Succession 1000
Succession 1000M
Succession 3.0 Software

Branch Office

Document Number: 553-3001-214
Document Release: Standard 1.00
Date: October 2003

Revision history

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously included in the following legacy document, now retired: 553-3023-221 - Branch Office.

Contents

About this document

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

Subject

This document describes Succession Branch Office features, planning, installation, configuration, and maintenance. Its chapters complement corresponding documents in the Succession 1000 and Succession 1000M documentation suites, as listed in "Related information".

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:

- Succession 1000

- Succession 1000M Chassis

- Succession 1000M Cabinet

- Succession 1000M Half Group

- Succession 1000M Single Group

- Succession 1000M Multi Group

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

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
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 who install, configure, and maintain Succession Branch Office locations for organizations using the Succession 1000 or Succession 1000M systems.

Conventions

Terminology

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

- Succession 1000
- Succession 1000M

The following systems are referred to generically as "Small System":

- Succession 1000M Chassis
- Succession 1000M Cabinet

The following systems are referred to generically as "Large System":

- 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:

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

- *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180)

- *ESN Transmission* (553-3001-181)

- *Dialing Plans: Description* (553-3001-183)

- *Circuit Card: Description and Installation* (553-3001-211)

- *Signaling Server: Installation and Configuration* (553-3001-212)

- *IP Peer Networking* (553-3001-213)

- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)

- *System Management* (553-3001-300)

- *Software Input/Output: Administration* (553-3001-311)

- *Emergency Services Access: Description and Administration* (553-3001-313)

- *Succession 1000 Element Manager: System Administration* (553-3001-332)

- *Meridian Integrated Conference Bridge: Service Implementation Guide* (553-3001-358)

- *IP Line: Description, Installation, and Operation* (553-3001-365)

- *Internet Terminals: Description* (553-3001-368)

- *Basic Network Features* (553-3001-379)

- *Software Input/Output: Maintenance* (553-3001-511)

- *Small System: Planning and Engineering* (553-3011-120)

- *Small System: Installation and Configuration* (553-3011-210)

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

- *Large System: Planning and Engineering* (553-3021-120)

- *Large System: Installation and Configuration* (553-3021-210)

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

- *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)

- *Succession 1000 System: Maintenance* (553-3031-500)

- *CallPilