature description

Internet Telephone Enhancements enhances the functionality of the i2002 and i2004 Internet Telephones and the i2050 Software Phone.

i2002 and i2004 Internet Telephones

Internet Telephone Enhancements introduces the following enhancements to i2002 and i2004 Internet Telephones:

- Three new user-selectable languages for the display and menus:
  - Latvian
  - Russian
  - Turkish

- The Ringer/Buzzer sounds while the user adjusts the ring/buzz level.
- Both the registered and configured TNs are displayed in the Set Info menu.

Volume settings

The i2002 and i2004 Internet Telephones have additional non-volatile memory, which enables the TPS to store the user volume settings in the Internet Telephone. The previous versions of the i2002 and i2004 Internet Telephones lost the volume settings, and reverted back to the default values, if the system is initialized, if the LTPS fails, or if there is a power-up cycle.

i2050 Software Phone

The following enhancements to existing functionality affect the i2050 Software Phones:

- Both the registered and configured TNs are displayed in the Set Info menu.
- Modem support to configure the Software Phone for dial-up access.

Operating parameters

The minimum required software to support Internet Telephone Enhancements is the following:

- Internet Telephone firmware 1.5x
- IP Line 3.1
- Succession 3.0 software

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

There are no specific packaging requirements associated with this feature.

Feature implementation

There are no feature interactions associated with this feature.

Feature operation

No specific operating procedures are required to use this feature.

Internet Telephone Virtual Office

Contents

This section contains information on the following topics:

Feature description

The Virtual Office feature enables users to log in to any Internet Telephone using their own User ID and password. This redirects the user's telephone calls and other features to the Virtual Office logged-in Internet Telephone. The users can perform most Internet Telephone functions exactly as if they were using their regular Internet Telephone.

Upon login, the Internet Telephone de-registers with the Call Server and registers to the Call Server associated with the given User ID. This can be the same Call Server or another Call Server within the network. If it is another Call Server, a Nortel Gatekeeper is required to provide the address of the Internet Telephone Terminal Proxy Server (TPS) node. Upon logout from Virtual Office, the Internet Telephone registers to the Call Server associated with the settings stored in its EEPROM: the S1 server and Terminal Number (TN).

To login using Virtual Office, the TN associated with the current Internet Telephone registration must be configured with the Virtual Office Login Allowed (VOLA) class of service. The TN associated with the User ID for the login must be configured with the CLS VOUA (Virtual Office User Allowed). For more information on VOLA and VOUA, refer to LD 11 and LD 81 in *Software Input/Output: Administration* (553-3001-311).

The i2002, i2004, and i2050 Internet Telephones support the Virtual Office feature. Refer to the following documents for more information:

- *Internet Terminals: Description* (553-3001-368)
- *i2002 Internet Telephone User Guide*
- *i2004 Internet Telephone User Guide*
- *i2050 Software Phone User Guide*

The Virtual Office feature supports only one customer. If two or more customers are configured, the one with the lowest customer number is supported.

Operating parameters

The following is the minimum software and hardware for Internet Telephone Virtual Office:

- Succession 3.0 software and hardware
- IP Line 3.1
- i2050 software build 301
- Element Manager

Firmware upgrade

The Virtual Office feature requires UNIStim protocol version 2.5, which is supported in firmware version 1.33 or later. No firmware upgrade takes place during a Virtual Office login.

The **umsUpgradeAll** command has no impact on Internet Telephones logged into Virtual Office. These telephones are not reset. If the Virtual Office login is within the same call server, the Internet Telephone firmware is upgraded after the user has logged out. If the Virtual Office login is between different call servers, the Internet Telephone simply registers back to its home TPS, and follows the normal firmware upgrade rules for regular registration.

Feature interactions

Automatic Call Distribution (ACD)

Automatic Call Distribution (ACD) agents that require the Virtual Office login must have a separate, single appearance DN assigned to a programmable feature key. This unique DN is the User ID for Virtual Office login.

Branch Office DN

When a Virtual Office login is used for a Branch Office DN, the Branch Office Internet Telephone is preempted.

When the Branch Office Internet Telephone is in survival mode and there is a Virtual Office login for that DN, the Branch Office DN becomes registered to the Main Office *and* the Branch Office. This situation is resolved when WAN connectivity resumes and the Internet Telephone, in local mode, is redirected to register with the Main Office TPS in a logged out state.

Gatekeeper end points

Virtual Office support is limited to Internet Telephones registered with Call Servers that are configured as end points in the same Gatekeeper. Virtual Office login between Internet Telephones registered with Call Servers that are configured as end points of different Gatekeepers is not supported.

Internet Telephone options

The Internet Telephone options are retained within the telephone regardless of the registered User ID. Remote Virtual Office logins display the time and date of the remote call server.

Multiple Appearance Directory Number (MADN)

When a Multiple Appearance Directory Number (MADN) is used for Virtual Office login, the TN is selected to match the provided SCPW. If this is not desirable, then a separate, secondary, single appearance DN can be assigned. After login using the single appearance DN, the user receives the assigned key map and feature key list that includes the MADN.

If there is no matching SCPW, an *Invalid ID* error displays. The login session assumes all the features of this TN (the same as a regular registration).

Registration lockout

If a user enters an incorrect password for the Virtual Office login three consecutive times, the TN is locked for one hour. This is known as *Password guessing protection.* When locked out, an information message is written to the call server history file and printed to the TTY. The craftsperson can unlock the TN by disabling and then re-enabling the TN in LD 32. This lockout does not survive re-registration of the Internet Telephone.

Virtual Office login using UDP

When a Branch User in local mode performs a Virtual Office login using UDP to a Branch User TN, the Internet Telephone attempts to register to the Main Office TN. Therefore, Virtual Office login using UDP will fail if the WAN connection to the Main Office is down.

Virtual Office preemption

If a user is already logged into Virtual Office, the user can log in again on another Internet Telephone. This is useful if the user forgets to log out of an Internet Telephone and returns to his/her desk. The home Internet Telephone or the logged in Virtual Office Internet Telephone is preempted upon a successful login on another Internet Telephone. The preempted Internet Telephone remains registered to the TPS but not to the Call Server, and is forced to register to the TN configured on the Internet Telephone.

Since only one registration can exist for each TN within a Call Server, the Internet Telephone is no longer operational, as indicated by the Logout Screen on the display.

The preempted Internet Telephone can be used by another user for a Virtual Office login or it can be re-registered as the home Internet Telephone. The preempted call server registration may be a regular registration (one in which the Internet Telephone's EEPROM S1 and TN settings match the login TN within the associated call server), a Virtual Office login, or a Branch User login. If it is a regular registration, the subsequent login is resolved within the call server as a regular registration, not a Virtual Office login or a Branch User login.

When a virtually logged in Internet Telephone resets, it attempts to register with the call server associated with its S1 and TN. If the TN has a Virtual Office login or Branch User login, then it does not register to its call server but displays the Logout Screen.

When attempting to login, if there is an existing log in to the same User ID or a home Internet Telephone for the User ID that is not in the idle state (for example, ringing, ringback, or in a call), the new login attempt gets a Login Busy message.

Feature packaging

Virtual Office requires the following packages:

- Virtual Office (VO) package 382
- Virtual Office Enhancement (VOE) package 387

Feature implementation

LD 11 – Configure Virtual Office.

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
TYPE:		Telephone type
	i2002	i2002 - Internet Telephone
	i2004	i2004 - Internet Telephone
	i2050	i2050 - Software phone
CUST	xx	Customer number, as defined in LD 15.
...		
CLS		Class of Service
	(VOLA)	Virtual Office Login Allowed on this TN
	VOLD	Virtual Office Login Denied on this TN
	(VOUA)	Virtual Office User Allowed on this TN using another telephone
	VOUD	Virtual Office User Denied on this TN using another telephone

Feature operation

Virtual Office supports the following operations:

- Virtual Office login
- Virtual Office connection
- Virtual Office logout

Virtual Office login

Since i2004 and i2050 Internet Telephones have more key functions than the i2002, a Virtual Office login from an i2002 Internet Telephone to an i2004 or i2050 TN is blocked if:

- Key 0 is ACD.
- Any key (from key 4 to key 15) is defined as AAK, CWT, DIG, DPU, GPU, ICF, MCN, MCR, MSB, PVN, PVR, SCR, or SCN.

If a login is attempted in the above situation, an error message displays.

Note: Features configured on DN/Feature keys higher than key 3 on the i2004 Internet Telephone or i2050 Software Phone are not accessible when logged in from an i2002 Internet Telephone.

This procedure explains how to log in to Virtual Office. The Internet Telephone is operating in Normal Mode.

Procedure 16
Performing Virtual Office login

1 Press the **Services** key to display the **Options** menu.

Note: The i2002 screen displays only one line at a time. Use the **up/down arrow** key to scroll through the menu.

2 Use the **down arrow** key to highlight **Virtual Office Login**.

3 Press the **Select** softkey.

The screen prompts for the User ID.

4 Enter the User ID.

The UserID is the user's internal telephone number. Depending on the network configuration of the system and where the Virtual Office login takes place, the UserID can be:

UserID	Explanation
UDP number	A user with a Home Location Code (HLOC) of 343 visits a site where the HLOC is 393. The UserID is 6 343 5555, where: 6 = network access code (access to ESN) 343 = Home Location Code (HLOC) 5555 = Directory Number (DN).
CDP number	A user with a HLOC of 343 wants to do a Virtual Office login from the same site (HLOC = 343), on a different Internet Telephone. The UserID is 5555. ***Note:*** The UserID of 6 343 5555 is also acceptable.
Transferable DN	A user with HLOC of 343, using a transferable DN, is permanently transferred to a site where HLOC is 393. The previous location DN (5555) is retained as the UserID. ***Note:*** The UserID of 6 393 5555 is also acceptable.

5 Press the **Select** softkey.

The screen prompts for the Station Control Password (SCPW).

6 Enter the SCPW for the Main Office Internet Telephone.

When the User ID is not found locally, the message Locating Remote Server displays to indicate that connection setup is ongoing. A Nortel Gatekeeper provides the node IP address of the Home TPS associated with the User ID. The local TPS confirms connectivity to the remote TPS, then the Internet Telephone is redirected to the remote Home TPS.

End of Procedure

Login failures and errors

A Virtual Office login fails if any one of the following states occurs:

- The login User ID is not local and there is a failure to get a response from a Gatekeeper.
- The User ID is not local and the Gatekeeper does not know the endpoint of the User ID.
- The User ID is not local and the Home TPS is unreachable.
- The User ID is not known or a MADN cannot be resolved at the Home call server.
- An SCPW is not configured for the User ID.
- The destination TN has Virtual Office User Denied (VOUD).
- There already exists a non-idle registered instance for the User ID.
- The user selects **Cancel** after a password failure.
- The password fails to authenticate after three attempts.
- The User ID entry in the Gatekeeper database points back to the originating Call server.

Refer to Table 44 for system messages, potential causes, and available actions.

Table 44
System messages (Part 1 of 3)

Message	Cause	Action
Busy, try again	Remote Internet Telephone is active (not idle).	Wait for remote Internet Telephone to become idle and try again.
	ACD is logged in.	Logout ACD before Virtual Office login from another Internet Telephone.
	Make-Set-Busy is inactive on ACD Internet Telephone.	Set Make-Set-Busy active on ACD Internet Telephone.

Table 44
System messages (Part 2 of 3)

Message	Cause	Action
Invalid ID (1)	Incorrect User ID entered. User ID is not in Gatekeeper database.	Enter correct User ID. Update Gatekeeper database to include User ID.
Invalid ID (2)	Incorrect User ID entered.	Enter correct User ID.
Invalid ID (3)	Incorrect User ID entered. User ID in Gatekeeper database points to originating call server.	Enter correct User ID. Change Gatekeeper configuration for the User ID to point to the correct endpoint.
Locked from Login	Three failed attempts to enter the correct SCPW.	Wait one hour for lock to clear automatically, or disable and enable the remote Internet Telephone in LD 32 at the call server to clear the lockout.
Logged Out	Home TN in use by Virtual Office.	Login to another TN using Virtual Office. Re-register as the Home (or Branch) Internet Telephone.
Permission Denied (1)	SCPW is not configured or enabled.	Configure a SCPW for the remote Internet Telephone.
Permission Denied (3)	Incorrect User ID entered. SCPW is not configured.	Enter correct User ID. Configure a SCPW for the remote Internet Telephone.
Permission Denied (4)	Incorrect User ID entered. Attempt to login to an i2004/i2050 TN from an i2002 Internet Telephone.	Enter correct User ID. Go to an i2004/i2050 Internet Telephone and try again.

Table 44
System messages (Part 3 of 3)

Message	Cause	Action
Permission Denied (5)	Incorrect User ID entered. The destination TN has Virtual Office User Denied (VOUD) configured.	Enter correct User ID. Configure the remote Internet Telephone with Virtual Office User Allowed (VOUA).
Permission Denied (6)	Incorrect User ID entered. Incorrect SCPW is entered.	Enter correct User ID. Enter correct SCPW.
Server Unreachable (1)	Gatekeeper is down. The link to Gatekeeper is down.	Bring Gatekeeper up. Restore link to Gatekeeper.
Server Unreachable (2)	Remote TPS is down. Link to remote TPS is down. Remote Call Server is down.	Restore remote TPS. Restore link to remote TPS. Bring remote Call Server up.

Virtual Office connection

An Internet Telephone is registered with the TN in its EEPROM and then a User ID and password are used to determine the home TPS for the Internet Telephone during the Virtual Office connection. A Nortel Gatekeeper is required, if the home TPS is not the TPS where the Internet Telephone is registered when the user initiates a Virtual Office login.

Upon login, the Internet Telephone receives the features, time, date, and tones of the home call server. The Internet Telephone becomes part of the home zone and receives call service from this call server. When this zone is remote, voice quality may be degraded because codec selection is based on the Internet Telephone being in its expected location (subnet). Firmware upgrade on a TPS node does not upgrade the telephones logged into Virtual Office.

The Internet Telephone options stored locally in the telephone's non-volatile memory retain the characteristics of the Internet Telephone. That is, items from the Option menu such as language, display contrast, date and time format, and ring type retain the Internet Telephone properties and do not change to reflect the preferences on the Virtual Office user's home Internet Telephone.

If the Virtual Office user changes these settings, the changes persist in the Internet Telephone even after logout, power-up, or reboot. In other words, changes to Telephone Options menu items are retained (in the Internet Telephone's EEPROM) regardless of who is registered. When changing any of these preferences, the original settings should be restored as a courtesy upon logout.

When connected to a call server through Virtual Office, local trunks are the home CO and a call for emergency service is directed to the home PSTN. This is not ideal when the home is remote.

Virtual Office logout

The Virtual Office user initiates a logout by:

- Performing a direct Virtual Office logout on the active Internet Telephone (see Procedure 17 on page 349).
- Returning to the home location and re-registering the home Internet Telephone (using the **Home** or **Branch** softkey). This forces a logout on the idle Virtual Office Internet Telephone registered to the same User ID.
- Performing a Virtual Office login on another Internet Telephone. This forces a logout on the idle Virtual Office Internet Telephone registered to the same User ID.

The Virtual Office user is forced to logout when:

- the Internet Telephone power cycles
- the Internet Telephone loses connectivity to the Home TPS
- the automatic logout activates (see "Virtual Office auto-logout" on page 349)

Upon logout, the Internet Telephone returns to its regular key map unless the TN owner has an active Virtual Office login or Branch User login. In these cases, the Internet Telephone displays the Logout screen. If connectivity to the Home Office is lost during a Virtual Office login, calls are not maintained and the Internet Telephone re-registers to its configured TN and call server.

Procedure 17
Performing Virtual Office logout

This procedure explains how to logout of Virtual Office. The Internet Telephone is operating in Normal Mode.

1 Press the **Services** key to display the **Options** menu.

Note: The i2002 screen displays only one line at a time. Use the **up/down arrow** keys to scroll through the menu.

2 Use the **down arrow** key to highlight **Virtual Office Logout**.

3 Press the **Select** softkey.

End of Procedure

Virtual Office auto-logout

The Virtual Office user can be configured to automatically logout of all Virtual Office connections at a specified hour. This is configured in LD 15 at the following prompts:

- VO_ALO (YES/NO) – enables/disables automatic logout.
- VO_ALOHR (0-23) – sets hour to activate automatic logout.

Refer to *Software Input/Output: Administration* (553-3001-311) for more information.

M3900 Full Icon Support

Contents

This section contains information on the following topics:

Feature description

The M3900 Full Icon Support feature enables distinct icons and flashing cadences for the display of different call states. These icons are displayed for the Directory Number (DN) keys on the Phase II and Phase III M3903 and M3904 telephones, as well as the Phase III M3905 telephones.

The icons also display on the Key-based expansion modules and Display-based expansion modules. This feature allows the user to quickly determine the call state of a DN, instead of viewing just the flashing cadence of a single generic icon to determine the call state.

The functions displayed with the Full Icon support feature are: I-Ringing, I-Active, U-Active, I-Hold, and U-Hold. The icons appear on the LCD

displays located next to the DN keys. The scenarios for these icons are as follows:

- **I-Ringing:** The I-Ringing icon is displayed on the ringing DN of a set that is being called.
- **I-Active:** The I-Active icon is displayed on DNs on sets in the active call state.
- **U-Active:** The U-Active icon appears on the MADN of a set when another set on the MADN is in the active call state.
- **I-Hold:** The I-Hold icon appears on the DN of the set that has a call on hold.
- **U-Hold:** The U-Hold icon appears on the MADN of a set when another set on the MADN has a call in the hold state.

The Ringing, I-Hold, U-Hold, and Active DN keys, represented by a generic icon  in previous releases, displays the following icons with the Full Icon Support feature:

Table 45
Icons and Cadences

Call/Feature state	DN key icon	Cadence
Ringing		Flash
I-Hold		Wink
U-Hold		Flicker
I-Active		On
U-Active		On

Operating parameters

The following systems support the M3900 Full Icon Support feature:

- Succession 1000M Cabinet or Meridian 1 Option 11C Cabinet
- Succession 1000M Chassis or Meridian 1 Option 11C Chassis
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81C CP PII

The M3900 Full Icon Support feature applies to the following:

- Phase II and Phase III M3903 and M3904 sets
- Phase III M3905 sets
- Key Based Expansion Module (KBA) or Display Based Expansion Module (DBA) accessories

The Full Icon Support feature does not support IP telephones, M3901, or M3902 sets.

The M3900 Full Icon Support feature requires a minimum of Release 9 of the Key Based Expansion module (KBA).

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The M3900 Full Icon Support feature requires the following packages:

- M3900 Full Icon Support (ICON_PACKAGE) package 397
- Digital Sets (DSET) package 88

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

- LD 17 - Enable M3900 Full Icon Support.
- LD 22 - Enable M3900 Full Icon Support for printing.

LD 17 – Enable M3900 Full Icon Support.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	PARM	System Parameters
.....		
ICON	YES	Enable the M3900 Full Icon Support feature. NO = Disable the M3900 Full Icon Support feature.

LD 22 – Enable M3900 Full Icon Support for printing.

Prompt	Response	Description
REQ	PRT	Print.
TYPE	PARM	System Parameters
.....		
ICON	YES	Enable the M3900 Full Icon Support feature for printing.

Feature operation

No specific operating procedures are required to use this feature.

Observe Agent Security

Contents

This section contains information on the following topics:

Feature description

This feature enhances the Automatic Call Distribution Supervisor feature to provide the following security options:

- a supervisor can observe a call only when logged in (a login control option)
- a supervisor can observe calls of specified agents only (by association of a list containing specific agent position IDs)
- an unauthorized person cannot observe an agent call (password control option for the observe feature)

This feature offers three levels of security: login control, restricted Observe for supervisor, and password control of the Observe function.

Login control

The login control option is set at the ACD queue level. When this option is set to YES, supervisors serving the ACD queue can observe only when logged in. Administrators set the security option for login control for supervisors in LD 23 at the Observe Security Control (OBSC) prompt. When OBSC is set to YES for an ACD DN, all supervisor telephones serving that DN must log in to invoke Observe. If a supervisor is in a logged out or MSB state, and presses the Observe key when the OBSC is set to YES, the Observe function is denied and the Observe key lamp remains dark.

Restricted observe for supervisor

An SCL containing specific Position IDs is associated with the supervisor position's OBV key. The first 100 entries in the SCL associated with the OBV key can be observed. If this level of security is not chosen, the supervisor need not have any SCL associations with the OBV key. The SCL is configured with the position IDs of agents that a particular supervisor or group of supervisors can observe. This SCL is associated with the supervisor's OBV key.

Two Classes of Service (CLS) Observe using SCL Allowed (OUSA) and Observe using SCL Denied (OUSD) have been added to LD 11. The response OUSA is accepted only for supervisor sets. With CLS OUSA configured for the supervisor telephone, the administrator must enter an SCL number while configuring an OBV key.

A service error is output if the administrator attempts to

- configure SCL with CLS OUSD
- configure SCL with OUSA and an attempt is made to configure an OBV key without SCL

With the OUSA Class of Service, a supervisor can observe only specified agents within the same customer. With OUSD, a supervisor can observe any agent in the same customer.

A Speed Call Controller key can be configured on one supervisor's telephone so that the SCL containing position IDs can be modified. This aids local changes in the SCL; however, for security reasons, the telephone with this capability should be located in a secure area to avoid unauthorized access.

Password control of observe

The administrator configures the supervisor passwords along with supervisor login IDs in LD 23. A one-to-one mapping of IDs and passwords should exist. The password is matched with the login ID of the supervisor for validation.

A timer is used to measure the duration from the completion of observation (the timer starts once an observe is completed). If the timer has expired, the supervisor must enter his or her password the next time that he or she presses the observe key. If the timer has not expired, the supervisor does not have to enter the password. If a supervisor logs out, the timer expires immediately.

A new type of data block is introduced in LD 23 to enable storage of supervisor login IDs and their corresponding passwords in an Observe password table. This is one table per customer. Each table can contain a maximum of 240 entries. Login IDs can be 16 digits long and passwords can be 8 digits long.

The Observe Password Timer (OBPT) prompt follows the OBSC prompt in LD 23 during ACD DN configuration. This prompt enables the configuration of the Observe password timer, in minutes.

This feature introduces two new Classes of Service (CLS) in LD 11—Observe Password Allowed (OBPA) and Observe Password Disabled (OBPD). The OBPA Class of Service is accepted only if the telephone has been configured with the SPV Class of Service. A telephone configured with a OBPA Class of Service must enter a password to invoke Observe. However, if the supervisor is not logged in, Observe cannot be invoked.

Operating parameters

This feature applies to the following systems:

- Succession 1000

- Succession 1000M
- Succession 1000M Chassis
- Succession 1000M Cabinet
- Succession 1000M Half Group
- Succession 1000M Single Group
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81C CP PII

Feature interactions

Meridian Link

Meridian Link services do not support the Invoke Observe functionality with Password Control.

Feature packaging

The Observe Agent Security feature introduces Observe Agent Security package (394).

The Observe Agent Security feature requires the following packages:

- Automatic Call Distribution, Package B (ACDB) package 41
- Automatic Call Distribution, Package C (ACDC) package 42
- Automatic Call Distribution, Package A (ACDA) package 45
- Automatic Call Distribution, Package D (ACDD) package 50

Feature implementation

Task summary list

The following is a summary of tasks to configure this feature:

1 LD 23 – Configure the ACD Queue with Observe Agent Security.

2 LD 23 – Configure the Observe Password Table.

3 LD 11 – Configure the telephone for Observe Agent Security.

4 LD 11 – Configure the telephone with the OBV key and SCL number.

5 LD 23 – Configure an ACD DN with OBSC = YES and OB = xx.

LD 23 – Configure the ACD Queue with Observe Agent Security. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data.
TYPE	ACD	Automatic Call Distribution DN block
CUST	xx	Customer number, as defined in LD 15
....		
MAXP	x	Maximum number of agents for this Queue
....		
OBSC	(NO) YES	Observe Security Control. Enables login/logout control, where: NO = off YES = on
OBPT	xx	Observe Password Timer Supervisor Inactivity Timer, in minutes (2 - (5) - 99)
....		

LD 23 – Configure the ACD Queue with Observe Agent Security. (Part 2 of 2)

Prompt	Response	Description
OBTN		Observation Tone
	(NO) AGT ALL	No Observation Tone given. Audible Observation Tone to Agent only. Audible Observation Tone to all parties.
....		

LD 23 – Configure the Observe Password Table.

Prompt	Response	Description
REQ	NEW CHG OUT	Create, change, or remove a data block
TYPE	OBVP	Observe Password table
CUST	xx	Customer number, as defined in LD 15
ADPD	xx..xx yy..yy	Supervisor login ID followed by supervisor Observe password (separated by a space)

LD 11 – Configure the telephone for Observe Agent Security. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Create or change a data block
TYPE:	aaaa	Telephone type , where aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 2050, 3000, 390X, i2002, i2004
TN		Terminal Number
	l s c u c u	For Large Systems For Small Systems and Succession 1000 systems
....		

LD 11 – Configure the telephone for Observe Agent Security. (Part 2 of 2)

Prompt	Response	Description
CLS		Class of Service, where:
	SPV	Supervisor Class of Service
	OUSA (OUSD)	Observe Using SCL Allowed Observe Using SCL Denied
	OBPA (OBPD)	Observe Password Allowed Observe Password Denied
KEY	xx OBV	Observe ACD Agent key (must have CLS = OUSD)
	xx OBV yy..yy	Observe key with Speed Call List Number (must have CLS = OUSD). Where: yy..yy = SCL number
KEY	xx AGT zzzz	Agent with Position ID

LD 11 – Configure the telephone with the OBV key and SCL number. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add new, or change existing data.
TYPE:	aaaa	Telephone type, where: aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 2050, 3000, 390X, i2002, i2004
	TNB	Terminal Number Block
TN		Terminal Number
	l s c u c u	For Large Systems For Small Systems and Succession 1000 systems
....		

LD 11 – Configure the telephone with the OBV key and SCL number. (Part 2 of 2)

Prompt	Response	Description
CLS		Class of Service
	SPV	Supervisor Class of Service
	OUSA (OUSD)	Observe Using SCL Allowed Observe Using SCL Denied
	OBPA (OBPD)	Observe Password Allowed Observe Password Denied
....		
KEY	xx OBV	Observe ACD Agent key (must have CLS = OUSD)
	xx OBV yy..yy	Observe key with Speed Call List Number (must have CLS = OUSD). Where: yy..yy = SCL number
KEY	xx AGT zzzz	Agent key with Position ID

LD 23 – Configure an ACD DN with OBSC = YES and OB = xx. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Add new data, or change existing data.
TYPE	ACD	ACD DN block
CUST	xx	Customer number, as defined in LD 15
....	....	....
MAXP	xx	Maximum number of Agents for this queue
....	....	....

LD 23 – Configure an ACD DN with OBSC = YES and OB = xx. (Part 2 of 2)

Prompt	Response	Description
OBSC	(NO) YES	Observe Security Control. Enables login/logout control, where: NO = off YES = on
OBPT	xx	Observe Password Timer Supervisor Inactivity Timer, in minutes (2 - (5) - 99)
....	....	....
OBTN		Observation Tone
	(NO) AGT ALL	No Observation Tone given. Audible Observation Tone to Agent only. Audible Observation Tone to all parties.
....	.....	....

LD 18 – Configure a Speed Call List with Position IDs as DN entries. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG	Create or change a data block
TYPE	SCL	Speed Call data block
LSNO	zz	Speed Call List number
DNSZ	4-(16)-31	Maximum number of digits in a list entry
SIZE	1-100	Number of entries in the Speed Call list for Observe Agent Security should not exceed 100

LD 18 – Configure a Speed Call List with Position IDs as DN entries. (Part 2 of 2)

Prompt	Response	Description
WRT	(YES) NO	Write Data is correct and list can be updated
STOR	xxx yy...yy	Store where: xxx = list entry number (0-90, 00-99, 000-999) yy = digits stored against entry (must be equal to or less than DNSZ)

Feature operation

To invoke Observe with password control enabled, perform the following steps:

1. Press the Observe key.

   The “Enter Authorization Code” display is shown on the telephone.

2. Enter the Observe password followed by “#”. The password is not displayed on the telephone; rather each digit in the password is represented with a “-”.

3. If the password is valid, the telephone displays “Observe Agent, Enter ID”. Enter the position ID of the agent and proceed.

4. If the password is invalid, the telephone displays “Release and Try Again” and the Overflow tone sounds.

Personal Call Assistant

Contents

This section contains information on the following topics:

Feature description

Personal Call Assistant (PCA) is a virtual Terminal Number (TN) that is placed in a Multiple Address Directory Number group. PCA can extend and ring calls to any dialable destination, thus enabling the creation of MADN groups across networks. If two calls arrive at the same time, the first caller is processed as outlined above, and the second caller receives busy treatment according to the current functionality of MADN.

Note: An attendant console cannot be the target of PCA.

PCA enables the simultaneous ringing of clients with different Directory Numbers (DNs) that are dispersed across a network. When simultaneous ringing is enabled, the Calling Line Identification (CLID) of the originating set is presented to the called set, provided CLID is available to PCA.

To support simultaneous ringing, MADN functionality has been enhanced as follows:

- MADN groups can exist across networks; end users can be located at any dialable location and have a different Directory Number (DN) than the MADN.
- The system can extend MADNs to local numbers if the switch is configured to forward to external numbers.
- Signaling is extended to the target node from the system to enable users on the system to access multi-media applications.

Every call associated with a target node user consists of an incoming call and an outgoing call that are joined after the call is answered. CDR records, pegs, and logs reflect these call dynamics.

If the original call is abandoned, the desktop stops ringing and PCA releases the extended call.

If a call is answered coincidentally on the target node desktop, then call treatment is queue-dependant as the messages are processed in the order in which they are received. If the trunk call is processed last, the call is released and the trunk is dropped. If the desktop call is processed last, dialtone is presented to the desktop.

A call that is not answered continues to ring until it either receives redirection treatment or is abandoned by the originator. The redirection treatment can be node-system initiated or can be the called party's arrangement on a residential or cell phone.

Call presentation to the desktop can be impacted by the Busy and Redirection treatment specified in the target (for example, in the cell phone).

PCA functionality enables multi-media capabilities on Succession 1000M, Succession 1000, and Meridian 1 systems that were previously restricted to the Succession Multimedia Xchange (MX).

The PCA feature supports the following telephones and terminals:

- analog (500/2500-type) telephones

- digital telephones
- IP terminals and clients (i2002, i2004, i2050 [soft client])

PCA can extend the call across all trunk types; however, CLID is supported only on ISDN PRI, PRI2, and H.323 trunks.

Operating parameters

The Personal Call Assistant feature applies to the following systems with Succession 3.0 and later software:

- Succession 1000
- Succession 1000M Half Group
- Succession 1000M Chassis
- Succession 1000M Single Group
- Succession 1000M Multi Group
- Succession 1000M Cabinet
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81C CP PII
- Meridian 1 Option 11C Cabinet
- Meridian 1 Option 11C Chassis

When multiple PCAs are configured with the same MADN, you cannot update individual PCAs using the FFC.

Network wide FFC operation is not supported; however, FFC does work with DISA.

FFCs cannot be invoked from the attendant console.

The HOT P DN length can be only 21 characters due to the space restrictions in the Call Register.

> ***Note:*** If the HOT P DN is updated using LD 11, the DN length can be a maximum of 32 characters.

Feature interactions

The PCA feature has the same feature interactions as the MADN feature, which are as follows.

Automatic Redial

An ARDL call from a Single Call Ringing (SCR) or Single Call Non Ringing (SCN) is redialed only when all sets that have the same DN are free.
An ARDL call from a Multiple Call Ringing (MCR) or Multiple Call NonRinging (MCN) is redialed only when the originating key is free.

Automatic Wake Up

All Multiple Appearance DNs are rung, including both primary and secondary DNs. Programming the wake up request using the Wake Up key applies only to telephones with the primary DN on key 0, and the Wake Up indicator operates as described only on the telephone that is currently programming the wake up request.

In addition, if two or more Multiple Appearance Primary DN telephones program a wake up request at the same time, the last telephone to finish overrides. All telephones with the same primary DN get the same request time of the last telephone to program a request. If the last telephone cancels the request, all requests are canceled. When the wake up programming sequence is finished, all Wake Up indicators on Multiple Appearance Prime DNs are updated unless a telephone is in the middle of Wake Up programming. If the AWU Recall option is chosen, the recall is presented to any idle attendant console in the same Console Presentation Group (CPG) equipped with the AWU key.

Note: An attendant console cannot be the target of PCA.

Automatic Wake up FFC Delimiter

For Multiple Appearance Directory Numbers, wake up information is stored, deleted, and queried from a DN's first primary appearance Terminal Number.

Call Detail Recording

CDR for Personal Call Assistant is handled in the following manner:

- If the call is answered on the desktop, there is no change from existing CDR operation.
- If the call is answered on a cell phone supported by the Succession MX, the following CDR records are created:
  - Succession 1000M, Succession 1000, and Meridian 1: PCA to DOD (Succession MX) and DID to DOD (after the call is joined to the Succession MX)
  - Succession MX: DID (from Succession 1000M, Succession 1000, and Meridian 1) to DOD (cell phone)

Call Detail Recording on Redirected Incoming Calls

If the DN of the set forwarding the call is a Multiple Appearance DN, the Terminal Number of the set is printed out in the AUX ID field (that is, line two of the Call Detail Recording record).

Call Forward by Call Type
Call Forward No Answer, Second Level

Call redirection parameters such as Call Forward No Answer are derived from the TN data block of the prime appearance of the called MADN. If there is more than one prime appearance, the parameters are selected from the last TN in the DN block. If more than one prime appearance of the MADN exists, the following information must be considered prior to configuring call redirection parameters for MADNs.

The DN Block organizes MADN information in numerical TN order. The TN with the highest numerical value (000-0-06-03) is placed at the beginning of the list. The list then continues in descending order with the lowest numerical TN (000-0-03-01) at the end of the list. Service change activity affects the organization of the DN list as described in the following paragraphs.

- If a telephone undergoes Service Change, its TN is moved to the beginning of the DN list, irrespective of the numerical value. This telephone remains at the beginning of the list until another service change or a SYSLOAD.

- If a DN appears on analog (500/2500-type) telephones, and digital telephones, the analog (500/2500-type) telephones are listed in numerical TN order at the top of the list. Digital telephones are listed in numerical TN order at the bottom of the list. A Service Change to an analog (500/2500-type) telephone moves its TN to the beginning of the list. A Service Change to a digital telephone moves its TN to the end of the list.
- A SYSLOAD restructures the list back to numerical TN order, with analog (500/2500-type) telephones at the top and digital telephones at the bottom. Call redirection parameters continue to be derived as described in the preceding paragraphs.

Call Forward, Remote (Attendant and Network Wide)

The Call Forward, Remote (RCFW) feature applies only to the primary appearances of Multiple Appearance DNs, and it is recommended that only one appearance of a Multiple Appearance DN be configured as the prime DN. For the case of multiple stations with the same prime DN and SCPW, the RCFW operation applies to the station that has the Multiple Appearance Redirection Prime (MARP) assigned to it.

If none of the stations having the DN and SCPW assigned are configured as the MARP TN for that DN, the RCFA and RCFD applies to all stations matching the DN and SCPW. The attendant-based RCFW feature applies remote call forward operation only to the prime DN with MARP status. If the DN is not the prime DN or does not have MARP status, the user receives overflow tone.

Call Waiting Redirection

The Call Waiting Redirection feature applies to unanswered Call Waiting calls that apply to single appearance DNs and primary appearance DNs of MADNs.

Calling Party Name Display Denied

For a ringing call to a Multiple Appearance DN, the name on the calling set display can be suppressed by configuring any of the Terminal Numbers with NAMD Class of Service. The digit display on the calling set cannot be suppressed — the called digits are displayed even though the Class of Service on any of the Terminal Numbers is DIGD. The called set display is subject to the Class of Service of the calling party. For an established call to a Multiple Appearance DN, the calling set display is subject to the Class of Service configured for the answering set. The answering set display only is subject to the Class of Service of the calling party – the displays of the other sets in the Multiple-appearance group are blank.

China – Attendant Monitor

If Attendant Monitor is attempted on a Multiple Appearance DN, the Multiple Appearance Redirection Prime (MARP) TN becomes the desired party.

Controlled Class of Service

Controlled Class of Service (CCOS) restriction levels are activated or canceled on controlled telephones through their Prime Directory Number (PDN). When the PDN of a digital telephone is made CCOS active, all DNs on that telephone are also restricted. If the DN is a PDN on other telephones, those telephones are also restricted (if they have CCSA Class of Service).

Controlled Class of Service, Enhanced

All Controlled Class of Service (CCOS) restriction levels are activated and canceled from the Prime Directory Number (PDN) for CCOS controlling telephones. The PDN for an SL-1 telephone is made CCOS active, and all DNs for that telephone are restricted as well. If that DN is a PDN on other telephones, they are also restricted (if they have CCSA Class of Service).

Digital Private Signaling System #1 (DPNSS1) Executive Intrusion

If the attendant tries to extend a call to a DN that appears on more than one set, this DN can either be:

- Multiple-Call Arrangement with Ringing (MCR). When a call terminates on this DN, all idle stations on which the DN appears are rung. The call is established only with the station which has answered first. All others are idle.
- Multiple-Call Arrangement with No Ringing (MCN). The only difference between MCN and MCR is that the called stations are not rung (only their DN keys flash).
- Single-Call Arrangement with Ringing (SCR). When a call terminates on this DN, all idle stations on which the DN appears are rung. The call is established only with the station which has answered first. All others are busy.
- Single-Call Arrangement with No Ringing (SCN). The only difference between SCN and SCR is that the called stations are not rung (only their DN keys flash).

Digital Trunk Interface (DTI) – Commonwealth of Independent States (CIS)

Since the ANI category is defined on a per-set basis, two stations with the same Multiple Appearance Directory Number (MADN) can be assigned different ANI categories.

Directory Number Expansion

The DN can have up to seven digits if the Directory Number Expansion package is equipped. If Loop Restriction Removal is allowed, telephones with MADNs can be moved across loops using Automatic Set Relocation (LD 25), the digital telephones data block (LD 11), the analog (500/2500-type) telephone data block (LD 10), or Attendant Administration.

Display Calling Party Denied

When a Multiple Appearance DN is ringing, the display of the calling telephone does not show the caller's name if at least one of the TNs has Named Denied (NAMD) Class of Service. The dialed DN displays even if one TN has a DN Denied (DDGD) Class of Service. The display of the called telephone shows the DN and the caller's name according to the Class of Service of the calling DN. When a Multiple Appearance DN is answered, the display of the calling telephone shows the DN and caller's name and DN according to the Class of Service of the answering TN. The display of the answering telephone remains the same, while the displays of the other telephones are blanked.

Electronic Lock Network Wide/Electronic Lock on Private Lines

The same locked or unlocked state applies to all Terminal Numbers with the same primary DN and the same SCPW. Terminal Numbers with the same DN, but not having the same SCPW, cannot be locked or unlocked.

Group Call

The maximum number of DNs that can be added as members of a Group Call is 20. Each Multiple Appearance, MCR/MCN DN reduces the number of telephone sets that can be added to a Group Call. For example, if two telephones have the same MCR appearance of a DN, the number of telephones in the Group Call becomes 19. That is, each appearance of a DN counts as one member, up to a maximum of 20, of the Group Call.

> ***Note:*** Multiple Appearance, SCR/SCN DNs count as one member of a Group Call, irrespective of its number of DN appearances.

Group Hunt

While Multiple Appearance DNs (MADN) single call arrangements are treated the same as Single Appearance DNs (SADN), MADN multiple call arrangements must be avoided in a group hunt list. With MADN multiple call arrangement, the idle or busy status of the MADN is determined by the Terminal Number (TN) data block of the prime appearance of the called DN. If there is more than one prime appearance of the called DN, the idle or busy status is then selected from the last TN in the DN block for the MADN (DNB prompt in LD 22). This means that there can be idle appearances of the MADN, while the hunt cycle regards them as busy and attempts to terminate on the next idle member of the group hunt list.

If an MADN multiple call arrangement must be used, a supervisor set must be assigned to the hunt group. This supervisor set must be given the only prime appearance of the MADN. Any other appearance must have the MADN programmed as a secondary DN (any DN key other than 0). In this way, the supervisor set controls the status of the MADN and thus the group hunt treatment. If the supervisor set is busy, the hunt does not terminate on the MADN.

Hunting

Hunting can be controlled by the MADN Redirection Prime (MARP) Terminal Number (TN). If the MARP system option is disabled, Hunting proceeds as if MARP did not exist. If all the telephones in the Multiple Appearance Directory Number (MADN) group are digital telephones, ringing telephones are placed at the top of the DN list, and non-ringing telephones are placed at the bottom.

If a Multiple Appearance Directory Number appears in a group with several telephone types, the telephone type affects the position of the TN in the list. The analog (500/250-type) telephones are listed at the top, and digital telephones are listed in numerical TN order at the bottom. A service change to an analog (500/2500-type) telephone moves its TN to the top of the list. A service change to a digital telephone moves it to the bottom of the list.

Call redirection follows the TN order from top to bottom. The MARP TN is always checked to determine if and how the call is to be redirected by Hunting, regardless of where the MARP TN resides in the TN list of the DN block. No searching of the TN list of the DN block is needed.

Hunting follows the hunt chain based on the originally dialed DN. The actual functioning and requirements for Hunting are not changed by the MARP feature. The basic change introduced by the MARP feature is to always have a designated TN, the MARP TN, as the TN supplying the call redirection parameters. If the MARP TN does not have Hunting control enabled, no Hunting is attempted. Other features for redirecting calls to busy DNs may be attempted based on the MARP TN.

A Short Hunting sequence begins when the MARP TN of a busy DN can perform Short Hunting. When a Short Hunt begins, it completes on that telephone before going to the Hunt DN. The precedence of Short Hunting over normal Hunting is maintained. Once a Short Hunting sequence is started on a digital TN, all the DNs in the Short Hunt sequence on that TN are attempted before redirecting the call to the TN's Hunt DN. Thus, a Hunt Chain connects Short Hunting sequences through Hunt DNs only.

Last Number Redial

A last number dialed on a Directory Number (DN) with multiple appearances is stored only against the telephone from which the number was originally dialed.

Loop Restriction

If Loop Restriction removal is not enabled, telephones with MADNs can be moved by using the Automatic Set Relocation feature (LD 25) or the Attendant Administration feature.

Meridian 911

The DN keys for multiple appearance sets can be defined as an SCR (single call ringing) key or as an MCR (multiple call ringing) key. For those DNs (keys on MADN sets) that are SCR, only one call can be answered at a time. That is, once a call taker answers a call, future calls to that DN receive busy tone until the call taker on that DN disconnects. For DNs that are MCR, calls are given busy tone once every call taker is busy answering a call. If one call taker is answering a call and there are other call takers available, a new call to that DN causes the sets of the available call takers to ring. Any available call taker can then answer the new call.

Message Registration

For Multiple Appearance Directory Number (MADN), the system selects the appropriate meter for the DN as follows. The MADN accesses the meter of the most recently configured telephone having a Prime DN (PDN) appearance and Message Registration Allowed (MRA) Class of Service. If no Terminal Number (TN) in the DN block has MRA Class of Service, the customer meter is charged. For the Message Registration Key (MRK), the system provides overflow and sets the MRK lamp to flash. For the Background Terminal (BGD), it prints a NO DATA FOUND message.

Privacy

If a Multiple Appearance, Single Call Arrangement (SCR) or Single Call Arrangement without Ringing (SCN) DN is shared by digital telephones only, Privacy is in effect. No one can enter a call unless the call is first placed on Hold, or unless Privacy Release is activated to enable another appearance to enter the call. If this configuration is shared between these telephones and single-line telephones, Privacy is not in effect for any appearance of the DN. Anyone sharing the DN can enter the call at any time.

Privacy Override

Since the Privacy feature is not active in this mode, telephones with a Privacy Override Denied Class of Service can bridge into an active call.

Privacy Release

Privacy Release has no effect on Multiple Appearance, Multiple Call Arrangement with Ringing (MCR), or Multiple Call Arrangement without Ringing (MCN) calls.

Remote Call Forward

With a Multiple Appearance Directory Number (MADN) and both sets having a Station Control Password (SCPW), Remote Call Forward does not operate as intended. That is, if Call Forward has been activated using the Remote Call Forward feature, Call Forward remains activated when an attempt to deactivate it is made from the set on which it is active.

Three Wire Analog Trunk – Commonwealth of Independent States (CIS)

Since the ANI category is defined on a per-set basis for Three Wire Analog Trunks, two stations with the same multiple Appearance DN can be assigned different ANI categories.

Voice Call

If a Voice Call DN is added to a second telephone, the DN becomes a Multiple Appearance DN (MADN). Voice Call does not support MADN. In addition to MADN interactions, PCA has the following feature interactions.

Feature packaging

This feature introduces the following package:

- Personal Call Assistant (PCA) package 398

Feature implementation

Task summary list

The following is a summary of tasks in this section:

- LD 15 - Enable PCA at the customer level.
- LD 57 - Configure FFCs for PCA control.
- LD 11 - Configure a new PCA.
- LD 97 - Add Virtual loops.

LD 15 – Enable PCA at the customer level. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	FTR	Features and options
CUST	xx	Customer number, as defined in LD 15

LD 15 – Enable PCA at the customer level. (Part 2 of 2)

Prompt	Response	Description
...	...	...
VO_ALO	(NO) YES	Enable (disable) Virtual Office Automatic Logout.
PCA	(OFF) ON	Enable (disable) Personal Call Assistant Configuration of the PCA is preserved and enabled regardless of whether or not the feature is enabled.
TPDN	yyy.y	Target PCA DN Where: yyy.y is the primary DN TPDN is prompted only if PCA is set to ON. If there is no DN configured against the HOT P key in LD 11, this value is used to extend the call using the PCA feature. Enter X to remove. However, if there is at least one PCA with no target DN configured in LD 11, then this operation does not succeed.

LD 57 – Configure FFCs for PCA control. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW CHG PRT	Create, change, or print a data record.
TYPE	FFC	Flexible Feature Code
CODE	PCAA	This is the code to activate PCA or change the HOT P DN.
PCAA	xxxx	Code number
CODE	PCAD	Code to deactivate PCA
PCAD	yyyy	Code number

LD 57 – Configure FFCs for PCA control. (Part 2 of 2)

Prompt	Response	Description
CODE	PCAV	Code to verify the status of PCA
PCAV	ZZZZ	Code number

LD 11 – Configure a new PCA.

Prompt	Response	Description
REQ:	NEW CHG	Add or change a PCA.
TYPE:	PCA	Personal Call Assistant
TN		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
CUST	xx	Customer number, as defined in LD 15
CLS	AHA	Automatic Hold Allowed (AHA). AHA is configured by default when the response to the TYPE prompt is PCA.
KEY	0 aaa yyy.y	Primary PCA DN Where aaa = MCN, MCR, SCN, or SCR and yyy.y = the primary DN Note: The PCA should never be configured as a MARP in a MADN group.
	1 HOT P x vvv.v	Target PCA DN where x = length of target DN vvv.v = the target DN Note: HOT P key is the default key. This key must be configured by the user.

LD 97 – Add virtual superloops.

Prompt	Response	Description
REQ	CHG	Add virtual superloops.
TYPE	SUPL	Superloop parameters
SUPL	vxxx	Add virtual superloops.

Feature operation

The PCA feature operates as outlined below.

Activating and deactivating PCA at the user level

Succession 3.0 introduces three Flexible Feature Codes (FFC) that enable the user to activate, deactivate, or change the target DN on PCA.

To activate or deactivate PCA, perform the following steps

1. Press the DN of any terminal connected to the PBX on which PCA is configured.
2. Enter one of the following FFC codes:
   - **a.** To activate or change PCA, enter PCAA FFC.
   - **b.** To deactivate PCA, enter PCAD FFC.
   - **c.** To verify the current status of PCA, enter PCAV FFC.
3. Enter the prime DN of the desktop.
4. When prompted for a password, enter the Station Control Password (SCPW) of the desktop set or that of PCA (if configured). If no desktop set is configured, the SCPW must be configured on PCA.
5. Enter #, the end-of-dialing digit.
6. Listen for a confirmation tone after entering the main extension number. This tone indicates that the password and extension match and the procedure was successful. If you receive a fast busy tone, the procedure failed and you must hang up and try again.

7 If you are done, enter # to complete the PCAA FFC. Optionally, to update the HOT P DN and activate PCA, enter a new target DN (HOT P DN) followed by #. Listen for a confirmation tone after entering the main extension number. This tone indicates that the password and extension match and the procedure was successful. If you receive a fast busy tone, the procedure failed and you must hang up and try again.

If any of the following events occur, the user hears the overflow tone:

- The SCPL prompt in LD 15 is set to 0 and there is no SCPW configured for the desktop set.
- The user enters the PCA FFCs and the system is not equipped with the PCA package.
- The user enters the PCA FFCs and the LD 15 customer data does not have PCA set to ON.
- The user enters the PCA FFCs for a set that has no PCA in the MADN group.
- The user enters the TPDN FFC for a set that has no PCA in the MADN group.
- The user enters an invalid DN.
- The user enters a DN other than BCS/Ether set DN.
- The user enters "*" or "#" as part of the password.
- The password does not match any SCPWs in the MADN group.

Setting up PCA

The following steps are used in the internal setup:

1 Associate PCA and desktop by sharing a common DN. Configure PCA with the MADN as the primary DN. To change the behavior of the MADN, use multiple and single call ringing. A virtual TN is required for each PCA.

2 Configure Key 0 with the same type of key 0 and DN as the desktop set.

3 Configure Key 1 as a new PCA key (equivalent to a Hot Line Key). If the DN is not configured, the system generates a blending service DN based on the customer setting in LD 15.

Note: Configuration can be simplified through the use of set models.

Trunk Route Optimization — Call Modification

Contents

This section contains information on the following topics:

Feature description

Succession 3.0 introduces Trunk Route Optimization – Call Modification (TRO-CM). This feature optimizes trunk paths for calls affected by call modification and improves voice quality by removing redundant trunks. After the transferred-to party answers and the call transfer completes, TRO-CM replaces an active connection in a Meridian Customer Defined Network (MCDN) with an optimized new connection. This feature optimizes IP Peer Virtual trunks, IP trunks, VNS trunks, ISL trunks, and BRI and PRI B-channels.

The TRO Call Modification feature uses network resources across all types of MCDN networks.

Trunk Route Optimization – Call Modification (TRO-CM), Trunk Optimization – Before Answer (TRO-BA), and Trunk Anti-Tromboning (TAT) are Meridian Customer Defined Network (MCDN) features designed to work together to optimize trunk connections for different call scenarios. These features are applicable to the following:

- IP Peer Virtual trunks
- IP trunks
- VNS trunks
- ISL trunks
- BRI and PRI channels

For maximum benefits, configure the three features on all the nodes in the MCDN.

TRO-BA and TRO-CM are configured by setting TRO = YES in the Route Data Block. TAT is configured by setting RCAP = TAT in the D-Channel data block.

Without the correct configuration and operation of the TRO and TAT features, automatic call redirections (for example, Call Forward-Busy or Call Forward-No Answer) and user-initiated call modifications (for example, Call Transfer and Conference calls) in an MCDN cannot optimize the route between the connected callers. Trunk Route Optimization features in an MCDN can be used in such scenarios to optimize the routes.

Trunk Optimization – Before Answer (TRO-BA)

The TRO-BA feature works for redirected calls (for example, Call Forward All Calls, Call Forward Busy, and Call Forward No Answer or Hunting).

TRO-BA does not optimize trunks for calls that have undergone any call modification (for example, Call Transfer or Conference).

For more information on this feature, refer to the Trunk Optimization – Before Answer (TRO-BA) section.

Trunk Anti-Tromboning (TAT)

TAT optimizes tromboned trunks for calls that are redirected or modified after answer. TAT optimizes tromboned trunks under the following conditions:

- The trunks are associated with the same primary channel.
- Both trunks belong to the same customer.

Note: TAT and NAS operations are improved for IP Peer Virtual Trunk and IP Trunk networks.

For more information on this feature, refer to the Trunk Anti-Tromboning (TAT) section.

Trunk Route Optimization – Call Modification (TRO-CM)

TRO-CM optimizes trunks after call modification in scenarios that are not handled by TRO-BA and TAT. This feature optimizes the path between the two connected agents for calls that are modified due to blind/supervised transfer and when conference calls revert to two-party calls.

TRO and TAT features make the most efficient use of network resources across MCDNs and they provide better voice quality for IP trunks.

Trunk Optimization – Call Modification, Trunk Anti-Tromboning, and Trunk Optimization – Before Answer provide the following benefits:

- Optimizes trunk resources to reduce operating costs for customers in TDM and Hybrid Networks (IP Trunk and IP Peer Networks).
- Reduces the number of physical TDM MCDN trunk carrier facilities, IP Trunk resources and Virtual Trunks and Voice Gateway channels that must be provisioned to achieve a given blocking Grade of Service.
- Eliminates most of the voice quality degradation associated with multiple tandem voice paths resulting from network call transfers in Hybrid networks.

- Eliminates redundant tandem Virtual Trunks (VTRK) resources and Voice Gateway resources in an IP Peer network.
- Minimizes service interruptions by eliminating unnecessary points of failure in the tandem nodes of established calls.

TRO-CM trunk route optimization

TRO-CM optimizes trunks for the following scenarios:

- calls blind-transferred from a station
- calls transferred after consultation (supervised transfer)
- calls extended by the attendant console
- calls reverting to a point-to-point call when one party disconnects from a three-party conference
- calls answered by voicemail and subsequently blind-transferred by Dial 0, Revert DN, or Automated Attendant service
- calls entering or leaving the private network on PSTN trunks; private network trunks are optimized after any call modification

Events that trigger TRO-CM

The system triggers TRO-CM in the following scenarios:

- transfer trigger
  The system invokes TRO-CM for calls transferred from a station across a network. The transfer can be blind or supervised.
  - manual transfer
    The user can manually initiate call transfer from a set. For example: Station A (node 1) calls Station B (node 2). Station B answers the call and initiates call transfer to Station C on a different node from the transfer key on the user's set.

— automated transfer
The system can also initiate call transfer using the Auto-attendant, Thru-dial or Call Sender features of Call Pilot/Meridian Mail. For example: Station A (node 1) calls Station B (node 2). Station B activates Call Forward to voicemail. Station A is connected to CallPilot/Meridian Mail. Station A activates the Dial 0 Revert DN feature. This invokes blind transfer to Station C at node 3. CallPilot/Meridian Mail completes the transfer.

- attendant extending call
The system triggers TRO-CM when the attendant at the tandem node extends the call to a station on another node and drops out of the call. This occurs only when the station answers the call. The attendant is able to drop out of the call up to the time the station answers the call.
- conference call on disconnection
The system triggers TRO-CM when a conference call reverts to a two-party call.

Notations used in graphics

Figures 57 and 58 show the notations used for the graphics in this chapter.

Figure 57
Notations used for examples

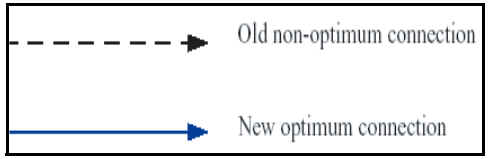
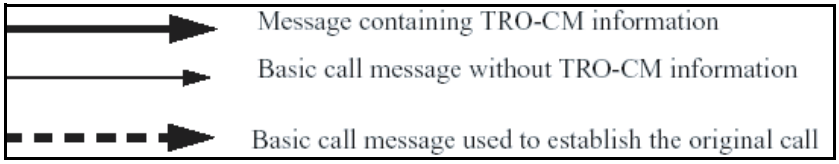
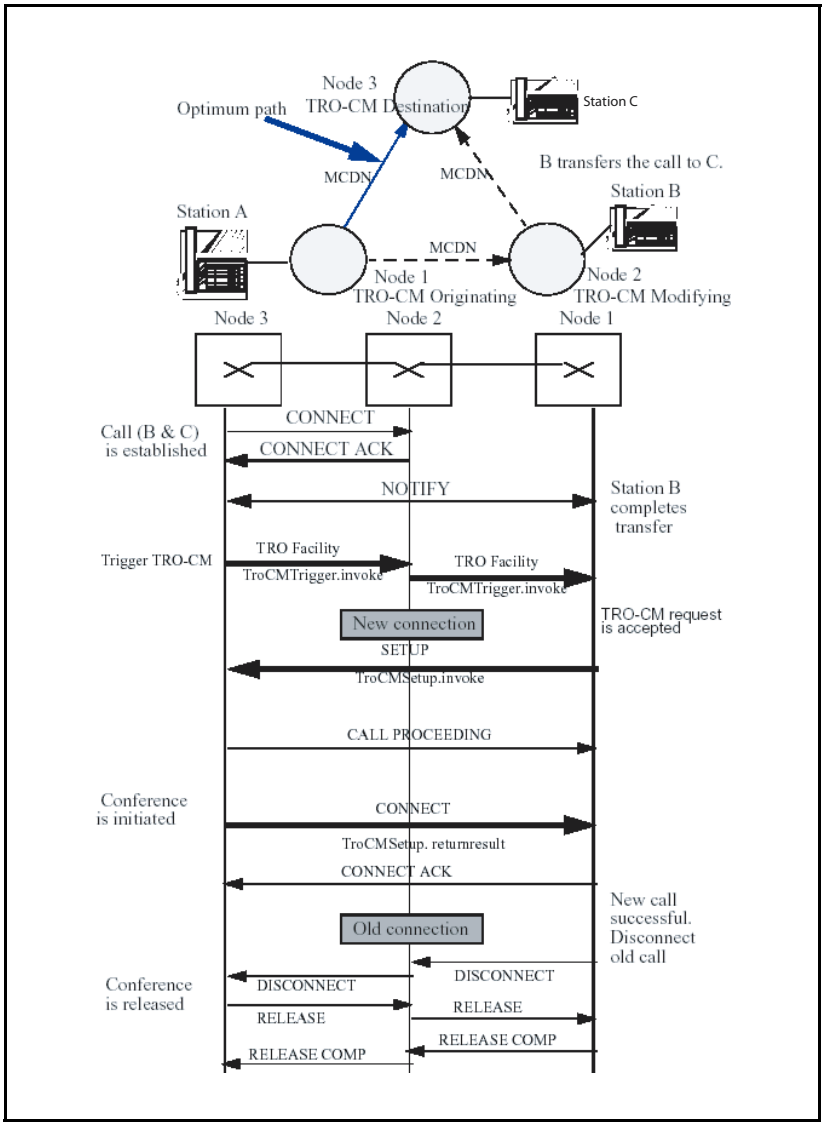


Figure 58
Notations used for message sequence examples



TRO-CM basic operation

Figure 59
TRO-CM basic operation



In Figure 59 Station A calls Station B. Station B answers the call and transfers to Station C. Station C answers the call and Station B completes the transfer. When Station B completes the transfer, the system sends NOTIFY messages to node 1 and node 3, informing them of the network call transfer. When the TRO-CM destination node receives this NOTIFY message, the system invokes TRO-CM operations.

In the case of a blind transfer, the system invokes TRO-CM operations only when Station C answers the call.

The TRO-CM destination node sends a message proposing optimization to the TRO-CM initiation node. This message is referred to as TroCMTrigger invoke FACILITY.

When the TRO-CM originating node receives the TroCMTrigger invoke FACILITY, it attempts to set up a new call to the TRO-CM destination node. This SETUP message includes a facility (TroCMSetup) identifying it as a TRO-CM call set-up.

If the new TRO-CM call setup fails, the system does not optimize the call and the TRO-CM destination node is notified that TRO-CM failed. The TRO-CM destination node tries to send TroCMTrigger invoke FACILITY again or aborts TRO-CM depending on the error cause.

On reception of TroCMSetup invoke SETUP, the TRO-CM destination node forms a conference between the originating party, the original path (still carrying speech), and the new (silent) path. It then sends a CONNECT message with a TroCMSetup return result.

On reception of this CONNECT message, the TRO-CM originating node connects the new path in place of the original one and disconnects the old path.

On receipt of the DISCONNECT of the old channel, the TRO-CM destination node breaks up the conference, connects the originating party to the new path, and clears the original path.

During TRO-CM operations, any key pressed on the terminating set aborts TRO-CM. For example, when Station C answers the call, TroCMTrigger FACILITY is sent. Any key pressed on Station C causes TRO-CM operations to abort.

The same applies to the originating set. Any key pressed on Station A causes TRO-CM operations to abort.

TRO-CM originating node rejects TRO-CM facility message

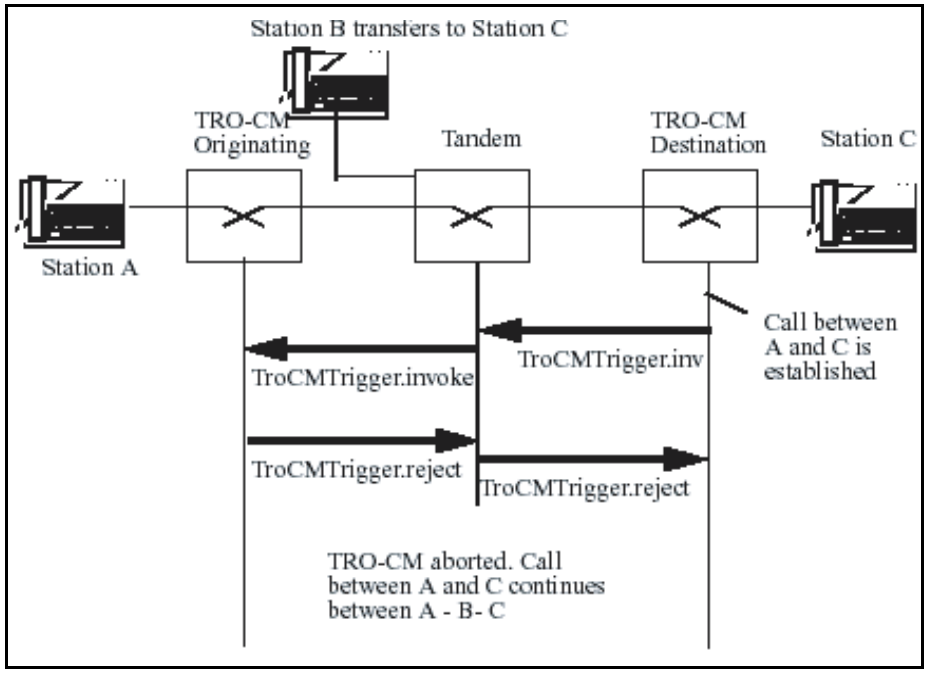
When a TRO-CM trigger request fails, the system:

- cancels all optimization processes; in the case of the TRO-CM Not Available Error, the call continues over the non-optimum path
- retransmits TroCMTrigger facility in the case of temporary failures

In Figure 60 on page 391, when Station A calls Station B, Station B answers and transfers the call to Station C. Station C answers the call. Once Station C answers the call, node 3 sends a TroCmTrigger Invoke message to node 1. If node 1 is unable to accept the invoke, it directly rejects the invoke message.

Once node 3 receives the reject message, the system aborts all TRO-CM processes.

Figure 60
TRO-CM originating node rejects TROCM Trigger



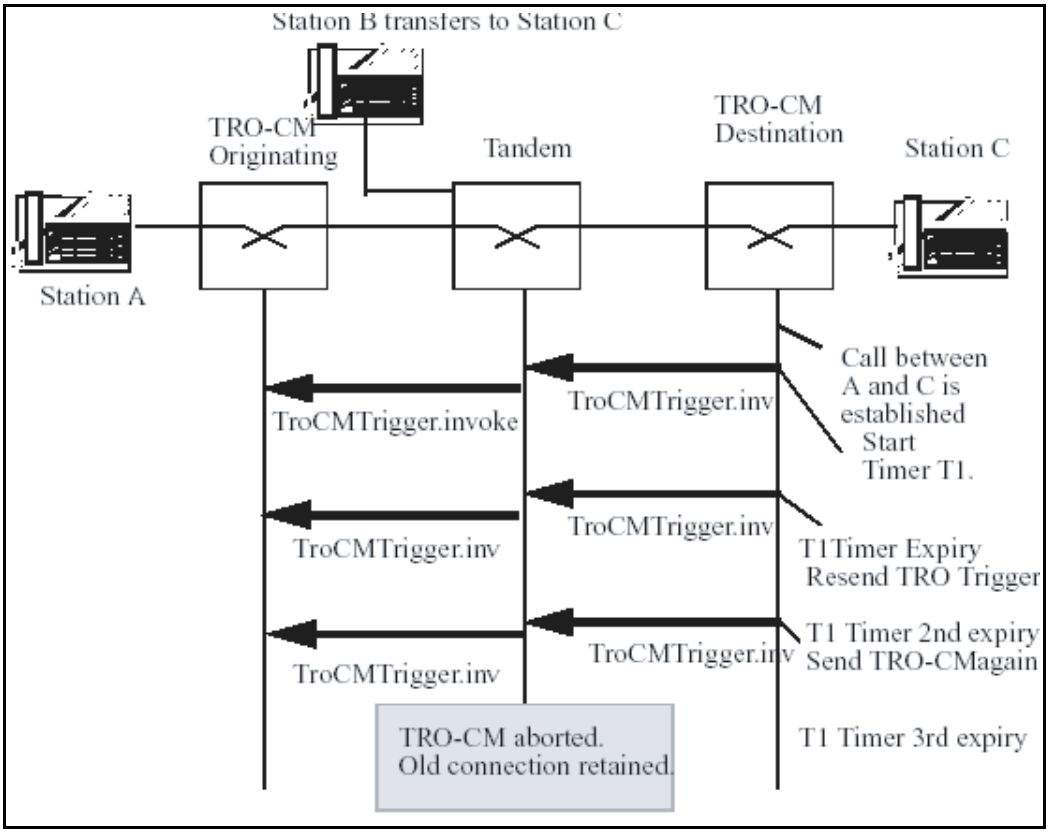
TRO-CM originating node makes no response to TRO-CM facility trigger

When the TRO-CM destination node sends a TRO-CM trigger, it starts a timer (T1). When the TRO-CM destination node does not receive a response from the TRO-CM originating node to the TroCMTrigger Invoke message, the TRO-CM destination node waits until the timer expires.

On expiry of timer (T1), the TRO-CM destination node resends the TroCMTrigger. It waits for 30 seconds and resends TRO-CM trigger the second time. When the TRO-CM destination does not receive a response to this message, the system aborts all TRO-CM processes.

See Figure 61 on page 392 for the message sequence in this scenario.

Figure 61
No response after TRO-CM proposed



Operating parameters

This feature depends on the TRO-BA feature. It requires all the packages and the configuration of TRO-BA.

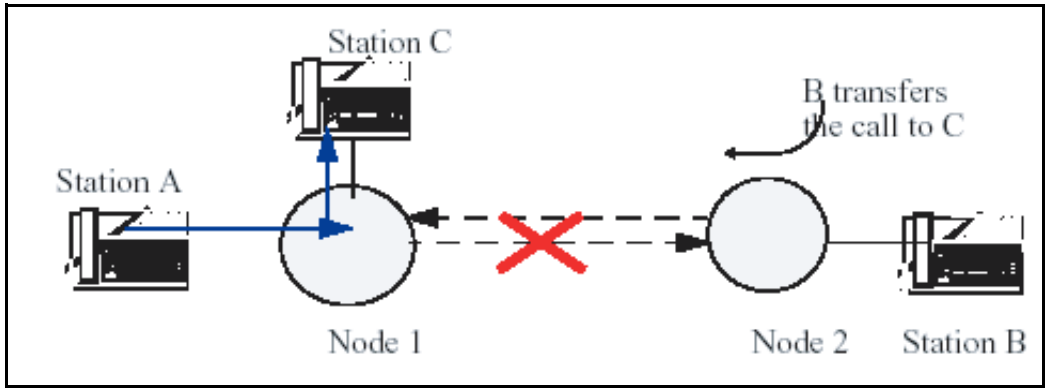
Only MCDN connections support TRO-CM.

Anti Tromboning

TRO-CM does not release when an outgoing trunk call comes back to the same node either on the same D-Channel or on two different D-channels, or two different customers are on the same D-channel.

However, if the same D-channel holds the outgoing call and the incoming transferred call, then Trunk Anti Tromboning (TAT) triggers and releases the trunks. See Figure 62.

Figure 62
Tromboning



Attendant calls

If the originator of the call is an Attendant on the TRO-CM originating node, then the system defers the TRO-CM request while the attendant is active on the call. The system accepts TRO-CM when the attendant leaves the call.

The TRO-CM destination node does not attempt TRO-CM for attendant calls, because attendant calls are usually short term calls or extended to another party.

Call originator transfers

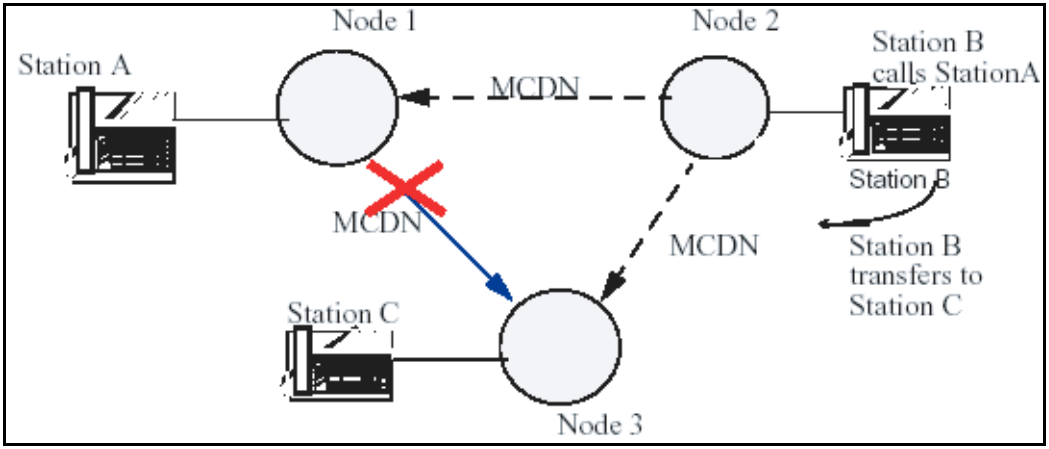
TRO-CM does not optimize the call when the call originator transfers the call to another node.

For example, in Figure 63, Station B calls Station A. Station A answers the call. Station B transfers the call to Station C. TRO-CM fails.

TRO-CM fails when the conference originator drops out of the conference.

In Figure 63, Station B calls Station A. Station A answers the call. Station B conferences Station C and Station B drops out of the conference. TRO-CM fails.

Figure 63
Originating party transfers the call

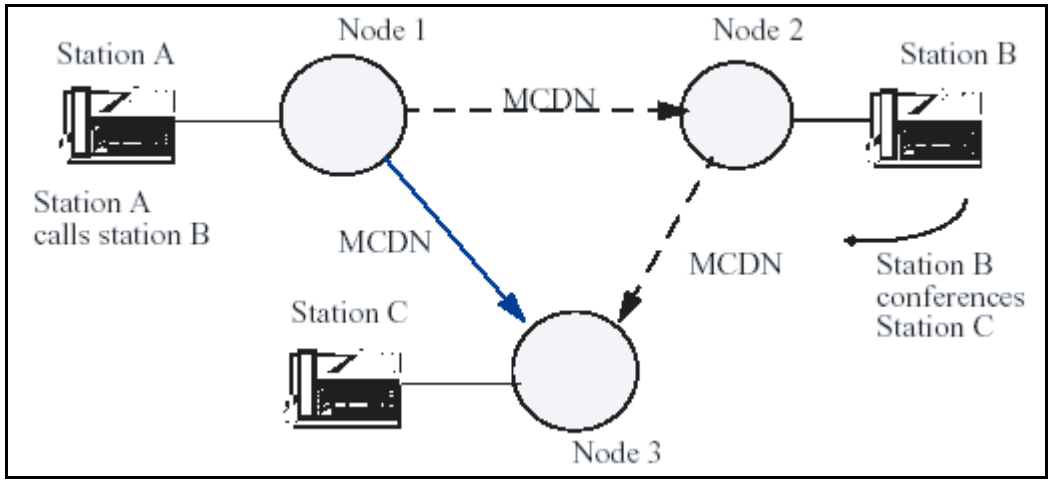


Conference call on disconnection

The system triggers TRO-CM when a conference call reverts to a two-party call.

For example, in Figure 59 on page 388, Station A (node 1) calls Station B (node 2). Station B answers the call. Station B initiates the conference to Station C on node 3. Station C answers the call. Station B completes the conference. The 3 parties are in conference. Station B drops out of conference. The system triggers TRO-CM to optimize the path between Station A and Station C.

Figure 64
TRO-CM operation after conference call

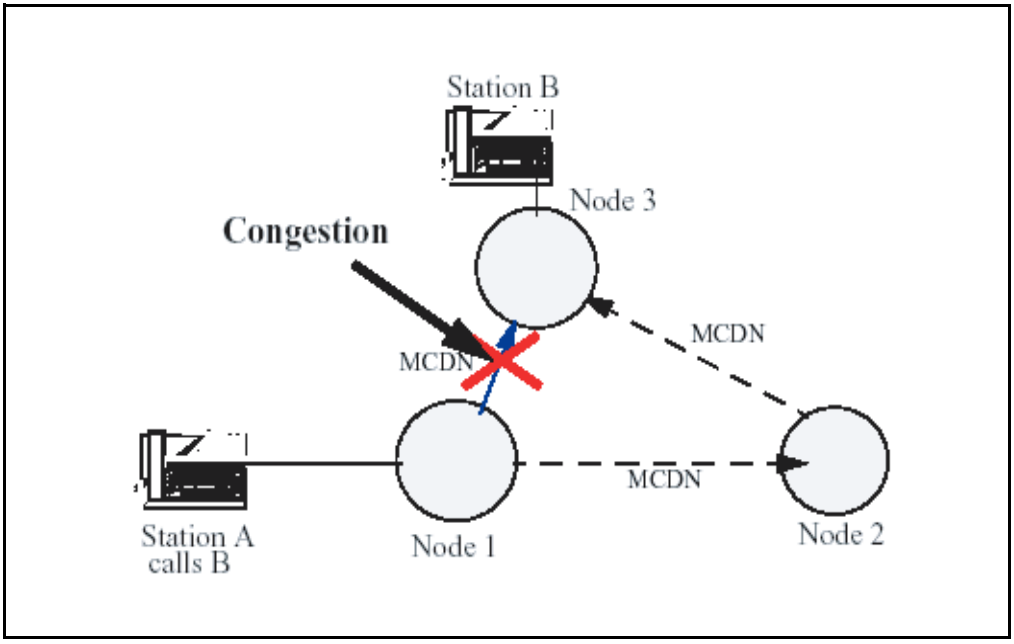


Congestion trigger

Unlike QSIG Path Replacement (QPR), the system does not trigger TRO-CM if non-optimum path results exist because of congestion.

Refer to Figure 65. Station B receives an incoming call from Station A. The system routes the call through node 2 because the link between node 1 and node 3 is congested. Station B answers. Upon reception of a connect indication from node 3, node 1 does not initiate optimization. The link between nodes 1 and 3 stays in place for the duration of the call. The system does not optimize TRO-CM.

Figure 65
Network congestion



Data and Fax Calls

The system can lose or corrupt data during speechpath swapping due to the following:

- pads introduced by the conference card
- continuous conference warning tone

Data applications, such as fax machines, which use normal voice line cards and configuration, are subject to momentary loss of speech during the change-over of speechpaths. This change-over can cause a loss of synchronization between the devices concerned. The system does not trigger TRO-CM during data calls, because this affects data transmission.

The TRO-CM feature does not optimize a call involving an analog (500/2500-type) set configured with the Fax Allowed (FAXA) class of service. This also applies to T.38 Fax calls as the Class of Service for these machines is FAXA.

First choice route

The system attempts TRO-CM only on the first choice route on the TRO-CM originating node.

The system attempts TRO-CM on all tandem nodes on the first choice route if the systems run Succession 3.0 software. If the tandem nodes are running an earlier software release, the system selects any available route for the optimized call.

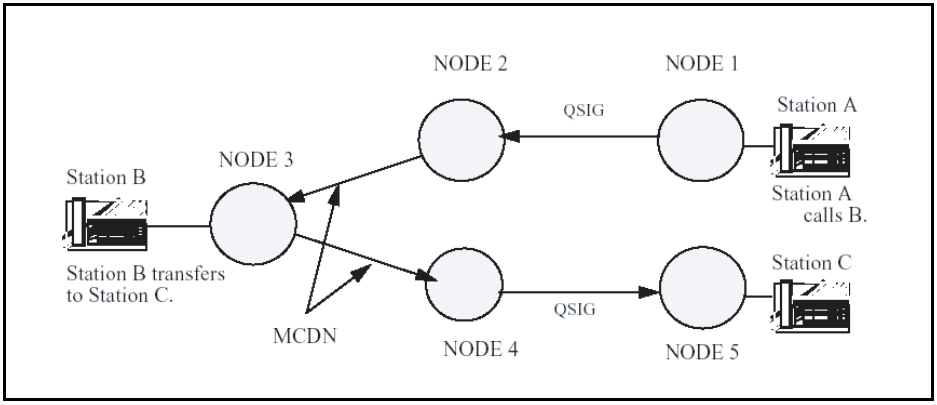
On the TRO-CM originating node and on all the tandem nodes on Succession 3.0 software, the system does not attempt TRO-CM if the system does not find an idle trunk on the first choice route when trying to optimize the call.

Gateway functionality

TRO-CM does not support Gateway functionality with other equivalent features like QSIG Path Replacement (QPR), DPNSS Route Optimization (RO), EuroISDN Explicit Call Transfer (ECT) and Release Link Trunk (RLT) on DMS100/ DMS250 features.

Refer to Figure 66. Node 4 rejects the QPR trigger from node 5, when the system completes the transfer. The system does not map QPR messages into equivalent TRO-CM messages.

Figure 66
Gateway functionality



Initialization

The system loses conferences when it initializes.

On the TRO-CM destination node

If a system initialization occurs on the TRO destination node, the system aborts all TRO-CM operations.

During call process optimization, when the old and the new paths are in conference on the TRO-CM destination node, an initialize on the destination node causes the call to be lost.

On the TRO-CM originating node

A system initialization causes all received TRO-CM requests to be lost. The system does not inform the TRO-CM destination node that the request was cancelled.

The TRO-CM destination node resends the TRO-CM trigger if the TRO-CM originating node initializes before setting-up the new connection. It disconnects the new path on the expiry timer T2, if the TRO-CM originating node initializes after the system sets up the new connection.

Interworking

The system invokes TRO-CM at the interworking node. For example, the system optimizes calls entering or leaving the private network on PSTN/private network trunks after any call modification. However, the system only optimizes the MCDN network.

Figure 67
TRO-CM successful at an interworking node

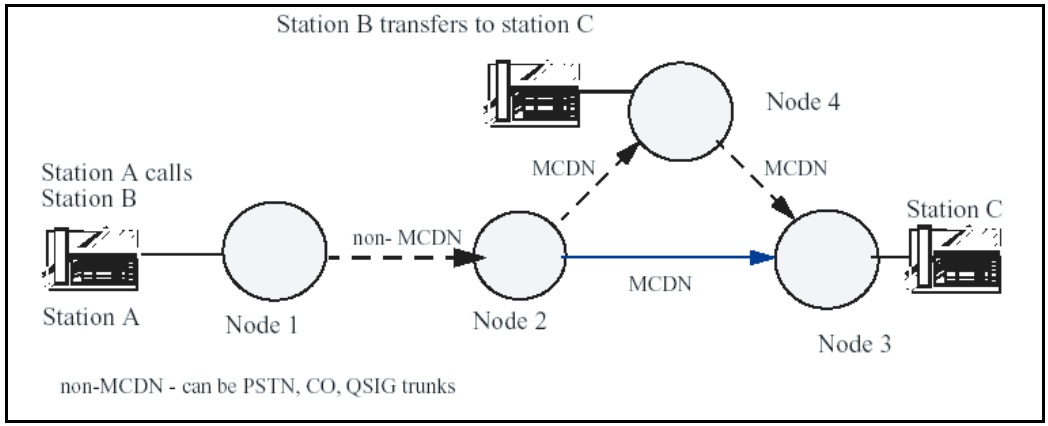
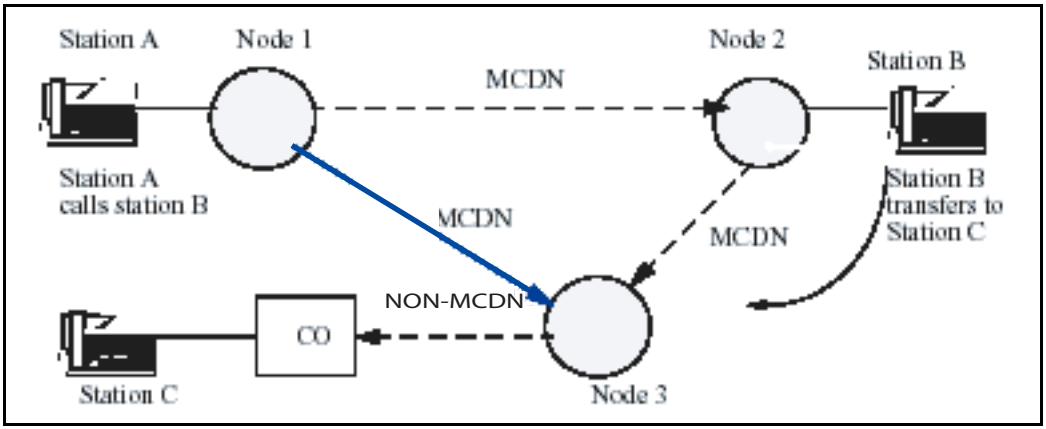


Figure 68
Non-MCDN trunk terminations

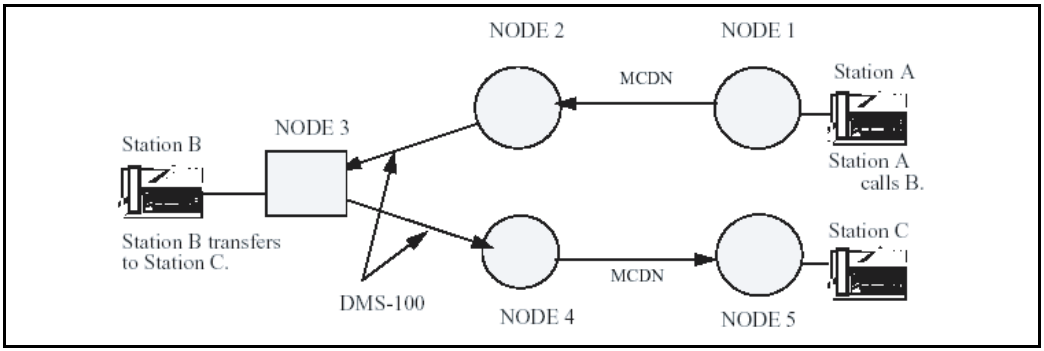


MCDN Release Link Trunk

TRO-CM does not support interworking with DMS switches or SL-100 systems equipped with MCDN RLT feature.

For example, in Figure 69, the system triggers TRO-CM to optimize the MCDN nodes or triggers Release Link Trunk (RLT) on the CO trunks to optimize the trunks between nodes 1 and 5.

Figure 69
Interworking with DMS-100



Numbering plans

The numbering plan scheme chosen for the MCDN network must be a consistent numbering plan. This is essential for the correct operation of the TRO-CM feature operation.

This feature is only supported when CDP or UDP is used. This feature does not support route access codes or the use of transit nodes to modify digits. This feature does not support a mix of CDP and UDP.

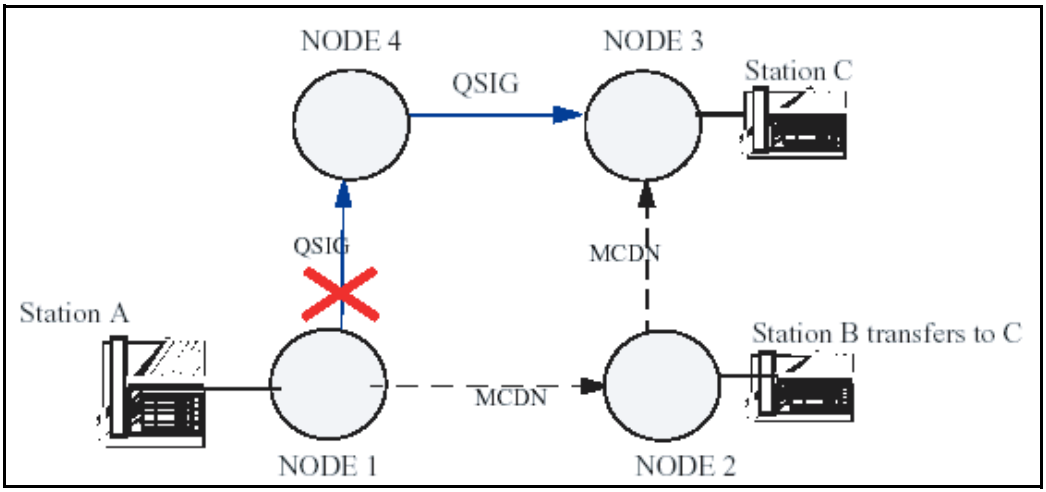
TRO-CM can fail in a network with a non-uniform numbering plan. For example:

- route access codes used
- nodes convert incoming digits
- mix of CDP and UDP

Optimum path – non-MCDN link

The optimum path must be an MCDN link. In Figure 70, station A calls station B. Station B is diverted to station C. Node 1 initiates a new call, but the optimum path from node 1 to node 3 is a QSIG link. The system does not optimize when the optimum path is on VNS because the bearer trunks are non-MCDN trunks. TRO-CM fails.

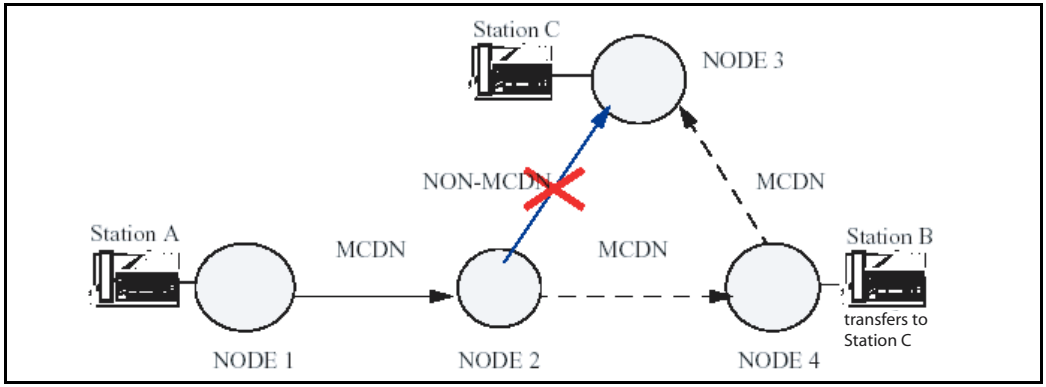
Figure 70
TRO-CM fails when the optimum path is not an MCDN trunk



The system supports TRO-CM only on MCDN trunks on an end-to-end basis. In the scenario in Figure 71, the system does not optimize the call.

Station A calls Station B tandem through node 2. Station B answers the call and transfers to Station C. The system has no direct MCDN TIE between node 2 and node 3; therefore, the system does not optimize the call.

Figure 71
Non-MCDN trunks



Route access code

The system attempts TRO-CM only when the system makes the call through the ESN Uniform Dialing Plan or Coordinated Dialing Plan (CDP). TRO-CM does not support calls initiated with a route access code.

Feature interactions

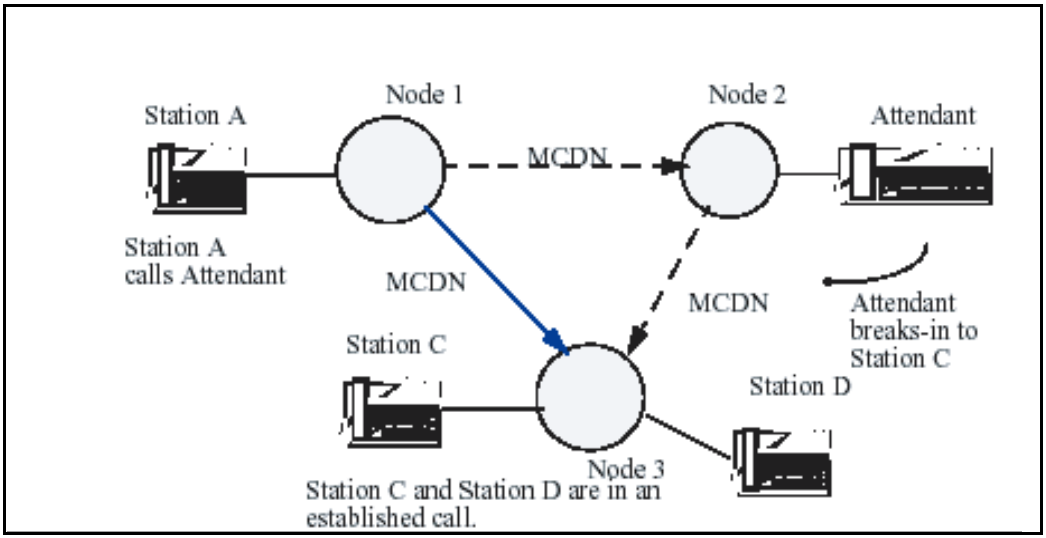
Attendant Break-in
Networkwide Break-in

The system does not optimize any call that is a result of pre-dial or post-dial break-in. After break-in, the system attempts optimization if the call is eligible for TRO-CM. For example, calls transferred or attendant extended calls.

For example, in Figure 72, Station C is on a call with Station D. Station A calls the attendant on node 2. The attendant performs a pre-dial or post-dial break-in to Station C. This does not trigger TRO-CM.

Once Station D disconnects, the attendant completes the extension of the incoming call. The system treats the call as a normal modified call. The system triggers TRO-CM from node 3.

Figure 72
Attendant Break-In

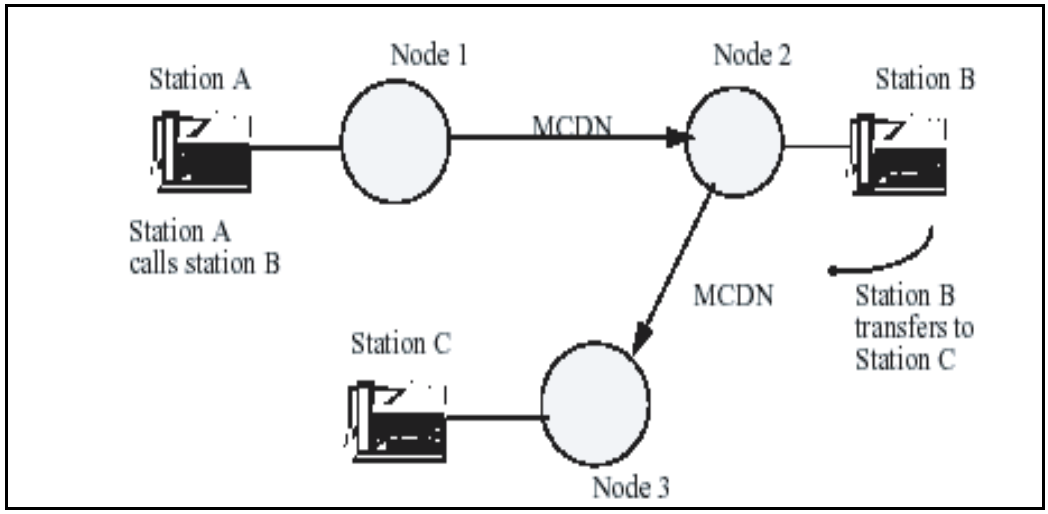


On the TRO-CM destination node, when the system sends the trigger and before the new setup is received, if break-in is attempted on Station C, the system aborts TRO-CM. See Figure 73 on page 405.

When TRO-CM is in progress on the TRO-CM destination node, and when the original path and the new path are in conference, break-in is not possible.

When the system receives the TRO-CM Trigger on the TRO-CM originating node and Station A is broken-into, the system rejects TRO-CM when there is a permanent failure reason. This is because the break-in is attempted to disconnect the old call. See Figure 73.

Figure 73
Before TRO-CM operation



Automatic Call Distribution

When the Automatic Call Distribution (ACD) agent at the TRO-CM destination node answers the call, the system triggers the TRO-CM.

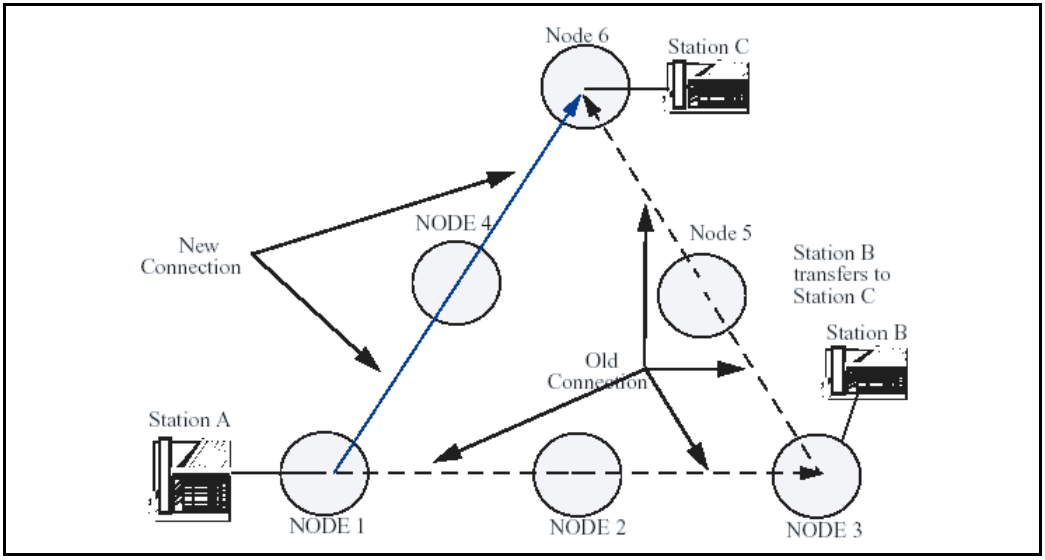
Barge in

Barge-in calls are attendant-originated; therefore, they do not optimize.

Call Detail Recording

In Figure 74, Station A calls Station B. Station B transfers the call to Station C. Station C answers the call, Station B completes the transfer. The system triggers TRO-CM, and a new connection between node 1 and node 6 through node 4 is set-up.

Figure 74
Triangulation



Old path disconnect

The following happens during TRO-CM when the system disconnects the old path:

- The TRO-CM originating node and TRO-CM destination node (node 1 and node 6) do not print CDR records for the old connection.
- The tandem nodes (node 2 and node 5) print CDR information that shows the release of the old connection.
- Node 3 prints an end record to indicate the release of the old connection.

Cleared call between Station A and Station C

The following occurs when the system clears the call between Station A and Station C:

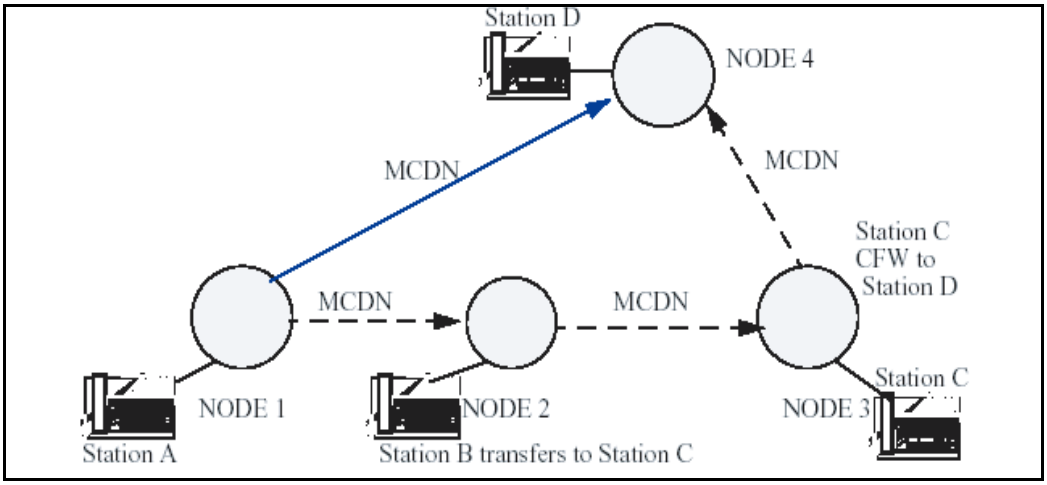
- The CDR records printed on node 1 and node 6 indicate the call started when the system made the old connection. Node 1 displays Station A, the originator of the new connection, as the originator of the old connection. Node 6 displays Station C, the terminator of the new connection, as the terminator of the old connection.
- Node 4 (Tandem Node) prints CDR information that shows the release of a connection, which started when the new connection was made.

Call Forward
Call Forward Busy
Call Forward All Calls
Call Forward Hunt

When Call Forward Busy, Call Forward All Calls, and Call Forward Hunt follow a blind or supervised transfer, the system triggers optimization only after the terminating party answers the call.

For example, as shown in Figure 75, Station A calls Station B. Station B initiates a transfer to Station C. Station C is call forwarded to Station D. Station B completes the transfer. Station D answers the call. TRO-CM optimizes the call between Station A and Station D.

Figure 75
Transfer followed by Call Forward



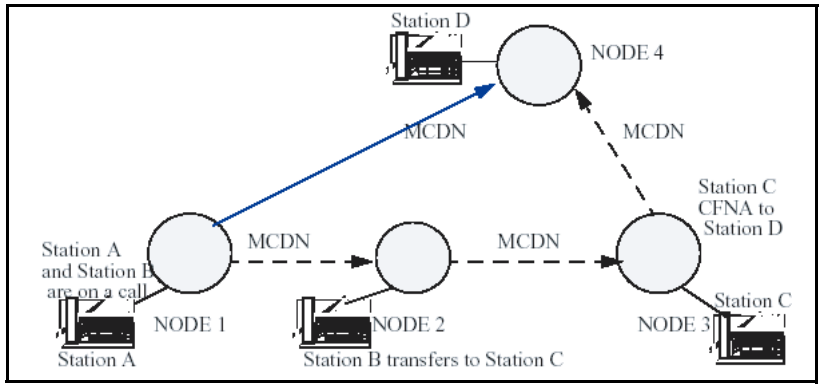
Call Forward No Answer

The system triggers TRO-CM upon answer only if CFNA follows a supervised transfer. The system optimizes Call Forward No Answer calls only on answer.

In Figure 76, Station A calls Station B. Station B initiates a transfer to Station C. Station C is CFNA to Station D. Station D answers the call. Station B completes the transfer. TRO-CM optimizes the call between Station A and Station D.

However, if Station B performs a blind transfer to Station C, the system does not trigger TRO-CM.

Figure 76
Supervised transfer followed by CFNA



Call Hold

The system aborts the TRO-CM operation when the terminating party or originating party attempts to put the call on hold.

If the call on the TRO-CM originating node is on hold, when the TRO-CM Trigger is received, the system rejects TRO-CM when there is temporary failure reason.

Call Park

The system does not optimize Parked calls. For example, when Station A on node 1 calls Station B on node 2, Station B transfers the call to Station C on node 3. Station C parks the call. Station B completes the transfer. The system does not trigger TRO-CM.

When Station A on node 1 calls Station B on node 2, Station B initiates transfers to Station C on node 3. Station B completes the transfer. The system triggers TRO-CM. When Station C attempts to park the call, the system aborts the TRO-CM process.

If Station A parks the call on the TRO-CM originating node, when the TRO-CM trigger is received, the request is rejected.

If station A parks the call on the TRO-CM originating node, the destination node rejects the request, when the originating node receives the TRO-CM trigger.

If Station A attempts to park the call when a TRO-CM setup facility has been sent to the TRO-CM destination node, the system cancels the TRO-CM operations.

Call Pick-up
Network Call Pick-up

The system does not optimize picked-up calls. For example, Station A on node 1 calls Station B on node 2. Station B initiates a transfer to Station C on node 3. While Station C is ringing, B completes the transfer. Station D (on the same node or on a different node) picks up Station C's call. The system does not trigger TRO-CM.

The system triggers TRO-CM if Station B does a supervised transfer.

Call Transfer

When the system sends the trigger from the TRO-CM Destination node and before the Originating node receives the new setup, if Station C attempts to transfer the call, the system aborts TRO-CM operations. See Figure 73 on page 405.

When TRO-CM is in progress on the TRO-CM destination node, and when the original path and the new path are in conference, transfer is possible.

If Station A on the TRO-CM originating node performs a transfer when the TRO-CM trigger is received, or completes the transfer before the TRO-CM trigger is received, the request is rejected.

When Station A attempts to transfer when a TRO-CM setup facility was sent to the TRO-CM destination node, the system aborts TRO-CM operations.

When the system completes the transfer, it updates the display on the sets. The system invokes TRO-CM only after the system updates the display on the sets. TRO-CM does not alter the display of the users.

A local Call Transfer does not trigger a TRO-CM request.

Call Waiting

The system does not invoke TRO-CM on a waiting call. However, the system invokes TRO-CM, if eligible, when the intended party answers the waiting call.

For example, in Figure 73 on page 405, Station A calls Station B. Station C is busy on another call. Station B attempts to transfer the call to Station C. Station B's call is waiting on Station C. This does not trigger TRO-CM. However, when Station C picks up the waiting call, the system triggers TRO-CM.

Camp-On

The system does not invoke TRO-CM on a camped-on call. However, the system invokes TRO-CM, if eligible, once the intended party answers the camped-on call.

For example, in Figure 72 on page 404, Station A calls the attendant on node 2. Station C is busy on another call. The attendant camps the call on Station C. This action does not trigger TRO-CM. However, once Station C is free and answers the camped-on call, the system triggers TRO-CM.

Conference

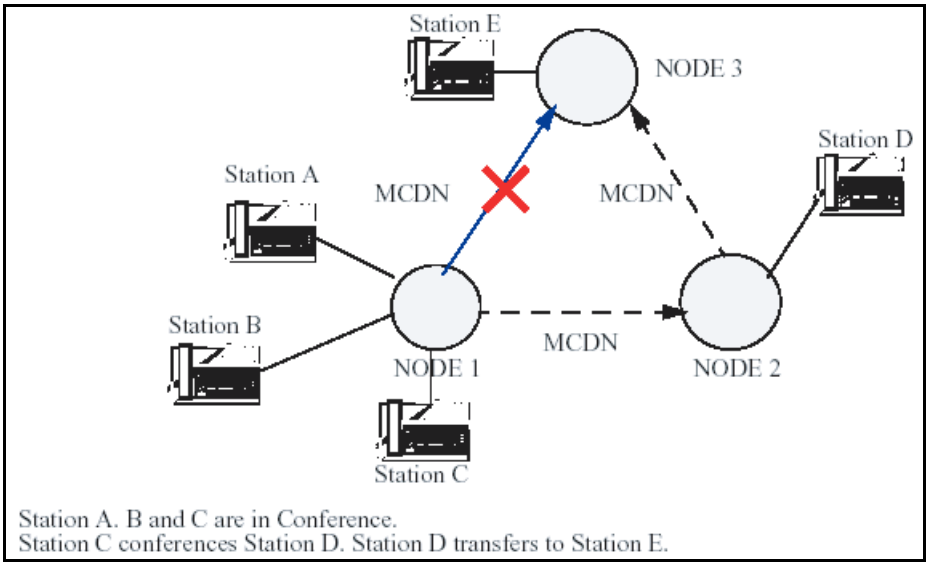
The system does not send a TRO-CM request for a user involved in an established conference.

The system rejects any TRO-CM request from a destination node, when the target station is in an established conference.

The system initiates TRO-CM when it releases the conference, if applicable.

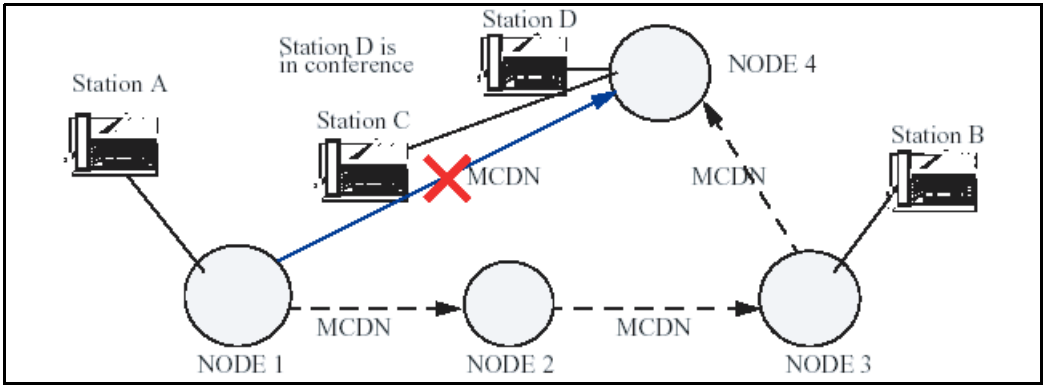
In Figure 77, when Station D transfers (blind or supervised) to Station E and Station E answers, node 1 rejects the TRO-CM request and the system aborts TRO-CM.

Figure 77
Conference at the TRO-CM originating node



In Figure 78, Station A calls Station B. Station B initiates a transfer to Station C. Station C answers the call and conferences Station D. Station B completes the transfer. The system does not invoke the TRO-CM request.

Figure 78
Conference at the TRO-CM destination node



End to End Signaling

The system delays TRO-CM when it detects use of End-to-End Signaling. The TRO-CM destination node reattempts TRO-CM twice. If End-to-End Signaling completes within this time, TRO-CM is successful.

Music

On the TRO-CM destination node, if the call is connected to a music trunk, TRO-CM is not triggered. Any request from the TRO-CM destination node on a call for which music is provided is temporarily rejected. The TRO-CM destination node reattempts TRO-CM twice. If Music is withdrawn from the call within this time, TRO-CM will be successful.

If the system connects the call on the TRO-CM destination node to the Music trunk, then the system does not trigger TRO-CM. The system temporarily rejects any call on a music trunk.

Radio Paging

TRO-CM does not take place on a paged call. As a result, the system does not invoke TRO-CM on a paged call. Any request from the TRO-CM destination node is permanently rejected.

Recorded Announcement

If the system connects the call on the TRO-CM destination node to the RAN trunk, it does not trigger TRO-CM. If the TRO-CM destination node makes any request on a call that has RAN provided, then the system rejects the request. The TRO-CM destination node reattempts TRO-CM twice. If the system withdraws RAN during this time, then TRO-CM is successful.

Feature packaging

TRO-CM requires Advanced Network Services (NTWK) package 148.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. LD 16 – Configure trunk route optimization.
2. LD 17 – Configure ADAN. In the case of a VNS D-channel, make the required change to ADAN.

   Note: Configure the RLI entry 0 as the direct route to the destination node. The system chooses the RLI entry 0 to route the new optimized call. If a direct route is not possible, configure the shortest route to reach the destination node.

LD 16 – Configure trunk route optimization. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	RDB	Route Data Block
CUST	xx	Customer number, as defined in LD 15
ROUT	 0-511 0-127	Route number For Large Systems For Small Systems and Succession 1000 systems
DTRK	(NO) YES	Digital Trunk Route Must be YES to prompt ISDN
ISDN	(NO) YES	Integrated Services Digital Network
IFC	SL1	Interface type

LD 16 – Configure trunk route optimization. (Part 2 of 2)

Prompt	Response	Description
NCRD	(NO) YES	Network Call Redirection. Allows Network Call Redirection messages to be sent (or blocks messages if NCRD = NO). Must be YES to prompt TRO.
TRO	(NO) YES	Trunk Route Optimization

LD 17 – Configure ADAN. In the case of a VNS D-channel, make the required change to ADAN.

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	ADAN	Change or add information to the data block
ADAN	CHG DCH xx	Action Device and Number
USR	 VNS SHAV	User Virtual Network Services Shared Virtual Network Services
...		
VCRD	YES	Network Call Redirection Allowed
VTRO	YES	VNS TRO allowed

Timers

All TRO-CM timers implemented on the system are not service-changeable.

Table 46
TRO-CM Timers

Timer	Description	Value	Applicable Node	Action on expiry
T1	Started by the TRO-CM destination node to protect against the absence of a response to TROCMTrigger invoke Facility. The response can be a TROCMTrigger return error IE or a TROCMSetup invoke IE.	30s	TRO-CM destination	When timer T1 expires, the system sends TRO-CM Trigger again. The system attempts TRO-CM twice. If the system does not succeed in the second attempt, all TRO-CM operations are cancelled.
T2	Started by the TRO-CM destination node to protect against failure to release the old connection.	20s	TRO-CM destination	The TRO-CM destination node disconnects the new connection on expiry.

Feature operation

There are no operating procedures specified for this feature.

UIPE D-channel Monitoring Tool Enhancement

Contents

This section contains information on the following topics:

Feature description

The UIPE D-Channel Monitoring Tool Enhancement enables the Q.931 message monitoring to support the decoded message format. For enabled messages, it also supports channel-based, message-based, and SET TN-based filtering.

The UIPE D-Channel Monitoring Enhancement modifies the monitor output so the debug option prints in three formats. It also removes the existing password protection for the Q.931 monitor.

If the monitor is enabled and the number of Call Registers in the idle queue drops below 10%, message monitoring is suspended. If the monitor is enabled and the number of idle call registers exceeds 10%, message printing starts again. For UIPE messages, the UIPE D-Channel Monitoring Tool Enhancement includes a real-time clock stamp on all messages printed on the terminal.

LD 96 introduces commands to support message filtering based on the ISDN TNs and the message type for Q.931 messages.

LD 96 also introduces a command to set filtering options for a D-channel based on terminals. This filtering option is a filtering paradigm that applies to UIPE proprietary messages and Q.931 messages. In the data block called MON_DATA, the system accepts TNs for set-based filtering based on user input at new prompts. Set-based filtering applies only to digital and analog terminals.

The LD 96 command that prints the monitor options status for a D-channel is modified to print the newly supported levels and options for the Q.931 messages.

For UIPE proprietary messages and Q.931 messages, the system provides the ON or OFF status of set-based filtering.

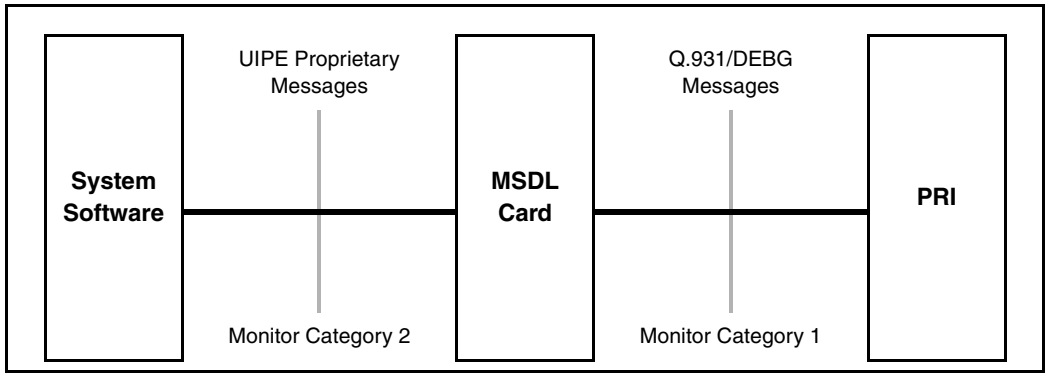
Points of monitoring

Figure 79 on page 419 shows the two monitors available for the Meridian 1, Succession 1000, and Succession 1000M systems:

- Q.931 debug monitor for UIPE interfaces
- UIPE proprietary messages monitor (Internal Software Monitor)

Monitor category 1 (Debug Monitor) indicates messages exchanged between the Meridian 1, Succession 1000, Succession 1000M systems and the external world (Q.931 messages). Monitor category 2 (Internal Software Monitor) indicates messages (UIPE proprietary) exchanged between system software and the Multi-purpose Serial Data Link (MSDL) card.

Figure 79
Points of monitor



Enhancement summary

Table 47 on page 419 shows enhancements to the UIPE and Q.931 monitoring tool.

Table 47
Enhancement summary

Message Type	Monitor level			Based on		
	0	1	2	Channel	Message	Set TN
Q.931	×	✓	×	×	×	×
UIPE	✓	✓	✓	✓	✓	×

✓ Existing with continued support

× Supported after enhancements

Outgoing messages

Table 48 on page 420 indicates the message mnemonics for outgoing messages for UIPE proprietary and Q.931 messages.

Table 48
Outgoing messages (Part 1 of 2)

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Supported on Q.931
ALER	CC_ALERT_REQUEST	ALERTING	✓
DISC	CC_DISCONNECT_REQUEST	DISCONNECT	✓
FAC	CCC_FAC_REQUEST	FACILITY	✓
FRNC	CC_FAC_REG_NULL_CRF	FACILITY	✓
FJNC	CC_FACREJ_REQ_NULL_CRF	FACILITY REJECT	✓
INFO	CC_INFORMATION_REQUEST	INFORMATION	✓
MIFO	CC_MORE_INFO_REQUEST	SETUP ACK	✓
NOTF	CC_NOTIFY_REQUEST	NOTIFY	✓
PROC	CC_PROCEEDING_REQUEST	CALL PROCEEDING	✓
PROG	CC_PROGRESS_REQUEST	PROGRESS	✓
REJ	CC_REJECT_REQUEST	RELEASE COMPLETE	X
RLS	CC_RELEASE_RESPONSE	RELEASE	✓
RLSR	CC_RELEASE_RESPONSE		
STP	CC_SETUP_REQUEST	SETUP	✓
STPR	CC_SETUP_RESPONSE	CONNECT	✓
STEN	CC_STATUS_ENQ_REQUEST	STATUS ENQUIRY	✓
STAT	CC_STATUS_REQUEST	STATUS	✓
RST	CC_RESTART_REQUEST	RESTART	X
RSTR	CC_RESTART_RESPONSE	RESTART ACK	X

Table 48
Outgoing messages (Part 2 of 2)

SVC	SERVICE MESSAGES	SERVICE	✓
SVCR	SERVICE RESPONSE	SERVICE RESPONSE	✓
RSTJ	CC_RESTART_REJECT	RESTART REJECT	X

Incoming messages

Table 49 on page 421 indicates the message mnemonics for incoming messages for UIPE proprietary and Q.931 messages.

Table 49
Outgoing messages (Part 1 of 2)

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
ALER	CC_ALERT_INDICATION	ALERTING	✓
DISC	CC_DISCONNECT_INDICATION	DISCONNECT	✓
FAC	CCC_FAC_INDICATION	FACILITY	✓
FIDC	CC_FAC_IND_NULL_CRF	FACILITY	✓
FJDC	CC_FACREJ_IND_NULL_CRF	FACILITY REJECT	✓
INFO	CC_INFORMATION_INDICATION	INFORMATION	✓
MIFO	CC_MORE_INFO_INDICATION	SETUP ACK	✓
NOTF	CC_NOTIFY_INDICATION	NOTIFY	✓
PROC	CC_PROCEEDING_INDICATION	CALL PROCEEDING	✓
PROG	CC_PROGRESS_INDICATION	PROGRESS	✓
RLSC	CC_RELEASE_CONFIRMATION	RELEASE COMPLETE	X
RLS	CC_RELEASE_INDICATION	RELEASE	✓
REJ	CC_REJECT_INDICATION	RELEASE COMPLETE	✓

Table 49
Outgoing messages (Part 2 of 2)

STP	CC_SETUP_INDICATION	SETUP	✓
STPC	CC_SETUP_CONFIRMATION	CONNECT	✓
STEN	CC_STATUS_ENQ_INDICATION	STATUS ENQUIRY	✓
STAT	CC_STATUS_INDICATION	STATUS	✓
RST	CC_RESTART_INDICATION	RESTART	X
RSTC	CC_RESTART_CONFIRMATION	RESTART ACK	X
SVC	SERVICE MESSAGES	SERVICE	✓
SVCR	SERVICE RESPONSE	SERVICE RESPONSE	✓

Operating parameters

UIPE D-channel Monitoring Tool Enhancement is not applicable for BRI because the debug option is not supported for BRI.

For set-based monitoring, attendant consoles and ISDN terminals are not supported.

For set-based filtering of messages, incoming calls to a set are not supported.

For channel-based monitoring, the messages that do not have channel ID IE or call reference in the call reference table are not supported. This is also applicable for set-based monitoring.

> ***Note:*** Messages that do not have channel ID IE or valid call references in the call reference table always have the channel number printed as NCAL in the message header.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The UIPE D-channel Monitoring Tool Enhancement feature requires the following packages:

- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146
- International Primary Rate Access (IPRA) package 154
- Multi-purpose Serial Data Link (MSDL) package 222

The UIPE D-Channel Monitoring Tool Enhancement does not introduce a software package.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1 LD 15 - Enter the TNs of the sets to be monitored (Set-Based Monitoring).

2 LD 96 - Enable or disable the monitor.

3 LD 96 - Query the status of the monitor and the filtering options.

4 LD 96 - Set monitor level.

a Mon. 0 for Craft level monitoring

b Mon. 1 for Raw format

c Mon. 2 for IE level decoded

LD 15 – Enter the TNs of the sets to be monitored (Set-Based Monitoring).

LD 15 accepts new data for set-based monitoring. Enter the TNs of the sets to be monitored. If UIPE Set-Based Monitoring (USBM) is set to YES, the subsequent TN prompts are prompted. If USBM is set to NO, the values for the TN are cleared.

Note: The TNs entered are data dumped and retained after sysload.

LD 15 – Enter the TNs of the sets to be monitored (Set-Based Monitoring).

Prompt	Response	Description
REQ:	CHG NEW	Add new data. Change existing data.
TYPE:	MON	Monitoring
USBM	(NO) YES	Accept and prompt the next prompts if YES. If NO is entered, subsequent prompts are not prompted, and all the TNs configured earlier are flushed. If <CR> previously stored value taken.
TN1	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems
TN2	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems
TN3	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems
TN4	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems
TN5	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems
TN6	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems

LD 96 – UIPE D-channel Monitoring Tool Enhancement commands

In LD 96 you can:

- Enable or disable the monitor.
- Query the status of the monitor and the filtering options.
- Set the monitor level.
  - Mon. 0 for Craft level monitoring
  - Mon. 1 for Raw format (Default)
  - Mon. 2 for IE level decoded

LD 96 – UIPE D-channel Monitoring Tool Enhancement commands (Part 1 of 3)

Command	Description
ENL MSGI <dch> DEBG MSG msg1 msg2 msg3	
	Enable the debugging of all monitored incoming messages from D-channel This command can be entered more than once. In one command, only 3 message mnemonics can be given.
ENL MSGO <dch> DEBG MSG msg1 msg2 msg3	
	Enable the debugging of all monitored outgoing messages from D-channel This command can be entered more than once. Only 3 message mnemonics can be given in one command.
DIS MSGI <dch> DEBG MSG msg1 msg2 msg3	
	Disable the debugging of all monitored incoming messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.

LD 96 – UIPE D-channel Monitoring Tool Enhancement commands (Part 2 of 3)

Command	Description
DIS MSGO <dch> DEBG MSG msg1 msg2 msg3	
	Disable the debugging of all monitored outgoing messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.
ENL MSGI <dch> DEBG CH <loop><channel>	
	Enable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
ENL MSGO <dch> DEBG CH <loop><channel>	
	Enable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
DIS MSGI <dch> DEBG CH <loop><channel>	
	Disable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
DIS MSGO <dch> DEBG CH <loop><channel>	
	Disable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.

LD 96 – UIPE D-channel Monitoring Tool Enhancement commands (Part 3 of 3)

Command	Description
ENL MSGI <dch> DEBG SET	
	Enable debug SET on all incoming messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.
ENL MSGO <dch> DEBG SET	
	Enable debug SET on all outgoing messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.
DIS MSGI <dch> DEBG SET	
	Disable debug SET on all incoming messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.
DIS MSGO <dch> DEBG SET	
	Disable debug SET on all outgoing messages from D-channel. This set-based filtering is enhanced for UIPE proprietary messages.

Feature operation

There are no specific operating procedures required by this feature.

Succession 1000 Element Manager

Contents

This section contains information on the following topics:

Feature description

The Succession Signaling Server hosts a new web server that supports a web interface. This web interface, which is called Succession 1000 Element Manager, enables an administrator to use a browser to configure and maintain system components. Before Element Manager, configuration and maintenance tasks were completed in overlays. Element Manager also supports application management on the Succession Signaling Server.

Element Manager increases the speed, efficiency, and accuracy of the configuration process. Configuration parameters are now organized into logical groups, which provides the following advantages to administrators:

- no need to print information in overlays (LDs 20, 21, 22) before loading a different overlay to edit the configuration

- no need to enter several carriage returns to change a single prompt
- can access data from multiple overlays on a single web page

Element Manager permits administrators to hide and show information. This facilitates focus on information of interest, without the distraction of multiple parameters.

Element Manager provides full text descriptions as well as acronyms for each parameter. This benefits users by:

- presenting a friendly interface for new administrators
- keeping existing acronyms for experienced administrators

Element Manager simplifies parameter value selection by:

- pre-selecting default values
- providing a drop-down list of allowed values
- displaying a range of values for numeric entries
- using Yes/No checkboxes

Administrators can use Element Manager to configure and maintain the following components of Succession 3.0 software:

- Succession Signaling Server
- Call Server
- Media and Branch Office Gateways
- IP Line 3.1 / Voice Gateway
- IP telephony
- Gatekeeper

In Succession 3.0, administrators can use Element Manager to perform the following management tasks:

- **Get System Status.** Perform maintenance activities on IP Telephony and Call Server components:
  - D-channel

- MSDL
- TMDI
- Digital trunk
- Clock controller
- Network and Peripheral Equipment
- Trunk diagnostic
- Zone Diagnostic
- IP Telephony Service Management
- Core Common Equipment Diagnostic
- Call Server Report Log
- System Incremental Software Management (ISM) Parameters
- Equipped Feature Packages List
- Peripheral Software Version Data

- **Configuration.** Configure:
  - Customer data, routes, and trunks (traditionally done in LDs 15, 16, and 14)
  - D-channel and Common Equipment data (LD 17)
  - Digital Trunk Interface (LD 73)
  - Flexible Code Restriction and Incoming Digit Conversion (LD 49)
  - IP telephony

- **Network Numbering Plan**. Configure all ESN data blocks for the Call Server as well as the Gatekeeper.
- **Software Upgrade**. Upgrade IP telephony firmware and loadware. It is also used to upload firmware and loadware files for storage on the Signaling Server.
- **Patching.** Download, activate, and deactivate patches for:
  - the Call Server
  - Media Gateways

— IP telephony

- **System Utilities**. Backup and restore Call Server data, as well as set the system date and time.

For more information on Succession 1000, see *Succession 1000 System: Overview* (553-3031-010).

Succession Signaling Server

After software installation and basic configuration of the Succession Signaling Server, components of the Succession Call Server, Succession Signaling Server, and IP Line 3.1 / Voice Gateway Media Cards can be configured using the web-based interface. The web server is installed on each Succession Signaling Server within a Succession 1000 or Succession 1000M system. All HTML web pages and data files required for web-based Element Manager are installed on the Succession Signaling Server.

Element Manager enables administrators to perform the following system activities on the Signaling Server:

- reset
- access the maintenance window
- download new firmware
- view report log
- run Operational Measurements (OM) reports
- Telnet

Succession Call Server, Media Gateway, and Branch Office H.323 WAN Gateway

For Call Servers, Media Gateways, and Succession Branch Office Gateways, Element Manager enables administrators to configure and manage the following data:

- Configuration Record
  - — Supports ADAN, CEQU, and PWD data blocks
- Customer Data Block

— Supports ANI, FCR, FTR, LDN, NET, and NIT data blocks

- Route Data Blocks
- Trunks
- ESN Data Block

IP Line 3.1 / Voice Gateway

Element Manager enables administrators to perform the following activities on the IP Line 3.1 / Voice Gateway:

- View and configure SNMP parameters and add IP addresses for forwarding SNMP traps.
- View and configure VGW profile data.
- View and edit Quality of Service (QoS) parameters.
- Use LAN configuration to configure the ELAN, TLAN, and routes.
- View and edit SNTP Server and Client information.
- View and configure file server access for downloading firmware to Internet Telephones.
- View and select the Loss and Level Plan for your country.
- Add, remove, view, and edit card properties of Voice Gateway Media Cards.
- Add, remove, view, and edit Signaling Server information.

The following maintenance activities are supported using Element Manager for the IP Line 3.1 / Voice Gateway:

- Reset Voice Gateway Media Card.
- Enable/Disable Voice Gateway Media Card.
- Access the maintenance window to the Voice Gateway Media Card.
- Download new loadware/firmware for upgrades.
- Run Syslog reports.

- Run Operational Measurement (OM) reports.
- Telnet to the card.

Changes specific to Succession 3.0

The Element Manager interface was originally introduced with the deployment of Succession CSE 1000 Release 2. Systems equipped with a Signaling Server that are ported to Succession 3.0 can support the following features and enhancements:

- **Large system support**:
  - display different system types in the System Information page
  - TN formats used by large systems
  - increased capacity (different ranges of values for large systems)
  - backup and restore on large systems
- **D-Channel configuration:** Displays the current RCAP selection and all valid inputs for the RCAP prompt. In the previous D-Channel configuration web page, you had to type in RCAP values without knowing which values were currently selected and what inputs were valid.
- **Subnet mask entry validation**: Validate subnet mask entries on IP Telephony web pages.
- **Ability to download more than one patch at a time:**
  - Enable selection of more than one patch to download and activate on the switch for the Call Server, Signaling Server, and IP Line Cards.
- **Context-sensitive field values in LD 16**:
  - The implementation of context-sensitive prompts was introduced in Succession CSE 1000 Release 2, but individual field selections were not context-sensitive. This enhancement introduces implementation of context-sensitive fields for LD 16 web pages.

- **LD 135 Maintenance commands support**:

  — This enhancement provides a web page interface for the following diagnostic and maintenance commands in LD 135:

  DIS CNI c s p

  DSPL <ALL>

  ENL CNI c s p

  IDC CNI s, IDC CPU

  JOIN

  SCPU

  SPLIT

  STAT CNI, STAT CPU, STAT SUTL

  TEST CNI, TEST CPU, TEST SUTL

  The Element Manager System Information page displays the dual CPU redundancy information and the Health state.

- **IP Telephony Operation:** A summary page indicates which IP Telephony nodes have changed and must be transferred. The system provides meaningful information about the telephony SUBMIT/TRANSFER operation of config and bootp node files. The following areas are enhanced:

  — The SUBMIT button has been renamed to **"Save and Transfer"**. Clicking it saves node configuration files on the Call Server side and also transfers files to every element within the node. Previously there were two separate buttons required to SUBMIT and TRANSFER.

  — OTM 2.1 introduces new fields in config and bootp files that also add to configuration files maintained by Element Manager. These fields track the time, date, and authoring application of the last modification of the configuration files.

— On the IP Node summary page, a new button called **TRANSFER/STATUS** replaces the TRANSFER button. If any element within the Node fails to transfer either bootp or config files, the button will be highlighted in RED. A click on this button will redirect the administrator to a page where:

  – the previous status of the node will be displayed, and

  – the reason for failure will be displayed for elements in nodes that failed to get configuration files (*config.ini* and *bootp.tab*) from the Call Server side.

  The **TRANSFER/STATUS** button will be highlighted in YELLOW if the transfer status of the node elements is unavailable. When the administrator edits the Node and clicks the **"Save and Transfer"** button, transfer status information will be updated and displayed.

— Node elements that failed to get configuration files will continue to display on the transfer progress status page when the IP Telephony node configuration file is submitted and transferred.

— The Transfer status page displays two buttons:

  – **Transfer to Selected Elements.** Re-transfers node configuration files only to selected elements, regardless of a "Transfer Failed" state.

  – **Transfer to Failed Elements.** Only transfers node configuration files to elements in a "Transfer Failed" state.

Note: This button will display only when at least one element on the Node failed to transfer either a *bootp.tab* or *config.ini* in the previous operation.

For more information on IP Line or IP Peer Networking, see *IP Line: Description, Installation, and Operation* (553-3001-365) or *IP Peer Networking* (553-3001-213).

- **Software version display in Peripheral Equipment cards:** Enables the administrator to see the versions of all downloaded software in the Peripheral Equipment cards (for example, MSDL and others). This is very useful on large systems. Information from LD 96 and LD 48 will be used to display information along with the LD 22 PSWV command, which shows what is stored on the Call Server.

Operating parameters

Element Manager is available for all Succession 3.0 systems equipped with a Signaling Server.

Since the Signaling Server is optional in a Succession 3.0 system, Element Manager cannot be the only administrative interface. Once the IP Line Media Cards are upgraded to Succession 3.0 software, subsequent loadware/firmware upgrades can be performed through Element Manager web pages.

For Succession 3.0, not all aspects of configuration/maintenance will be available for the Call Processor through the web interface. The main focus of Succession 3.0 is the configuration and maintenance of routes, trunks, ISDN, ESN and zone parameters.

Large Systems have superloop configurations as a basic configuration. Superloop overlay support is not implemented from the Element Manager web browser in Succession 3.0. The administrator must still perform superloop configuration using the TTY before configuring anything else from Element Manager.

Supported Browsers

The Element Manager web interface supports Microsoft Internet Explorer 6.0.

Security

Element Manager web access requires password protection to prevent unauthorized access to configuration and maintenance options.

New or Concurrent Software/Hardware/Firmware/Loadware

Dependencies are as follows:

- availability of Signaling Server platform and Signaling Server base software
- availability of IP Line 3.1 Voice Gateway Media Card application software running on ITG SA (ITG card with Strong Arm Processor) and ITG P (ITG card with Pentium processor) platforms

Feature interactions

The Element Manager interface interacts with data residing on the Call Server and traditionally configured in the following overlays:

- LD 2 - Time/Date Set
- LD 14 - Trunk Data Block
- LD 15 - Customer Data Block
- LD 16 - Route Data Block
- LD 17 - Configuration Record
- LDs 20-22 - Print Reports
- LD 32 - Network and Peripheral Equipment Diagnostic
- LD 36 - Trunk Diagnostic
- LD 43 - Equipment Datadump
- LD 49 - New Flexible Code Restriction and Incoming Digit Conversion

- LD 60 - Digital Trunk Interface and Primary Rate Interface
- LD 73 - Digital Trunk Interface
- LDs 86, 87, 90 - Electronic Switched Network
- LD 96 - D-Channel diagnostic
- LD 117 - Zone Configuration and Diagnostic
- LD 135 - Core Common Equipment Diagnostic

Feature packaging

No new software packages are introduced.

Feature implementation

This feature introduces changes to one overlay to enhance Print routines.

LD 21 – Print Routine 2.

Prompt	Response	Description
REQ:	LCS	List configured customers
	LRT	List configured Routes associated with a customer

This feature introduces two new STAT commands to obtain the status of a virtual trunk.

LD 32 commands

Command	Description
IDU <TN>	Prints the MAC address, Model Vendor, software version, Set IP address, etc. of the polled set.
STVT <cust no> <route no> <start member> <end member>	
	Displays the vtrunk status, specified by customer, route, start and end member number.

This feature introduces two new STAT commands for LINK and server information.

LD 117 commands (Part 1 of 4)

Command	Description
STAT LINK APP <application type>	
	Where: application type = LPTS, VGW, H323, GK, etc.
STAT LINK IP <ip address>	
	Displays the link information status of the server for the specified IP address, or contained in the specified sub-net. Where: IP address is the ELAN IP address of the VGMC / Signaling Server. IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.
STAT LINK NAME <hostName>	
	Displays the link information status of the servers based on the supplied host name. Where: hostName = MAINSERVER

LD 117 commands (Part 2 of 4)

Command	Description
STAT LINK NODE <node id>	
	Displays the link information status of the specified node. Where: node id is a number from 0 - 9999. It identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.
STAT LINK SRV <server type>	
	Displays the link information status of the servers for the specified server type. serverType = ITGP (ITG Pentium) serverType = SMC (Succession Media Card) serverType = SS (Signalling Server)
STAT SERV APP <application type>	
	Displays the link information status of the servers running the specified applications. applicationType = LTPS (Line TPS) applicationType = VGW (Voice Gateway) applicationType = H323 (H323 Virtual Trunk) applicationType = GK (GateKeeper)
STAT SERV IP <ip address>	
	Displays the link information status of the server for the specified IP address, or contained in the specified sub-net. Where: IP address is the ELAN IP address of the VGMC / Signaling Server. IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.

LD 117 commands (Part 3 of 4)

Command	Description
STAT SERV NAME <host name>	
	Displays the link information status of the servers based on the supplied host name. Where: host name = MAINSERVER
STAT SERV NODE <node id>	
	Displays the link information status of the specified node. Where: node id is a number from 0 - 9999. It identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.
STIP HOSTIP <ip address>	
	Displays information contained in the rlm table corresponding to the specified HOSTIP address, or HOSTIP addresses contained in the specified sub-net. Where: IP address is the ELAN IP address of the VGMC / Signaling Server. IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.
STIP NODE <node id>	Displays information contained in the rlm table corresponding to the specified node id. Where: node id is a number from 0 - 9999. It identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.

LD 117 commands (Part 4 of 4)

Command	Description
STIP TERMIP <ip address>	
	Displays information contained in the rlm table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net. Where: IP address is the TLAN IP address of the set / vgw. IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.
STIP TN l s c u	Displays the rlm information for the specified TN or group of TNs as denoted by the l s c u parameters for large systems, and the c u parameters for Small Systems and Succession 1000 systems.
STIP TYPE <aaa>	Displays the rlm information for the specified TN type, where up to 3 types can be specified. Valid types are: i2002 - i2002 sets i2004 - i2004 sets i2050 - i2050 sets ISET - all IP sets VGW - Voice gateway resources IPTI- Virtual trunk and ITG trunks
STIP ZONE <zone>	Displays the rlm information for the specified zone number / range of zones. Where: the zone is any valid zone number (0 - 255) in the system.

This feature introduces new commands for supporting Graceful Disable CLI commands.

Graceful Disable services

Command	Description
disGK	The local Gatekeeper is gracefully put out-of-service, and the alternative Gatekeeper (if available) is put in-service.
disServices	The server gracefully switches registered resources to other services in the same node.
disTPS	The TPS gracefully switches the registered line TPS and TN to other cards in the same node.
disVTRK	The VTRK gracefully switches the registered virtual trunks to another SIgnaling Server in the same node.

Force Disable services

Command	Description
forcedisGK	The local gatekeeper is forced out-of-service.
forcedisServices	The server is forced to switch registered resources to other services in the same node.
forcedisTPS	The registered line TPS and TN are forced to unregister from the local server.
forcedisVTRK	The registered virtual trunks are forced to unregister from the local server.

EnableServices

Command	Description
enlGK	The local gatekeeper is forced into service.
enlServices	The services are forced to accept registration of resources.
enlTPS	The TPS application is enabled and forced to accept set registrations.
enlVTRK	The signaling server is forced to accept virtual trunk registrations.

Load Balance CLI

Command	Description
loadBalance	The service will attempt to balance the load of sets between itself and other node components.

Status CLI

Command	Description
servicesStatusShow	The services (iset/vtrk/gk) display their status.

Feature operation

This feature includes a web interface that supports element configuration, maintenance, upgrade, and patching.

For information on how to install and configure Succession 1000 Element Manager, see *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232).

For information on Succession 1000 Element Manager system administration, see *Succession 1000 Element Manager: System Administration* (553-3001-332).

Optivity Telephony Manager

Contents

This section contains information on the following topics:

Overview

OTM 2.1 contains updates to support Succession 3.0 Software. Key changes are as follows:

- Operating System support
- hardware requirements for specific configurations
- additional support for USB dongles
- OTM Navigator dialog boxes
- Station Administration functionality
- OTM Common Services functionality

Operating System support

OTM 2.1 operates on the same Operating System software as OTM 2.0 with the following changes:

- Support for English MS Windows XP Professional
- Does not support Windows 98 and Windows NT Workstation

Operating Systems running OTM 2.1 require the following Service Packs.

Table 50
Service Pack requirements

Operating System	Required Service Pack
Windows NT4 Server	Service Pack 6a
Windows 2000 Server	Service Pack 3
Windows 2000 Professional	Service Pack 3
Windows XP Professional	Service Pack 1

Web server support

Accessing OTM web applications requires that IIS is running on the OTM server. The versions of IIS supported on the OS platforms are:

- Windows NT Server: IIS 4.0
- Windows 2000: IIS 5.0
- Windows XP Professional: IIS 5.1

Web browser support

The following web browsers are supported to access OTM:

- Internet Explorer 6.0 with SP 1 (Windows only)
- Netscape Communicator 4.79 (UNIX only)
- Netscape Communicator 4.79 is required on the OTM server/standalone to retrieve the certificate needed for configurations requiring LDAP SSL connection.

Note: It is not recommended to run more than one web client from Windows 2000 Professional or Windows XP Professional.

Hardware requirements

Hardware requirements for OTM 2.1 are as follows:

Table 51
OTM 2.1 Hardware Requirements (Part 1 of 2)

	Server Configuration	Single (stand alone) Configuration	Client Configuration
Recommended CPU	Intel Pentium III Processor 600 MHz	Intel Pentium III Processor 400 MHz (600 MHz for XP)	Intel Pentium III Processor 400 MHz (600 MHz for XP)
Minimum CPU	Intel Pentium III Processor 400 MHz	Intel Pentium II Processor 233 MHz (PIII 400 MHz for XP)	Intel Pentium II Processor 233 MHz (PIII 400 MHz for XP)
Recommended RAM	512 MB	256 MB, 512 MB for Windows XP	256 MB, 512 MB for Windows XP
Minimum RAM	256 MB	128 MB 256 MB for billing applications, or for Windows XP	128 MB, 256 MB for Windows XP
Hard Drive Space	2 GB (1 GB plus customer data storage)	2 GB (1 GB plus customer data storage)	500 MB
SVGA Color Monitor and interface card	800 X 600 or higher Resolution	800 X 600 or higher Resolution	800 X 600 or higher Resolution
3 1/2-inch 1.44 MB floppy disk drive	Required	Required	Required
CD-ROM drive	Required	Required	Required

Table 51
OTM 2.1 Hardware Requirements (Part 2 of 2)

	Server Configuration	Single (stand alone) Configuration	Client Configuration
Ethernet Network Interface Card	1 or 2	1	1
Hayes compatible modem is optional for connection to remote sites, required for polling configurations. Please note: "WinModems" are incompatible and therefore are not supported.	56K BPS recommended	56K BPS recommended	56K BPS recommended
PC COM port with 16550 UART	Required	Required	Required
Parallel printer port (configured) or USB port (required for dongle)	Required	Required	Required
Two button Windows compatible mouse or positioning	Required	Required	Required

USB dongle

OTM 2.1 supports the USB dongle for Windows 2000 Server, Windows 2000 Professional, and Windows XP Professional as well as the onboard parallel port dongle. As in previous releases, USB dongles are not supported on Windows NT Server.

Dongle requirements are unchanged from previous releases, with the following additions:

- Only one dongle can be connected to an OTM server. A dongle connected to a USB port at the same time as one connected to a parallel port is not supported. Two USB dongles connected at the same time are not supported.
- USB dongles are not supported by connecting through a USB hub. USB dongles must be connected to USB ports on the motherboard or on USB PCI cards.

OTM Navigator dialog boxes

When operating OTM 2.1, Navigator interfaces display the following changes in features and functions:

— the **OTM Restore Wizard** shows Survivable systems

— when deleting a phone, the command **Confirm Delete** provides an option to delete the current directory

— for Succession 3.0 Software, the **System Properties** dialog box adds a **Signaling Server present** checkbox

— when performing an Update System, a **Warning** message displays for PE/EPE Blocking

Station Administration

The following features are added to Station Administration functionality:

- Called Party Name Display (CPND)
  - — **Station Graphical view** – drop-down list for Directory Options and a Details button that directly opens the Employee Editor.
  - — **Keys Assignments** – CPND name and Link to Directory feature when the Key type is selected.
  - — **Global Preferences** – sets default behaviour for new DNs and links CPND to directory (available from the Options menu)
- Forms UI

  - — **Form Edit** – drop-down list for Directory Options combining Employee information
  - — **MyForm** – links to Directory feature
- Adding Stations
  - — **Multiple Station Add** – drop-down list for Directory Options and a Details button that directly opens the Employee Editor

OTM Common Services

The OTM Common Services functionality is modified to support:

- parsing new version values from LD 22
- upgrading from X11 Release 25 or earlier to Succession 3.0
- upgrading from X21 Release 2 to Succession 3.0
- downgrading from Succession 3.0 to X11 Releases
- backing up or restoring Succession 3.0 Large and Small Systems
- adding a Succession BCM Billing switch
- updating to Meridian 1 Option 61C CP PII

For full OTM 2.1 operating and installation procedures, refer to the following documentation:

- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230).
- *Optivity Telephony Manager: System Administration* (553-3001-330).

Software Input/Output prompts, responses, and commands

Contents

This section contains information on the following topics:

Introduction

The following tables outline new information included in Meridian 1, Succession 1000, Succession 1000M Software Input/Output: Administration and Maintenance NTPs.

The Numerical list of packages table lists the new software packages for Meridian 1, Succession 1000, Succession 1000M.

Overlays containing new commands, prompts, and responses for Meridian 1, Succession 1000, Succession 1000M Software Input/Output: Administration and Maintenance are 11, 15, 17, 20, 21, 23, 32, 81, 96, 117, and 135.

Numerical list of packages

Table 52
Numerical list of packages

Number	Mnemonic	Name
394	OAS	Observe Agent Security
393	UUI	Call Center Transfer Connect
397	ICON_PACKAGE	M3900 Full Icon Support
398	PCA	Personal Call Assistant
396	M3900_RGA_PROG	M3900 Ring Again
382	VO	Virtual Office
387	VOE	Virtual Office Enhancement
399	H323_VTRK	H323 Virtual Trunk

LD 11: Meridian Digital Telephone Administration

Prompts and responses

Prompt	Response	Comment
REQ:	NEW CHG	New or Change.
TYPE:	aaaa	Telephone type aaaa = SL1, 2006, 2008, 2009, 2016, 2018, 2112, 2216, 2317, 2616, 3000, 390X, i2002, i2004
	PCA	Personal Call Assistant
	PCAA	Personal Call Assistant in Active Mode (SIMRING)
...		
CLS	SPV	Supervisor Class of Service
	(OUSD) OUSA	Observe Using SCL Denied Observe Using SCL Allowed
...		
KEY	xx AGT zzzz	Agent key with Position ID
	xx OBV	Observe key
	xx OBV yy	Observe key with Speed Call List number

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
CLS	SPV	Supervisor Class of Service	oas-3.0
	(OUSD) OUSA	Observe Using SCL Denied Observe Using SCL Allowed	
KEY	xx OBV	Observe key	oas-3.0

Prompt	Response	Comment	Pack/Rel
	xx OBV yy	Observe key with Speed Call List number	oas-3.0
TYPE:	PCA	Terminal type: Personal Call Assistant	pca-3.0
	PCAA	Terminal type: Personal Call Assistant in Active Mode (SIMRING)	pca-3.0

LD 15: Customer Data Block

Prompts and responses

Prompt	Response	Comment
REQ:	NEW CHG	New or Change.
TYPE:	MON_DATA	Subsequent prompts for MON_DATA are displayed. MON_DATA is prompted for type CDB after LDN_DATA.
PCA		Personal Call Assistant
	(OFF) ON	Disable or enable Personal Call Assistant at Customer level.
		Note: Configuration of the PCA is preserved and allowed regardless of whether the feature is enabled.
USBM		UIPE (Universal ISDN Protocol Engine) Set-based monitoring, where:
	(NO) YES	(NO) = all previously configured TNs are flushed, and subsequent prompts are not prompted. YES = accept and prompt the next prompts. <CR> = previously stored value taken.
TN1		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
TN2		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems

Prompt	Response	Comment
TN3		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
TN4		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
TN5		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
TN6		Terminal Number
	l s c u	For Large Systems
	c u	For Small Systems and Succession 1000 systems
OPT		Options
	PCAR	Personal Call Assistant Restricted.
	PCAU	Personal Call Assistant Unrestricted.
TPDN	yyy.y	Target PCA DN
		Note 1: TPDN is prompted only if PCA is set to ON.
		Note 2: If there is no DN configured against the HOT P key in Overlay11, this value is used to extend the call using the PCA feature.
VPNI		Virtual Private Network Identifier for Bandwidth Management feature.
	(0) - 16383	0 or X = disable feature 1 - 16383 = enable feature <cr> = no change

Data Block: NET (Networking)

Prompts and responses

Prompt	Response	Comment
REQ:	CHG	Change existing data block
TYPE:	NET_DATA	Networking
...	...	...
VNR	(NO) YES	Vacant Number Routing
...	...	...
- UDPL	1 - (19)	Flexible length of Vacant Number Routing (VNR) Uniform Dialing Plan digits (UDP). Enter the maximum number of UDP digits expected by VNR.

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
OPT		Options	
	PCAR	Personal Call Assistant Restricted.	
	PCAU	Personal Call Assistant Unrestricted.	
PCA		Personal Call Assistant	pca-3.0
	(OFF) ON	Disable or enable Personal Call Assistant at Customer level. ***Note:*** Configuration of the PCA is preserved and allowed regardless of whether the feature is enabled.	

Prompt	Response	Comment	Pack/Rel
TPDN	yyy.y	Target PCA DN ***Note 1:*** TPDN is prompted only if PCA is set to ON. ***Note 2:*** If there is no DN configured against the HOT P key in Overlay11, this value is used to extend the call using the PCA feature.	pca-3.0
TN1	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TN2	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TN3	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TN4	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TN5	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TN6	 l s c u c u	Terminal Number For Large Systems For Small Systems and Succession 1000 systems	
TYPE:	MON_DATA	Subsequent prompts for MON_DATA are displayed. MON_DATA is prompted for type CDB after LDN_DATA.	basic-1
UDPL	1 - (19)	Flexible length of Vacant Number Routing (VNR) Uniform Dialing Plan digits (UDP). Enter the maximum number of UDP digits expected by VNR.	

Prompt	Response	Comment	Pack/Rel
USBM	(NO) YES	UIPE (Universal ISDN Protocol Engine) Set-based monitoring, where: (NO) = all previously configured TNs are flushed, and subsequent prompts are not prompted. YES = accept and prompt the next prompts. <CR> = previously stored value taken.	basic-3.0
VPNI	(0) - 16383	Virtual Private Network Identifier for Bandwidth Management feature. 0 or X = disable feature 1 - 16383 = enable feature <cr> = no change	basic-2

LD 17: Configuration Record 1

Gate Opener: OVLY (Overlay)

Prompt	Response	Comment
REQ	CHG	Change existing data block.
TYPE	OVLY	Change Overlay area options
...		
-TODR	0-23	Time of Daily Routines
-MID_SCPU	(NO) YES	Midnight Switch Cores Deny or allow Midnight Switch Core, where: Deny causes the system to perform the 3PE test during the Midnight routine instead of switching CPUs. Allow causes the system to switch CPUs during the Midnight routine instead of performing the 3PE test. ***Note:*** Applicable to CPP systems only.

Gate Opener: PARM (System Parameters)

Prompt	Response	Comment
REQ	CHG	Change existing data block.
TYPE	PARM	System parameters
...		
PCDR	(NO) YES	Priority to CDR

Prompt	Response	Comment
ICON	(NO) YES	Disable or enable M3900 Full ICON Support.
RCAP		Remote Capabilities
	UUI	User to User Signaling is Enabled.
	XUU	User to User Signaling is Disabled.

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
ICON	(NO) YES	Disable or enable M3900 Full ICON Support.	ICON_PACKAGE-3.0
-MID_SCPU		Midnight Switch Cores	CPP_CNI - 3.0
	(NO) YES	Allow or deny Midnight Switch Core, where: Deny causes the system to perform the 3PE test during the Midnight routine instead of switching CPUs. Allow causes the system to switch CPUs during the Midnight routine instead of performing the 3PE test. ***Note:*** Applicable to CPP systems only.	
RCAP		Remote Capabilities	UUI-3.0
	UUI	User to User Signaling is Enabled.	
	XUU	User to User Signaling is Disabled.	

LD 20: Print Routine 1

Prompts and responses

Prompt	Response	Comment
REQ	PRT	Print
TYPE	PCA	Personal Call Assistant
...		
FOR	i2004 i2050	Internet Telephone Software Telephone

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
FOR	i2004 i2050	Internet Telephone Software Telephone	basic-3.0
TYPE	PCA	Personal Call Assistant	pca-3.0

LD 21 Print Routine 2

Prompts and responses

Prompt	Response	Comment
REQ:	PRT	Print data block for the TYPE specified.
TYPE:	MON_DATA	Print Monitor data

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
TYPE	MON_DATA	Print Monitor data	basic-3.0

LD 23: Automatic Call Distribution, Management Reports, Message Center

Prompts and responses

Prompt	Response	Comment
REQ	NEW CHG	New or Change.
TYPE	OBVP	Observe Password table
CUST		
ADPD	xx..xx yy..yy	Supervisor's Agent ID and Password Supervisor login ID followed by Supervisor Observe password.
...		
OBSC	(NO) YES	Login/Logout Control
OBPT	2-(5)-99	Supervisor Inactivity Timer
...		
UUI	(NO) YES	Allow or deny User to User Information.

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
ADPD	xx..xx yy..yy	Supervisor's Agent ID and Password Supervisor login ID followed by Supervisor Observe password.	
OBPT	2-(5)-99	Supervisor Inactivity Timer	
OBSC	(NO) YES	Allow or deny Security option.	
UUI	(NO) YES	Allow or deny User to User Information.	UUI-3.0

LD 32: Network and Peripheral Equipment Diagnostic

Alphabetical list of commands

Command	Description	PACK/REL
ECNT CARD L S C <customer>	This command prints the number of Internet Telephones registered for the specified card. • If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter. A customer cannot be specified in this case. Example: ecnt card 81 << Card 81 >> Number of Register Ethersets: 5 Number of Unregistered Ethersets: 27	basic-3.0
ECNT NODE nodeNum	This command prints the number of Internet Telephones registered for the specified node. • If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ecnt node 8765 << Zone 8765 >> Number of Register Ethersets: 3	basic-3.0

Command	Description	PACK/REL
ECNT SS hostName	This command prints the number of Internet Telephones registered for the specified Signaling Server. • If hostName parameter is not entered, the count is printed for all signaling servers. Example: ecnt ss << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Register Ethersets: 1000	basic-3.0
ECNT ZONE zoneNum <customer>	This command prints the number of Internet Telephones registered for the specified zone. • If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. Example: ecnt zone 0 0 << Zone 0 Customer 0 >> Number of Register Ethersets: 4 Number of Unregistered Ethersets: 17	basic-3.0

LD 81: Features and Station Print

Prompts and responses

Prompt	Response	Comment
REQ	LST	List
CUST	xx	Customer Number
...		
FEAT		Features requested
	PEPE	Print all TNs and cards configured on the PE/EPE shelves.

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
FEAT	PEPE	Print all TNs and cards configured on the PE/EPE shelves.	basic-3.0

LD 96: D-channel Diagnostic

Alphabetical list of commands

Command	Description	PACK/REL
DIS MSGI <dch>	DEBG CH <loop><channel>	basic-3.0
	Disable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	
DIS MSGI <dch>	DEBG MSG msg1 msg2 msg3	basic-3.0
	Disable the debugging of all monitored incoming messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.	
DIS MSGI <dch>	DEBG SET	basic-3.0
	Disable debug SET on all incoming messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	
DIS MSGI <dch>	SET	basic-3.0
	Disable SET on all incoming messages from D-channel This set based filtering is enhanced for UIPE proprietary messages.	
DIS MSGO <dch>	DEBG CH <loop><channel>	basic-3.0
	Disable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	

Command	Description	PACK/REL
DIS MSGO <dch> DEBG MSG msg1 msg2 msg3	Disable the debugging of all monitored outgoing messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.	basic-3.0
DIS MSGO <dch> DEBG SET	Disable debug SET on all outgoing messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	basic-3.0
DIS MSGO <dch> SET	Disable SET on all outgoing messages from D-channel This set based filtering is enhanced for UIPE proprietary messages.	basic-3.0
ENL MSGI <dch> DEBG CH <loop><channel>	Enable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	basic-3.0
ENL MSGI <dch> DEBG MSG msg1 msg2 msg3	Enable the debugging of all monitored incoming messages from D-channel This command can be entered more than once. In one command, only 3 message mnemonics can be given.	basic-3.0
ENL MSGI <dch> DEBG SET	Enable debug SET on all incoming messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	basic-3.0

Command	Description	PACK/REL
ENL MSGI <dch> SET		basic-3.0
	Enable SET on all incoming messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	
ENL MSGO <dch> DEBG CH <loop><channel>		basic-3.0
	Enable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.	
ENL MSGO <dch> DEBG MSG msg1 msg2 msg3		basic-3.0
	Enable the debugging of all monitored outgoing messages from D-channel This command can be entered more than once. Only 3 message mnemonics can be given in one command.	
ENL MSGO <dch> DEBG SET		basic-3.0
	Enable debug SET on all outgoing messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	
ENL MSGO <dch> DEBG SET		basic-3.0
	Enable debug SET on all outgoing messages from D-channel. This set based filtering is enhanced for UIPE proprietary messages.	

LD 117: Ethernet and Alarm Management

Command	Description	PACK/REL
CHG ZBRN<Zone><a...a>	Define a zone as a Branch Office zone, where: a...a = Yes or No	
CHG ZACB <Zone>[ALL] [<AC1...AC2> <AC1...AC2>]	Define the access codes used to modify local calls in the Branch Office zone, where: • ALL = both AC1 and AC2 receive digit manipulation and no re-translation occurs • AC1 = the first Access Code parameter defines which NARS Access Code to consider as the source of local calls • AC2 = the second Access Code parameter defines which NARS Access Code to send the modified number to for retranslation. If NARS is configured as recommended in the NTPs, this would be AC2 for local call and AC1 for retranslation.	

Command	Description	PACK/REL
CHG ZDP <Zone> <DialingCode1> <DialingCode2> <DialingCode3>	Define the dialing plan for the Branch Office zone, where: • DialingCode1: Prefix, represents the access code for long distance or international access. In North America, it is "1" for long distance access and "011" for international access. Outside North America, it is "0" for national access and "00" for international access. • DialingCode2: The country code or trunk code. Normally NPA when calling from within North America, and "1" when calling from outside North America. • DialingCode3: Destination network code. Normally not used in North America. Outside North America, it is a combination of region, city, or district codes.	
CHG ZESA <Zone> <ESARLI> <ESAPrefix> <ESALocator>	Defines the Emergency Services Access (ESA) parameters for the Branch Office zone. These parameters are only used if the ESA package is enabled. Where: • ESARLI = the route to use to send emergency calls to the Branch Office Gateway by way of the VTRK • ESAPrefix = a digit string of up to 15 digits that is added to the start of the ESDN before it is sent to the route indicated by the ESARLI. This allows the Gatekeeper to differentiate the different destinations for otherwise identical ESDN's. • ESALocator = the DID phone number to be sent for use by the PSAP to locate the source of the emergency call.	

Command	Description	PACK/REL

CHG ZDST <Zone> a...a <StartMonth> <StartWeek> <StartDay> <StartHour> <EndMonth> <EndWeek> <EndDay> <EndHour>

Specifies whether the Branch Office zone observes daylight savings time. Where:

- a...a = Yes or No, During daylight saving time, the clock automatically advances one hour forward.
- StartMonth = start month of year (1-12)
- StartWeek = start week in month (1-5)
- StartDay = start day in week (1-7)
- StartHour = start hour of day (1-23) of the start of DST
- EndMonth = end month of year (1-12)
- EndWeek = end week in month (1-5)
- EndDay = end day in week (1-7)
- EndHour = end hour of day (1-23) of the end of DST.

In North America, DST normally starts on the 1st Sunday in April at 2am and ends on the last Sunday in October at 2am.

CHG ZTDF <Zone> <TimeDifferenceFromHeadOffice>

Specify the time difference between the Main Office and the Branch Office when both are not in Daylight Saving Time. The time difference is specified in minutes and the range is from -1380 to 1380 minutes. (Minus 23 hours to plus 23 hours.)

CHG ZDES <Zone> <ZoneDescription>

Assign the Zone a descriptive name (ZoneDescription) that is only used in the data display and status commands to make the zone numbers more meaningful.

PRT ZBW [<Zone>]

Print a table of zone bandwidth utilization.

Command	Description	PACK/REL

PRT ZACB [<Zone>]

Print a table of Branch Office zone dialing plan entries.

PRT ZONE [<Zone>]

Print zone information for specified zones.

Sample output:

```
_____________________________________________________________________________
_
|     |       |       Intrazone            |          Interzone            |    |
|Zone |State  |----------------------------------------------------------|MO/ |
|     |       |BandWidth|Strategy| Usage |Peak|BandWidth|Strategy|Usage |Pea |SBO |
|     |       | (Kbps)  |        | (Kbps)| %  | (Kbps)  |        |(Kbps)| %  |    |
|-----------------------------------------------------------------------------|
|  0  | ENL | 1000000 | BQ     | 0     | 0  | 1000000 | BQ     | 0    | 0  | MO |
|-----------------------------------------------------------------------------|
|  20 | ENL | 10000   | BQ     | 0     | 0  | 10000   | BQ     | 0    | 0  | SBO|
|-----------------------------------------------------------------------------|
Number of Zones configured = 2
```

Command	Description	PACK/REL

PRT ZBW [<Zone>]

Print a table of zone bandwidth utilization.

Sample output:

```
_____________________________________________________________________________
_
|         |       |         Intrazone             |                Interzone   |
|  Zone   |State |-------------------------------------------------------------
|         |       |BandWidth|Strategy| Usage|Peak|BandWidth|Strategy|Usage |Peak|
|# DES    |       |  (Kbps) |        |(Kbps)| %  | (Kbps)  |        |(Kbps)| %  |
|-----------------------------------------------------------------------------
|0 Default | ENL  | 1000000  | BQ     | 0    | 0  | 1000000| BQ     | 0    | 0  |
|   Zone   |      |
|-----------------------------------------------------------------------------
|20       | ENL  | 10000    | BQ     | 0    | 0  | 10000   | BQ    | 0    | 0  |
|-----------------------------------------------------------------------------
|
Number of Zones configured = 2
```

Command	Description	PACK/REL

PRT ZDES [<DESMatchString>]

Print a table of the zone description entries.

Sample output:

```
_____________________________________________________________________________
_
|   |                                                                         |
| # |DES                                                                      |
|   |                                                                         |
|   |                                                                         |
|-------------------------------------------------------------------------------
|
| 0 |THE_DEFAULT_ZONE                                                         |
|-------------------------------------------------------------------------------
|
| 20|BRANCH-5566_BELLEVILLE_ON                                                |
|-------------------------------------------------------------------------------
|
Number of Zones configured = 2
```

PRT ZDST [<Zone>]

Print a table of Branch Office zone time adjustment properties entries.

PRT ZTDF [<Zone>]

Print a table of Branch Office zone time adjustment properties entries.

Command	Description	PACK/REL

PRT ZESA [<Zone>]

Print a table of Branch Office zone Emergency Services Access (ESA) entries.

Sample output:

```
_____________________________________________________________________
|                             |         | Emergency Services Access    |
| Zone                        |State    |--------------------------    |
| |                           |         |Route|     |PrePend|          |
| # DES |                     |         | #   | AC  |Digits | Locator  |
|-------------------------------------------------------------------|
| 10 BRANCH-4439_FREDERICTON,NB| DIS    | 68  | AC1|506    |5065552211 |
|-------------------------------------------------------------------|
| 20 BRANCH-5566_BELLEVILLE,ON | DIS    | 0   |None|       |           |
|-------------------------------------------------------------------|
| 30 BRANCH-6872_VANCOUVER,BC  | ENL    | 77  |AC1 |604    |604551122  |
|-------------------------------------------------------------------|
Number of Branch Office Zones with ESA Active = 1
Number of Branch Office Zones configured = 3
Number of Zones configured = 4 |6045551122 |
```

Command	Description	PACK/REL

PRT ZDP [<Zone>], or PRT ZACB [<Zone>]

Print a table of Branch Office zone dialing plan entries

Sample output:

```
_____________________________________________________________________________
_
|                                |      |Dialing Codes and Access Code Behaviour|
| Zone                           |State |---------------------------------------|
|                                |      |Dialing |Dialing |Dialing |Local | LD  |
| # DES                          |      |Code 1  |Code 2  |Code 3  | AC   | AC  |
|--------------------------------------------------------------------------------
|
| 10 BRANCH-4439_FREDERICTON,NB | DIS | 1      | 506    | None   | AC1  | AC2 |
|--------------------------------------------------------------------------------
|
| 20 BRANCH-5566_BELLEVILLE,ON  | ENL | 1      | 613    | None   | AC1  | AC2 |
|--------------------------------------------------------------------------------
|
| 30 BRANCH-6872_VANCOUVER,BC   | ENL | 1      | 604    | None   | AC1  | AC2 |
|--------------------------------------------------------------------------------
|
Number of Branch Office Zones with Local Dialing Active = 2
Number of Branch Office Zones configured = 3
Number of Zones configured = 4
```

PRT ZTP [<Zone>], or PRT ZTDF [<Zone>], or PRT ZDST [<Zone>]

Print a table of Branch Office zone time adjustment properties entries.

Sample output:

Command	Description	PACK/REL

```
_____________________________________________________________________________
|                                 |       |       Time Change Properties      |
| Zone                            |State  |-----------------------------------|
|                                 |       |USE|DST| DST Start | DST End   | Time |
| # DES                           |       |DST|ACT| mm w d hh | mm w d hh | Diff |
|---------------------------------------------------------------------------|
|10 BRANCH-4439_FREDERICTON,NB    | ENL   |Yes|No |  4 1 1 2  | 10 4 1 2  | 60   |
|---------------------------------------------------------------------------|
|20 BRANCH-5566_BELLEVILLE,ON     | DIS   |No |No |  0 0 0 0  | 0 0 0 0   | 0    |
|---------------------------------------------------------------------------|
|30 BRANCH-6872_VANCOUVER,BC      | ENL   |Yes|No |  4 1 1 2  | 10 4 1 2  | -180 |
|---------------------------------------------------------------------------|
Number of Branch Office Zones with Time Change Active = 2
Number of Branch Office Zones configured = 3
Number of Zones configured = 4
```

ENL ZBR <Zone> [ALL] [LOC] [ESA] [TIM]

Enable features for the Branch Office zone. If no specific features are specified, then ALL is assumed.

DIS ZBR <Zone> [ALL] [LOC] [ESA] [TIM]

Disable features of the Branch Office zone. If no specific features are specified, then ALL is assumed.

Command	Description	PACK/REL

STAT ZONE [<Zone>]

Display zone status table.

```
_____________________________________________________________
|   |       |       |                                       |
| # |State  | Flags |DES                                    |
|   |       |       |                                       |
|   |       |       |                                       |
|-----------------------------------------------------------|
| 0 | ENL   |       |THE_DEFAULT_ZONE                       |
|-----------------------------------------------------------|
| 10| ENL   |Br     |BRANCH-4439_FREDERICTON,NB             |
|-----------------------------------------------------------|
| 20| ENL   |Br     |BRANCH-5566_BELLEVILLE,ON              |
|-----------------------------------------------------------|
| 30| ENL   |Br     |BRANCH-6872_VANCOUVER,BC               |
|-----------------------------------------------------------|
Number of Zones configured = 4 (0 disabled)
Number of Branch Office Zones configured = 3 (0 disabled)
```

STAT ZBR [<Zone>]

Display status of Branch Office zones (displays which local dialing)

Sample output:

```
_____________________________________________________________
|   |      |              |                                  |
| # |State | Flags        |DES                               |
|   |      |              |                                  |
|   |      |              |                                  |
|-----------------------------------------------------------|
| 10| ENL |TIM            |BRANCH-4439_FREDERICTON,NB        |
|-----------------------------------------------------------|
| 20| ENL |LOC            |BRANCH-5566_BELLEVILLE,ON         |
|-----------------------------------------------------------|
| 30| ENL |ESA LOC TIM    |BRANCH-6872_VANCOUVER,BC          |
-------------------------------------------------------------
Number of Zones configured = 4 (0 disabled)
Number of Branch Office Zones configured = 3 (0 disabled)
```

Command	Description	PACK/REL
STAT LINK APP <applicationType>	Display the link information status of the server for the specified application. Where: applicationType = LTPS (Line TPS), VGW (Voice Gateway), H323 (H.323 Virtual Trunk), GK (GateKeeper)	
STAT LINK IP <IP address>	Display the link information status of the server for the specified IP address, or IP addresses of the specified sub-net. Where: IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card ***Note:*** The IP address can be in full or partial IP address format (e.g., "10.11.12.13" or "10.11").	
STAT LINK NAME <hostName>	Display the link information status of the servers based on the supplied host nam. Where: hostName = MAINSERVER	
STAT LINK NODE <nodeID>	Display the link information status of the specified node. Where: nodeID = a number from 0 - 9999 ***Note:*** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.	

Command	Description	PACK/REL
STAT LINK SRV <serverType>	Display the link information status of the servers for the specified server type. Where: serverType = ITGP (ITG Pentium), SMC (Succession Media Card), SS (Signaling Server)	
STAT SERV APP <applicationType>	Display the link information status of the server for the specified application. Where: applicationType = LTPS (Line TPS), VGW (Voice Gateway), H323 (H.323 Virtual Trunk), GK (GateKeeper)	
STAT SERV IP <IP address>	Display the link information status of the server for the specified IP address, or IP addresses contained in the specified sub-net. Where: IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. ***Note:*** The IP address can be in full or partial IP address format (e.g., “10.11.12.13” or “10.11”).	
STAT SERV NAME <hostName>	Display the link information status of the servers based on the supplied host name. Where: hostName = MAINSERVER	

Command	Description	PACK/REL
STAT SERV NODE <nodeID>	Display the link information status of the specified node. Where: nodeID = a number from 0 - 9999. The nodeID identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.	
STAT SERV TYPE <serverType>	Display the server information of the specified server type. Where: serverType = ITGP (ITG Pentium), SMC (Succession Media Card), or SS (Signaling Server)	
STIP HOSTIP <IP address>	Displays information contained in the rlm table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net. Where: IP address = the TLAN IP address of the set or vgw. ***Note:*** IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.	

Command	Description	PACK/REL
STIP NODE <nodeID>	Display information contained in the resource locator module table corresponding to the specified node ID. Where: nodeID = a number from 0 - 9999. The nodeID identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.	
STIP TERMIP <IP address>	Display information contained in the resource locator module table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net. Where: IP address = the TLAN IP address of the Internet Telephone or Voice Gateway Media Card. ***Note:*** IP address can be in full or partial IP address format. For example, “10.11.12.13”, or “10.11”.	
STIP TN l s c u	Display the resource locator module information for the specified TN, or group of TNs, as denoted by the l s c u parameters for large systems, and the c u parameters for small systems.	

Command	Description	PACK/REL
STIP TYPE <aaa>	Display the resource locator module information for the specified TN type, where up to 3 types can be specified. Valid types are: i2002 = i2002 sets i2004 = i2004 sets i2050 = i2050 sets ISET = all IP sets VGW = Voice Gateway resources IPTI = Virtual Trunk and IP Trunks	
STIP ZONE <zone>	Display the resource locator module information for the specified zone number, or range of zones. Where: zone = any valid zone number (0 - 255) in the system.	

LD 135: Core Common Equipment Diagnostic

Prompts and responses

Commands	System Response	Description
STAT HEALTH		Display Tier 1 and 2 health counts and the status of the hardware components that do not have a health weight.
STAT HEALTH AML		Display the health count of the configured ELAN connections to AML applications.
STAT HEALTH ELAN		Display Tier 2 health count.
STAT HEALTH HELP		Display the meaning of the mnemonics used for the hardware components.
STAT HEALTH HW		Display Tier 1 health count and the status of the hardware components that do not have a health weight.
STAT HEALTH IPL		Display the health count of the IPL connections.

Alphabetical list of prompts

Commands	Description	Pack/Rel
STAT HEALTH	Display Tier 1 and 2 health counts together with the status of the hardware components that do not have a health weight.	basic-3.0
STAT HEALTH AML	Display the health count of the configured ELAN connections to AML applications.	basic-3.0
STAT HEALTH ELAN	Display Tier 2 health count.	basic-3.0

Commands	Description	Pack/Rel
STAT HEALTH HELP	Display the meaning of the mnemonics used for the hardware components.	basic-3.0
STAT HEALTH HW	Display Tier 1 health count together with the status of the hardware components that do not have a health weight.	basic-3.0
STAT HEALTH IPL	Display the health count of the IPL connections.	basic-3.0

System messages

The following system error messages are new for Succession 3.0:

AUD: Software Audit

AUD0094 x y z	Loop with no physical timeslots is marked with faulty timeslots. May cause AUD0017 or AUD0018 Parameter 1 = loop Parameter 2 = TSEFAULTWORD Parameter 3 = TSOFAULTWORD
AUD0095	Audit message for printing diagnostic information related to ISA MIN-MAX
AUD0096	DWC; ACD Calls Waiting show very large numbers, related to CCR

BUG: Software Error Monitor

BUG0102	User has been registered at Branch Office for more than 2 weeks. **Action:** Force to disconnect and redirect to Main Office.
BUG0113	Unit type configured on PBX card is not defined, due to possible corruption.
BUG0116	AML: Could not register <mod_name> **Action:** Contact technical support.
BUG0117	AML: Could not send to Comm Manager. **Action:** Contact technical support.
BUG0118	AML: Tying to send null message.

Action: Contact technical support.

BUG0119 AML: Null message received.

Action: Contact technical support.

BUG0121 AML: Could not send to amlMsgQId.

Action: Contact technical support.

BUG0122 AML: Could not create amlAppSem.

Action: Contact technical support.

BUG0123 AML: Could not create amlMsgQId.

Action: Contact technical support.

BUG0124 AML: Could not re-create amlMsgQId.

Action: Contact technical support.

BUG0126 AML: Error deleting amlMsgQId.

Action: Contact technical support.

BUG0127 AML: Could not send update health message to the other side.

Action: Contact technical support.

BUG0128 AML: Could not send add application message to the inactive side.

Action: Contact technical support.

BUG0129 AML: Could not send delete application message to the inactive side.

Action: Contact technical support.

BUG0131 On-hook from AUTOVON trunk in AWAIT-REPLY state. Procedure TRUNKS/EM_DX_TRUNK

BUG0132 AML: Wrong message received of type <type>.

Action: Contact technical support.

BUG0133 AML: Failed to init task.

Action: Contact technical support.'

BUG0134 AML: Failed to recover task.

Action: Contact technical support.

BUG0136 AML: Task spawn failed.

Action: Contact technical support.

BUG0137 STATION_INDEX for single appearance 500 set should not exceed 1.

Procedure: SC_FIX_CR

Output: STATION_INDEX

Action: Save a hard copy of the BUG printout and contact technical support.

BUG0149 DR: Disk synchronization has failed due to an unknown message [type = 0x%x] received.

Action: Contact technical support.

BUG0154 SEG: invalid size [x] requested, where *x* is the size requested.

Action: Contact technical support.

BUG0156 SEG: invalid block to be freed: ptr [x], header ptr [y], where *x* is the pointer to the block and *y* is the header pointer to the block.

Action: Contact technical support.

BUG0157 SEG: invalid block to be freed: ptr [x], header ptr [y] magic [z], where *x* is the pointer to the block, *y* is the header pointer to the block, and *z* is the magic cookie for the block.

Action: Contact technical support.

BUG0158 SEG: Function [x] called, where *x* is the name of the function.

BUG0159 SEG: No free space to be allocated.

Action: Contact technical support.

BUG0162 SEG: semMCreate failed during initialization.

Action: Contact technical support.

BUG0163 SEG: Failed to get vm state at page addr [a] for addr [b], where *a* is the page boundary address and *b* is the memory address.

Action: If messages persists, contact technical support.

BUG0164 SEG: Failed to set vm state at page addr [a] for addr [b], where *a* is the page boundary address and *b* is the memory address.

Action: If messages persists, contact technical support.

BUG0169 SWO: failed to initialize tSwoTask, errno [err].
Action: Contact your Technical Support.

BUG0171 SWO: Failed to activate SWO task.
Action: Contact your Technical Support.

BUG0172 SWO: Failed to send to swoMsgQId, errno [err].
Action: Contact your Technical Support.

BUG0173 SWO: Failed to create swoMsgQId, errno [er].
Action: Contact your Technical Support.

BUG0174 SWO: failed to register with Communication Manager.
Action: Contact your Technical Support.

BUG0176 SWO: failed to receive from swoMsgQId [msgQID], errno[err].
Action: Contact your Technical Support.

BUG0177 SWO: failed to stop all HI periodic jobs.

BUG0178 SWO: failed to start all HI periodic jobs.

BUG0179 SWO: failed to send to lcsMsgQId.
Action: Contact your Technical Support.

BUG0182 SWO: Received unknown message of type %d.
Action: Contact your Technical Support.

BUG0183 LCS: Can't stop SL1 task.
Action: Contact your Technical Support.

BUG0184 IPM: Failed to assign the HSP IP address to fei1 in ipmPostSwo.
Action: Contact your Technical Support.

BUG0186 SWO: Stop And Copy failed.
Action: Check the HSP.

BUG0187 LCS: Can't proceed with graceful switchover. Can't stop SL1 task.
Action: Contact your Technical Support.

BUG0188 LCS:Graceful switchover unsuccessful. Inactive side failed to receive the SWO message.

Action: Contact your Technical Support.

BUG0189 LCS: Graceful switchover unsuccessful. Stop&Copy failed and LcsSCFail message lost.

Action: Contact your Technical Support.

BUG0192 CM: HSP init failed.

Action: Contact your Technical Support.

BUG0193 Failed to start task [%s], errno: [err].

Action: Contact your Technical Support.

BUG0197 Sending to %s [msgQID] failed, errno: [err].

Action: Contact your Technical Support.

BUG0198 CM: Secondary server ether socket bind fail.

Action: Contact your Technical Support.

BUG0199 Failed to create %s message queue, errno: [err].

Action: Contact your Technical Support.

BUG0202 Failed to delete %s [semaphoreID] semaphore, errno:[err].

Action: Contact your Technical Support.

BUG0203 CM: Secondary server socket receive Error.

Action: Contact your Technical Support.

BUG0204 cmPriProcessMsg: CM dispatch local message fail, Destination is [%d].

Action: Contact your Technical Support.

BUG0206 Failed to delete %s [0x%x], errno: [err].

Action: Contact your Technical Support.

BUG0207 CM: Can't create cmSockClntSem semaphore.

Action: Contact your Technical Support.

BUG0208 CM: HSP Server init failed.

Action: Contact your Technical Support.

BUG0209 CM: HSP Server accept failed.

Action: Contact your Technical Support.

BUG0212 CM: Create %s socket failed.

Action: Contact your Technical Support.

BUG0213 CM: setsockopt error.

Action: Contact your Technical Support.

BUG0214 Receive from %s [0x%x] failed, errno [err].

Action: Contact your Technical Support.

BUG0216 CM: Can't Get remote IP.

Action: Contact your Technical Support.

BUG0217 CM: Can't Get local current IP.

Action: Contact your Technical Support.

BUG0218 CM: Can't Get remote Default IP.

Action: Contact your Technical Support.

BUG0219 CM: Secondary client can't Send to [%s]:[%d].

Action: Contact your Technical Support.

BUG0222 CM: Secondary client received bad message.

Action: Contact your Technical Support.

BUG0223 CPM: Invalid usage of the cmPrimarySend function.

Action: Contact your Technical Support.

BUG0224 CM: Detected message that is larger than primary connection's MTU.

Action: Contact your Technical Support.

BUG0226 Detected invalid message destination on primary connection.

Action: Contact your Technical Support.

BUG0227 cpmInit: deleting cpm task tCpmS.

Action: Contact your Technical Support.

BUG0228 malloc failed.

	Action: Contact your Technical Support.
BUG0234	HIREM: Data of object %p, %d bytes, is larger then the maximum size %d HIREM: Invalid msg option passed in hiRemSendCreateObj. **Action:** Contact your Technical Support.
BUG0236	CM: Can't connect to the other side. Create client socket failed. **Action:** Contact your Technical Support.
BUG0237	CM: Shutdown server timeout. **Action:** Contact your Technical Support.
BUG0238	CM: Can't write to the HSP. Client socket error. **Action:** Contact your Technical Support.
BUG0239	CM: Shutdown client timeout. **Action:** Contact your Technical Support.
BUG0243	CM: Can't init HSP Server. Create server socket failed with errno [err].Where [err]: error number. **Action:** Contact your Technical Support.
BUG0244	CM: Can't init HSP Server. Bind server socket failed with errno [err].Where [err]: error number. **Action:** Contact your Technical Support.
BUG0246	CM: Can't init HSP Server. Create cmSockSvrSem semaphore failed. **Action:** Contact your Technical Support.
BUG0247	CM: Can't init HSP Server. Create cmSockSvrSem semaphore failed. **Action:** Contact your Technical Support.
BUG0248	CM: HSP Server accept returned error, errno [err]Where [err]: error number. **Action:** Contact your Technical Support.
BUG0249	Observe is not allowed because OUSA CLS is configured and SCL associated with the OBV key does not exist.
BUG0251	PCA Phones ISM counter corruption encountered. Counter is reset to 0.
BUG0252	TRK_UNIT expected in MFC_COMPLETE.

BUG0253 Utility procedure called with invalid required data. Parameters: global number and optional debugging parameters.

Action: Report the problem text to the operating company.

BUG0254 Unknown bandwidth policy. Possible data corruption.

Action: Check zone table content in OVL117.

BUG0256 Call register ids invalid in IDLECR. Parameters: call register pointer.

Action: Report the problem text to the operating company.

BUG0257 Unable to map phantom loop to a real loop. Procedure FINDONEWAY. Output: TNX, TNY (unpacked format), *(CRPTR).

Action: Please contact technical support group. Go to the PDT and turn enhanced BUG CR printing option on in order to get more detailed BUG output (if the problem occurs again.)

BUG0258 Failed to spawn the tQoSIP task. errno [errno].

Action: Contact your local support group, the system cannot monitor QoS violation events.

BUG0261 Failed to created the qosIPMsgQ message queue. errno [errno].

Action: Contact your local support group, the system cannot monitor QoS violation events.

BUG0262 qosIPMsgQ message queue does not exist, ending the tQoSIP task.

Action: Contact your local support group, the system cannot monitor QoS violation events.

BUG0263 Unexpected message detected message number [msgNum].

BUG0266 ACTIVECR points to the call register that is in the IDLE queue.

Action: Contact technical support.

BUG0267 Protected pointer (DNPTR) is out of protected memory range.

Procedure DNTRANS2.

Output: DN (packed format: low word, hi word), lower bound of protected store, DNPTR, upper bound of protected store, customer number.

Action: Contact technical support.

BUG0268 Unit type is incorrect.
Output: Protected line pointer, unit type

Action: Contact technical support.

BUG0272 A BCS TN block is expected. Procedure SET_IS_2D_BUSY.
Output: packed TN and unit type for dialled N block, packed TN and unit type for terminating TN block, TERTN:CRPTR.

BUG0273 Mis Configured DSC. Location A and Location B has same distance steering code towards each other. The configuration is wrong (Cause Ping Pong). Please change the configuration.

BUG0274 Call register to be idled is found in ACD queue.

BUG0276 Call register to be idled is still linked to IVR CR.

BUG0277 NCFW DN is a combination of (LOC+ACD DN) or (ACOD+ACD DN).

BUG0278 IP Peer H.323 Trunks counter corruption encountered. Counter is reset to zero.

Action: Contact your technical support group.

BUG0279 A non idled DTR is found.

Action: Contact your technical support group.

BUG0281 Timing block pointer is out of range. Parameters: block pointer, queue, timer1, timer2 (queue and timers valid for errors in LINK).

Action: Report problem to the operating company.

BUG0282 Call register has an invalid block type. Parameters: call register pointer, block type, queue.

Action: Report problem to the operating company.

BUG0283 Block pointer is marked as a call register but is not in range. Parameters: block pointer, 7 words of the block header.

Action: Report problem to the operating company.

BUG0284 Timing block not marked as being in a queue contains invalid queue pointers. Parameters: block pointer, block type, forward link, backwards link.

Action: Report problem to the operating company.

BUG0287 ACTIVECR for an attendant console should be unused but contains a value.

Parameters: ACTIVECR, TN, (contents of ACTIVECR).

Action: Report the problem to the operating company.

BUG0288 Call is in ACD queue, but DIGIT_WORDS contains non ACD DN.

BUG0289 The KEYLINK on the Trans key should not be in IDLE state. The LAMP of the Trans key is set to DARK and the KEYLINK is set to nil. TN is printed. Procedure CALL_TRANSFER.

BUG0291 Loop number exceeded it's limits. Procedure: SETTONE.

Action: Contact your technical support group.

BUG0292 FUNC_DATA_PTR returned invalid pointer.

BUG0487 An attempt has been made to write to protected data that is in a block of memory that is unused. Data is not changed.

Parameters: logical page, address, new value, free memory block data (3 words), page_tail, and block count from the tail.

Action: This error indicates one of two errors. Either an incorrect pointer has been used to select an address to write, or a data block has two users. Data corruption is possible. Contact the operating company with the full text of the error message.

BUG2083 IPM: Can't send to CM.

Action: Contact your Technical Support.

BUG5073 % In procedure IDLECR, the destined callregister is already in idle queue.

BUG5136 CRPTR is NIL.

BUG7497 Ethernet initialization failed during the system startup because there has been a failure to correctly obtain network interface data or a failure to initialize the network interface.

Action: Check Ethernet address and network database file.

BUG8037 Warning, incorrect value in TRANSIT_PABX. Call Processing not affected.

BUG8137 VNS, UVNS_DNPTR is corrupt.

Action: Contact your Nortel Networks distributor.

BUG9280 The pointers to the list of free memory were corrupted and have been reset. No memory is available on this page. If this message is for page 0 and is not followed by a BUG9281 then the system is out of memory.

Parameters: page (0 for unprotected, 1 for protected), page head and page tail.

Action: If the page is 0 and BUG9281 is not printed perform a system initialization as soon as possible, without logging in. If the problem is on page 1 and occurs repetitively the system may run out of memory and a system reload will be required. Report the problem to the operating company with the full text of the error message.

BUG9281 Unused unprotected memory was not properly tracked. It has been recovered.

Parameters: page (always 0), address and size of recovered block.

Action: The problem has been corrected. No action is required for a single occurrence. If the error message occurs repetitively data corruption is likely - report the problem to the operating company with the full text of the error message.

BUG9282 Unused protected memory was not properly tracked. The memory will remain unavailable until the next system reload. Tracking is updated to reflect the change.

Parameters: page (always 1), address and size of the unavailable block.

Action: Report the problem to the operating company with the full error printout. If the problem persists the system may run out of memory and a system reload should be performed. A system initialization is unlikely to improve the memory condition.

BUG9283 A block of memory that is marked unused has been corrupted. It is discarded to avoid possible conflicts with a persistent misuse of the memory. The memory will be unusable until the next system initialization or reload (depending on the page).

Parameters: page and diagnostic information.

Action: Report the problem to the operating company with the full text of the message. If the problem persists the system may run low on memory and an initialization or reload may be required.

BUG9284 Two memory blocks in the free memory list are detected with block sizes out of order. The incorrect block is undetermined.

Recovery has been performed to avoid corruption, but may have caused a loss of free memory. If memory was lost it will not be recovered until the next system initialization or reload.

Parameters: page, first block address and size, second block address and size, new size for first block.

Action: Report error to the operating company with the full text of the error message.

BUG9285 A pointer to a free memory list was corrupted and is corrected.

Parameters: page, corrupted address, corrupted value, expected value.

Action: The error has been recovered. If it occurs again report the full text of the error message to the operating company.

BUG9286 A data block was released that overlaps a block already free. The newly released block is ignored to avoid duplicate

tracking of memory or possible corruption. This may cause a loss of available memory in the system.

Parameters: page, start and end addresses of the released block, start and end addresses of the free block.

Action: Report the problem to the operating company with the full text of the error message.

BUG9287 The free list of protected data has been determined to contain less memory than expected. Additional protected data will be

allocated from unused unprotected data if it is available.

Parameters: memory size requested, dynamic protected data store boundary, fixed protected store boundary, (largest protected data store block available).

Action: Load a service change overlay and check memory availability. If memory is low a system reload should be planned, to recover the unavailable memory.

BUG9288 FREE_DATA_BLK or COPY_DATA_BLK was called without data to free or copy.

Parameters: block size and logical page, or block size and source and destination pages and addresses.

Action: Report the problem to the operating company with the full text of the error message, and any known actions related to the problem occurring.

BUG9289 More memory was freed on a logical page than was allocated on that page. Either the logical pages were different for allocating and deallocating the memory, or a block has been deallocated twice. The current block may not be the incorrect block.

Parameters: page size, page number, block size and block address.

Action: Report the problem to the operating company with the full text of the error message.

BUG9889 Corrupted Backward Link in the Procedure SICE_RECOVERY.

CIOD: Core Input/Output Diagnostic

CIOD0056 <test> fails: can't read local hard disk

where <test> can be TEST RDUN or DATA RDUN.

Action: Check local hard disk.

CIOD0057 <test> fails: can't read remote hard disk

where <test> can be TEST RDUN or DATA RDUN.

Action: Check remote hard disk.

CIOD0058 <test> fails: can't start disk sync

where <test> can be TEST RDUN or DATA RDUN.

Action: Contact technical support.

CIOD0059 %s aborted

where <test> can be TEST RDUN or DATA RDUN

CSC: Customer Service Change

CSC0103 Model set cannot be installed because ISM limit would be exceeded.
Output:
x = model used for this set
y = TN (l s c u) of this set

Action: Check ISM limits in overlay 22.

DCH: D-channel

DCH4001 Invalid DCH number received in SSD message from Transport.

DROL: Daily Routine Overlay

DROL0000 DAILY ROUTINE BEGIN
Overlay Mnemonic LD overlay number

DROL0001 DAILY ROUTINE END
Overlay Mnemonic LD overlay number

DTC: Digital Trunk Clock Controller Diagnostic

DTC0076 Clock was just switched!

You should wait one minute before doing another clock switch.

DTI: Digital Trunk Interface Diagnostic

DTI0075 You should wait for one minute to do another clock switch!

If you still want to switch the clock use the SWCK FRCE command.

EDD: Equipment Data Dump

EDD0042 Backup to floppy unsuccessful.

Action: Contact technical support.

ELAN: Ethernet Local Area Network

ELAN0027 Parameters: 6

IP address of card/server (4 octets)

Major and Minor version of IPL (2).

Action: Upgrade software on IP Line card and Signaling Server.

ERR: Error Monitor

ERR0006 tn CLT or RLT key can only be used on terminals with Phase 3, or higher firmware.

Action: Upgrade firmware of the set on that tn.

ERR0029 Invalid State / Event in R26 PCA operation.

Where A is:

1. Invalid PCA state
2. Invalid PCA Event
3. Unexpected PCA Event

Where B is: Current State

Where C is: Current Event

ERR0038 x — Number of Dialed digits exceeded its limit during transformation.

Action: Change SPRE length as that SPRE + Access Code length shouldn't be greater the FFC length for customer x.

ERR0039 — All 8 output timeslots are busy on loop <#>, Xnet will be flushed to retry TN: 0x%x, MSG: 0x%x, TIME: 0x%x.

Action: Contact your technical support.

ERR0041 — All 8 output timeslots are still busy on loop <#>, message is lost TN: 0x%x, MSG: 0x%x, TIME: 0x%x.

Action: Contact your technical support.

ERR0042 — Active CR is NIL, but MSG_CRPTR is not NIL.

ERR5142 x y — Required Configurations for TRO-CM to work is missing.
Check TRO(Overlay 16) and/or VTRO (overlay 17) prompts.
Where:
X is the customer number.
Y is the route number.

Action: Enable TRO and/or VTRO

ERR5143 x y — OPD option in CDR not enabled. The CDR records printed may not be accurate as TRO-CM is operating.
Where:
X is the customer number.
Y is the route number.

Action: Enable OPD option in overlay 16.

ERR9290 — Available unprotected memory is below acceptable levels. A system initialization may recover memory if blocks have become unavailable or memory is heavily fragmented. If initialization does not eliminate the error, or is not possible in the operating environment, remove some data from the system to free up more memory. This error will continue to be printed periodically until the low memory condition is corrected.

Parameters: page (always 0), remaining memory.

Action: Perform a system initialization as soon as possible. Do not attempt to add data to the system until the this condition is corrected. Report the problem to the operating company if initialization does not eliminate the problem and data cannot be removed from the system.

ERR9291 Available protected memory is below acceptable levels. Service change should not be attempted. If this error occurs only once it may indicate a transient condition that has been corrected. If it occurs repeatedly a system initialization to recover fragmented unprotected memory may free enough memory to allow protected memory space to grow (16K required). If initialization does not eliminate the low memory condition a system reload may. If reload does not help then the system is reaching it's capacity and some data may need to be removed in order to allow other data to be created.

Parameters: page (always 1), memory available

Action: If the error occurs more than once (about 15 minutes apart) a system initialization should be performed as soon as possible. Check the memory available by loading a service change overlay. If memory is still low perform a system reload. If memory remains low after a reload then remove data that is less critical in order to create new data.

ERR9292 Corruption in TIDY values.

Action: Please configure the Route again.

ERR9999 DCH:3 EXP (XBFR QUE FULL)

ESA: Emergency Services Access

ESA0001 Remote Virtual Office user logged in from a site without ESA support.

Action: If this user dials the ESDN, their call will not be redirected to the PSAP serving their current location (remote) -- It will be directed to the PSAP serving the site local to the error message (local). The remote site signaled that it did not support ESA for Virtual Office. To correct the issue, make sure the software version of the remote site supports ESA for Virtual Office. Additionally, confirm that the remote site has the ESA package and that the customer ESA data is configured.

ESA0002 Remote Virtual Office user originated ESA call to local PSAP.

Action: A user has been connected to an incorrect PSAP without their knowledge. Verify that the emergency situation was dealt with. The site where the user is located (remote) signaled that it did not support ESA for Virtual Office. (see corresponding ESA0001) To correct the issue, make sure the software version of the remote site supports ESA for Virtual Office. Additionally, confirm that the remote site has the ESA package and that the customer ESA data is configured.

ESA0003 Active call preempted by Virtual Office ESA call Action: When a local IP phone registers to a remote Call Server using Virtual Office, the local TN is logged out. It is possible that a second user could use Virtual Office to occupy the logged out local TN. If the first user makes an ESA call, the IP phone will return to the local Call Server to place the ESA call. When this occurs, if there is a second user occupying the local TN then that user will be preempted. This message indicates that this has occurred to a user that had an established call.

ESA0004 Virtual Office login preempted by Virtual Office ESA call Action: When a local IP phone registers to a remote Call Server using Virtual Office, the local TN is logged out. It is possible that a second user could use Virtual Office to occupy the logged out local TN. If the first user makes an ESA call, the IP phone will return to the local Call Server to place the ESA call. When this occurs, if there is a second user occupying the local TN then that user will be reempted. This message indicates that this has occurred to a user that did not have any established call.

ESN: Electronic Switched Network

ESN0056 CAS and NAS are mutually exclusive and cannot be configured for the same customer.

Action: If you are configuring CAS, disable NAS in overlay 86. If you are configuring NAS, disable CAS in overlay 15.

FIJI: Fiber Junctor Interface

FIJI0070

FIJI0070 FIJI p1 p2 p3
Faulty card detected by I3 and IL tests
p1=Group, p2=side, p3=suspected area of failure.

Action: This card has a problem. Replace card as soon as possible.
P3 indicates the suspected area of failure:
1. DRP-to-ADD path
2. SPACE FPGA

FIJI0071

FIJI0071 FIJI p1 p2
Faulty card detected by I3 and IL tests
p1=Group, p2 = side

Action: A retest (test all) is recommended after replacing the card downstream that is reporting a SPACE FPGA failure. This will ensure that the DRP-to-ADD path works.

FIJI0072

FIJI0072 FIJI p1 p2
Faulty card detected by I3 and IL tests
p1=Group, p2 = side

Action: This card or one of the adjacent cards reporting an error condition has a problem.

FIJI0073

FIJI0073 FIJI p1 p2
Faulty card detected by I3 and IL tests
p1=Group, p2 = side

Action: Incomplete test results. This card is likely okay, however a retest (test all) is recommended so that all test results may be completed and a correct analysis given.

FIJI0074

FIJI0074 FIJI p1 p2 p3
Faulty card detected by I3 and IL tests
p1=Group, p2=side, p3=suspected area of failure

Action: Incomplete test results. This card, or one of the adjacent cards, has a problem. A reset (test all) is recommended so that all test results may be completed and a more accurate diagnosis made. P3 indicates the suspected area of failure had all the test results been complete:
1. DRP-to-ADD path
2. SPACE FPGA
3. This card is likely okay however a reset is recommended after replacing the card downstream that is reporting a SPACE FPGA failure.

FIJI0075

FIJI0075 FIJI p1 p2
Backplane test results not received from this group.
p1=Group, p2 = side

Action: Test results were not received for the fiji cards on this group. Backplane test should be performed on both.

FIJI0076

FIJI0076 FIJI p1 p2
Backplane test detected failure.
p1=Group, p2=Side

Action: All loops failed on this group and side. Test results were not received for the FIJI card on the other side. A backplane test is recommended for the other side before solid conclusions can be drawn.
1. If the other side's test results completely fail, then see FIJI0078.
2. If the other side's test results all pass, then see FIJI0079.
3. If some loops fail on the other side then it may indicate that both this FIJI card and the loops that the other side reported are bad. Replace this FIJI card first the retest. If both sides now agree on which loops are bad, then check those loops.

FIJI0077

FIJI0077 FIJI p1 p2 p3
Backplane test detected failure.
p1=Group, p2=Side,p3=loop (range 0-31)

Action: Some loops failed on this group and side. Test results were not received for the FIJI card on the other side. A backplane test is recommended for the other side before solid conclusions can be drawn.
1. If the other side's test results completely fail, then replace the FIJI card on the other side.
2. If the other side's results match that of this side, then see FIJI0080.
3. If the other side passes all loops then see FIJI0079.
4. If the other side's result show failures on different loops, then see FIJI0081.

FIJI0078

FIJI0078 GROUP p1
Backplane test detected failure.
p1 = Group

Action: All loops on both sides of this group failed. Check both PS cards. If they seem okay then replace each fiji card individually. Otherwise, check the backplane cables.

FIJI0079

FIJI0079 FIJI p1 p2 p3
Backplane test detected failure.
p1 = Group, p2 = Side, p3 = loop

Action: Only this side shows backplane failures on those loops. Replace the fiji card first and retest. If the same loops fail then check those loops. Otherwise,

check the fiji card's backplane connections.

FIJI0080 FIJI0080 FIJI p1 p2 p3
Backplane test detected failure.
p1=Group, p2=Side, p3 = loop

Action: Both sides of this group show failures on those loops. If all loops from 0 to 15 fail then check the PS card on side 0. If all loops from 16 to 32 fail then check the PS card on side 1. Otherwise, check the loops in error. If the loops do not seem to be bad then replace each fiji card individually. If this fails, then check the backplane connections.

FIJI0081 FIJI0081 FIJI p1 p2 p3
Backplane test detected failure.
p1=Group, p2=Side, p3 = loop

Action: Both sides of this group show unique loop errors. Replace both fiji cards and retest. If the same loops fail then check those loops. Otherwise check each fiji card's backplane connections.

FIJI0082 FIJI0082 FIJI p1 p2 p3
360 test detected failure
p1=Group, p2=Side, p3 = loop (0-31, or ALL)

Action: If every card in the ring fails the same link or ALL links then disable the fiji card in group 0 first and perform the 360 test on another card in the ring. If the same failure occurs then repeat this for every card downstream until the card is found that causes the failure. If individual cards have failures then replace those cards and perform the 360 test.

ISR: Intergroup Switch and System Clock Generator Diagnostic

ISR0006 n The clock controllers cannot be switched because clock controller n is software disabled.

Action: Enable the disabled pack provided it is operational.

ISR0063 You should wait one minute before doing another clock switch!

If you still want to switch the clock use the SCLK FRCE command.

ISR0223 Test fiji command cannot be used unless all cards in the ring are disabled first.

Action: Disable the ring.

ISR0225 FIJI Rings are in survival mode. FIJI test routine cannot be completed at this time.

ISR0226 There are some disabled FIJI card(s) on the ring. FIJI test routine cannot be completed at this time.

ISR0227 There are some other task running on the ring. FIJI test routine cannot be completed at this time.

ISR0228 There are some major alarm(s) on the ring. FIJI test routine cannot be completed at this time.

ISR0232 Starting FIJI test routine.

ISR0233 Starting I3 test.

ISR0234 Completed I3 test.

ISR0235 Starting IL test.

ISR0236 Completed IL test.

ISR0237 Starting BKPL test.

ISR0238 Completed BKPL test.

ISR0239 Starting 360 test.

ISR0240 Completed 360 test.

ISR0241 Completed FIJI test routine.

ISR0318 Duration for link test must be in the range of 1 to 60.

ITG: Integrated IP Telephony Gateway

ITG4043 %d(latency),%s(source),%s(destination),%d(tcid)

Latency Threshold Exceeded:%d(latency),%s(source),%s(destination),%d(tcid) Where: Latency is the (round trip delay)/2 in milliseconds Source is the reporting set IP or channel + port number Destination is the terminating set IP or channel Tcid is the channel id (if a dsp is reporting).

Action: Action: 1. Possible voice degedation in IP phone due to network congestion, please check your network configuration to ensure proper operation.

ITG4044 %d(jitter),%s(source),%s(destination),%d(tcid)

Jitter Threshold Exceeded:%d(jitter),%s(source),%s(destination),%d(tcid) Where jitter is in milliseconds Source is the reporting set IP or channel + port number Destination is the terminating set IP or channel Tcid is the channel id (if a dsp is reporting).

Action: Action: 1. Possible voice degedation in IP phone due to network congestion, please check your network configuration to ensure proper operation.

ITG4045 Latest election has changed the LTPS master of node <node ID> to <master's TLAN IP addr>.

NPR: Network and Peripheral Equipment Diagnostic (LD 32)

NPR0034 DISU command is blocked because the unit being disabled is experiencing a flash download.

NPR0035 The flash download for the following TN is terminated due to the ‘disable’ command.

Action: The flash download for the affected TN might need to be reactivated after the unit is enabled.

NPR0054 FDLC command completed. Download to sets will continue until complete.

NPR0055 H.323 virtual trunks can not be enabled when H323_VTRK is restricted.

PRI: Primary Rate Interface

PRI0008 UUI IE length exceeded the maximum allowed.

SCH: Service Change

SCH0361 Key number out-of-range 0-9 per key/lamp strip, 0-10 for M2012 and M3000, 0-8 for M2009, 0-17 for M2018, 0-5 for M2006, 0 for.

SCH1425 The CLT or RLT mnemonic can only be used on the M3903, M3904 or M3905 terminals.

SCH1427 Predefined set-to-set message file for the selected language cannot be loaded from the disk.

Action: Select another language and report the problem to the vendor.

SCH1429 On the M3903, M3904 and M3905, key 28 is reserved for the RLT mnemonic. No other mnemonic except NUL can be configured on that key.

SCH1430 The route must have an IDC table associated when SDID is enabled

SCH1445 Unit type configured o n PBX card is not defined.

SCH1450 This type of TN is not valid for Set based D-Channel monitoring.

SCH1452 TBCT is not configured.

SCH1457 Attempt to configure RCAP UUI without UUI package.

SCH1458 RCAP UUI only allowed for ESS4/ESS5 interfaces.

SCH1459 Attempt to configure ICON without ICON package.

SCH1460 OAS Package is not equipped.

SCH1461 Either the Customer Number is not same as the set under service change configuration or the first entry of the SCL is not a position ID.

SCH1462 For Service request CHG of Class Of Service OUSD to OUSA an SCL number needs to be associated with OBV key.

SCH1463 PCA ISM exhausted / insufficient.

SCH1464 PCA package not equipped.

SCH1465 Target DN in Customer Data Block and Target DN in HOT key cannot both be blank. A minimum of one DN must be defined.

Action: Make sure that at least one of the target DN is not Blank

SCH1466 Removal of TPDN may affect the R26 PCA functionality.

SCH1467 PCA configuration requires that key 1 be configured as a HOT P key.

SCH1468 Call Pickup is not allowed on telephones in group zero.

SCH1469 Loop/Shelf/Card/Unit you are trying to access is disabled because the support to this hardware has been stopped. No further operations on these TNs are possible. Please use overlay 81 to list all the components that are affected on your system.

SCH1470 Hebrew is supported only on M3904 sets.

Action: Select another language for this set.

SCH1471 SCB/ADS Block is not configured for this customer.

SCH1472 Observe Password Table already exists.

SCH1473 The combination of signalling and trunk type is not acceptable in United Kingdom (Package 190).

Action: Enter a valid input acceptable in United Kingdom. Or if Package 190 (UK) is equipped by mistake, delete the package.

SCH1474 Supervisor ID already exists.

SCH1475 Password required for the Supervisor ID entered in ADPD prompt.

SCH1476 Observe Password Table does not exist.

SCH1477 Not enough PDS available to create Observe Password Table.

SCH1478 Pointer to Observe Password Table does not exist.

SCH1479 LST is not a valid request for OBVP prompt in LD 23.

SCH1481 ACD is not allowed for i2001.

SCH1482 Maximum allowed entries for OBVP table is 240.

SCH1483 Entry does not exist in OBVP table.

SCH1484 Invalid XTRK type. Enter MC8, MC32, ITG8, ITGP or VTRK.

SCH1485 VTRK is not a valid XTRK type for VGW tn types.

SCH1486 Invalid input. Enter MC8 or MC32.

SCH1487 Invalid input, Enter ITG8 or ITGP.

SCH1489 H.323 Virtual Trunk package not equipped.

SCH1490 The number of IP Peer H.323 Trunks in the system exceeds the maximum number of IP Peer H.323 Trunks defined in the ISM parameter.

Action: Contact your technical support group.

SCH1493	AAA and AFNA are mutually exclusive and cannot be configured for the same customer. **Action:** If you are configuring AAA, disable AFNA in overlay 15. If you are configuring AFNA, disable AAA in overlay 15.
SCH1494	CAS and NAS are mutually exclusive and cannot be configured for the same customer. **Action:** If you are configuring CAS, disable NAS in overlay 86. If you are configuring NAS, disable CAS in overlay 15.
SCH1495	The TN "## ##" not configured.
SCH1496	No IP sets associated with the IP address "###.###.###.###".
SCH1497	No IP sets associated with the DN "###…".
SCH1498	The customer number "##" is invalid.
SCH1499	rfcCall in function "function_name" failed.
SCH1506	The IP Address "###.###.###.###" is invalid.
SCH1507	The MAP command wasn't processed completely. **Action:** Please try again. If the case repeats, contact your technical support group.
SCH1508	CFW must be entered for DCS sets. **Action:** Enter CFW at the FTR prompt.
SCH1509	Cannot MOV/OUT acquired TN. First De-acquire the TN and then proceed with MOV/OUT request. **Action:** De-acquire the TN and then proceed with MOV/OUT operation.
SCH1510	Invalid CLS input.
SCH1511	CLS FEDA/FEDD applies to DCS sets only.
SCH1516	MCA card supports only keys 0-7. **Action:** Move the key functions of the voice set in the range 0-7 if you intend to use MCA.
SCH1890	TBCT Package is equipped. **Action:** Enable TBCT Package.

SCH1891 TBCT/XTBC valid only for NI-2 interface.

Action: Enable NI-2 name display package.

SCH6679 Warning: The prime key does not have any of the following functions: SCR, MCR, SCN, MCN, ACD; it is set to SCR as default.

SRPT: System Reports

SRPT0031 Disk Redundancy: dosFsChk() returned ERROR on partition x.

Error value = y

Action: Please re-install software.

SRPT0091 HB: remote side ELAN health change: <n>

SRPT0092 AML: remote side AML connection <nr> to <ip> health change: <n>

SRPT0093 AML: local side AML connection <nr> to <ip> health change: <n>

SRPT0094 LCS: Cannot switchover: ELAN health better on remote side but hardware better on local.

SRPT0095 HIREM: <object> on remote side <side> is Out Of Service.

SRPT0096 HIREM: <object> on remote side <side> is In Service.

SRPT0100 CMDU on side <s> is Out Of Service.Please check CMDU where s = 0,1.

Action: Check CMDU on side <s>.

SRPT0101 LCS: CMDU on inactive side <s> is Out Of Service. Going to split mode where s = 0,1

Action: Check CMDU on side <s>.

SRPT0102 CMDU on side <s> is Out Of Service.Please check CMDU where s = 0,1

Action: Check CMDU on side <s>.

SRPT0103 DR: Core side%d cannot continue to send disk updates to inactive side.

Action: Contact your technical support.

SRPT0104 DR: Cannot send disk update messages to%s, errno [0x%x]. Queue is full. Disk resync will be attempted.

Action: If resync does not complete, try restart disk sync manually by INI the inactive side.

SRPT0106 LCS: Join denied. Incompatible IRQ order between both sides.

Action: Contact technical support.

SRPT0108 VO login Password retry failed 3 times. Tried to login as TN: 0x%x on the set TN: 0x%x.

Action: Let the login lock expire in one hour, or disable/enable the set through LD 32.

SRPT0109 LCS: Join Operation Aborted Due To CNI Objects Mismatch Between Core 0 And Core 1.Use stat cni command in overlay 135 to see CNI objects.

Action: Check that both sides have the same number of CNIs configured.

SRPT0110 CM: Primary client connection established.

SRPT0111 DR: Recovered the message queue (%s) and disk resynchronization has been initiated.

Action: Contact your technical support.

SRPT0112 DR: Can not start disk-sync due to file corrupt in local disk. Please re-install both software & database on this side!

Action: Contact your technical support.

SRPT0115 HIREM: Can't prevent graceful SWO while adding network groups.

Action: Contact your technical support.

SRPT0116 CM: Primary server restarted.

Action: Contact your technical support.

SRPT0117 CM: Server connection established.

SRPT0118 CM: Server connection lost.

Action: Contact your technical support.

SRPT0119 CM: Retrying server initialization.

Action: Contact your technical support.

SRPT0120 CM: Primary client recovery failed.

Action: Contact your technical support.

SRPT0121 CM: Secondary server recovery failed.

Action: Contact your technical support.

SRPT0122 CM: Secondary client recovery failed.

Action: Contact your technical support.

SRPT0123 MIDN: Starting graceful SWO from side <a> to side <b>Where <a>,<b> : 0 , 1.

SRPT0124 MIDN: Can't start graceful SWO. RDUN tests returned error.

Action: Check local and remote Hard drive.

SRPT0125 MIDN: Can't start graceful SWO. Local health is better than remote health.

SRPT0126 DR: Not allowed to sync while already syncing.

SRPT0127 LCS: Graceful switchover unsuccessful. Stop&Copy failed.

Action: Contact your technical support.

SRPT0129 LCS: Graceful switchover can't be performed. SWO is locked.

Action: Contact your technical support.

SRPT0130 LCS: Graceful switchover successful. LcsSCDone message lost.

SRPT0131 CM: Primary client can't connect to the other side.

Action: Check HSP connection.

SRPT0146 DPSDL: Unable to remove the file [%s], ErrNo is %d\n.

SRPT0147 DPSDL: Unable to rename the file [%s] as [%s], ErrNo is %d\n.

SRPT0148 DPSDL: During the next join the Psdl Files will be Synced to the other side \n.

SRPT0149 DPSDL: Unable to Backup the PSDL Files on the Inactive side.

SRPT0150 DPSDL: Started Syncing the PSDL Files to the other side.

SRPT0151 DPSDL: PSDL Sync is completed \n.

SRPT0152 DPSDL: Please use the command 'dpsdlSync' to sync the PSDL files \n.

SRPT0153 RST <D1> WARM START IN PROGRESS - Reason <d2>.Trap Data Block not saved. Where:
d = CPU side [0..1]
d2 = Reason for restart

SRPT0154 Disk synchronization has failed. The remote core side %d has a better disk image.

Action: Switch to core side %d before joining the cores. Contact your technical support.

SRPT0155 Disk synchronization has been aborted. Core side %d has a better disk image.

Action: Switch to core side %d before joining the cores. Contact your technical support.

SYS: System Loader

SYS0074 Predefined set-to-set messages for the selected language cannot be loaded from the disk.

Action: Select another language and report the problem to the vendor.

SYS0075 Unable to allocate protected memory for predefined set-to-set messages.

Action: Contact technical support.

SYS0121 UUI RCAP removed and/or UUI prompt for CDN removed, since UUI package is not equipped.

SYS0122 No CIS ANI reception table found in customer datablock. Default table is created.

SYS0123 No CIS/MFC CACC table found in customer datablock. Default table with one entry is created.

SYS0124 No protected data storage available for default CIS ANI reception table.

Action: Contact technical support.

SYS0125 No protected data storage available for default CIS/MFC CACC table.

Action: Contact technical support.

SYS0126 Warning. Illegal RGA program key found on M3903 - M3905 telephone. May cause undesirable set display/soft key updates if key is used. Prompted if ARDL (304) or M3900_RGA_PROG (396) packages are not equipped.

Action: Add missing packages or manually remove Programmable RGA keys from M3903-M3905 sets.

SYS0127 ICON PACKAGE NOT ENABLED.

SYS0128 The number of PCAs configured exceeds the PCA ISM Limit and no further PCAs can be sysloaded.

SYS0129 Existing M3900 language is changed from Hebrew to English since the HEBREW package is restricted.

SYS0130 The number of IP Peer H.323 Trunks exceeds the Limit or H323_VTRK package is restricted. No further H.323 Trunks can be sysloaded.

Action: Contact your technical support group.

SYS0271 The OAS package is disabled.

SYS0273 Observe Password Table is not loaded.

SYS9280 The pointers to the list of free memory were corrupted and have been reset. No memory is available on this page. If this message is for page 0 and is not followed by a BUG9281 then the system is out of memory.

Parameters: page (0 for unprotected, 1 for protected), page head and page tail.

Action: If the page is 0 and BUG9281 is not printed perform a system initialization as soon as possible, without logging in. If the problem is on page 1 and occurs repetitively the system may run out of memory and a system reload will be required. Report the problem to the operating company with the full text of the error message.

SYS9281 Unused unprotected memory was not properly tracked. It has been recovered.

Parameters: page (always 0), address and size of recovered block.

Action: The problem has been corrected. No action is required for a single occurrence. If the error message occurs repetitively data corruption is likely - report the problem to the operating company with the full text of the error message.

SYS9282 Unused protected memory was not properly tracked. The memory will remain unavailable until the next system reload. Tracking is updated to reflect the change.

Parameters: page (always 1), address and size of the unavailable block.

Action: Report the problem to the operating company with the full error printout. If the problem persists the system may run out of memory and a system reload should be performed. A system initialization is unlikely to improve the memory condition.

SYS9283 A block of memory that is marked unused has been corrupted. It is discarded to avoid possible conflicts with a persistent misuse of the memory. The memory will be unusable until the next system initialization or reload (depending on the page).

Parameters: page and diagnostic information.

Action: Report the problem to the operating company with the full text of the message. If the problem persists the system may run low on memory and an initialization or reload may be required.

SYS9284 Two memory blocks in the free memory list are detected with block sizes out of order. The incorrect block is undetermined.

Recovery has been performed to avoid corruption, but may have caused a loss of free memory. If memory was lost it will not be recovered until the next system initialization or reload.

Parameters: page, first block address and size, second block address and size, new size for first block.

Action: Report error to the operating company with the full text of the error message.

SYS9285 A pointer to a free memory list was corrupted and is corrected.

Parameters: page, corrupted address, corrupted value, expected value.

Action: The error has been recovered. If it occurs again report the full text of the error message to the operating company.

SYS9286 A data block was released that overlaps a block already free. The newly released block is ignored to avoid duplicate

tracking of memory or possible corruption. This may cause a loss of available memory in the system.

Parameters: page, start and end addresses of the released block, start and end addresses of the free block.

Action: Report the problem to the operating company with the full text of the error message.

SYS9287 Block size parameter is zero.

SYS9288 Attempt to release in low (reserved) memory.

SYS9289 Attempt to release beyond end of memory.

SYS9290 Available unprotected memory is below acceptable levels. A system initialization may recover memory if blocks have become unavailable or memory is heavily fragmented. If initialization does not eliminate the error, or is not possible in the operating environment, remove some data from the system to free up more memory. This error will continue to be printed periodically until the low memory condition is corrected.

Parameters: page (always 0), remaining memory.

Action: Perform a system initialization as soon as possible. Do not attempt to add data to the system until the this condition is corrected. Report the problem to the operating company if initialization does not eliminate the problem and data cannot be removed from the system.

SYS9291 Available protected memory is below acceptable levels. Service change should not be attempted. If this error occurs only once it may indicate a transient condition that has been corrected. If it occurs repeatedly a system initialization to recover fragmented unprotected memory may free enough memory to allow protected memory space to grow (16K required). If initialization does not eliminate the low memory condition a system reload may. If reload does not help then the system is reaching it's capacity and some data may need to be removed in order to allow other data to be created.

Parameters: page (always 1), memory available

Action: If the error occurs more than once (about 15 minutes apart) a system initialization should be performed as soon as possible. Check the memory available by loading a service change overlay. If memory is still low perform a system reload. If memory remains low after a reload then remove data that is less critical in order to create new data.

TFC: Traffic Control

TFC0001 QoS packet loss: [value of exceeded threshold], [source IP + port number], [source TN], [source zone], [destination IP], [destination TN], [destination zone]. [DSP Channel].

Action: IP Voice quality degradation has been detected, please check your IP network or contact you technical support group.

TFC0002 QoS latency: [value of exceeded threshold], [source IP + port number], [source TN], [source zone], [destination IP], [destination TN], [destination zone] [DSP Channel].

Action: IP Voice quality degradation has been detected, please check your IP network or contact you technical support group.

TFC0003 QoS jitter: [value of exceeded threshold], [source IP + port number], [source TN], [source zone], [destination IP], [destination TN], [destination zone] [DSP Channel].

Action: IP Voice quality degradation has been detected, please check your IP network or contact you technical support group.

TFC0004 QoS Report gathering temporary disable [End Point: source IP + port number / Server: IP Address / All].

Action: IP Voice quality degradation has been detected, please check your IP network or contact you technical support group.

Meridian 1, Succession 1000,
Succession 1000M

What's New for Succession 3.0

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.
SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.
Publication number: 553-3001-015
Document release: Standard 1.00
Date: October 2003
Produced in Canada

NORTEL NETWORKS™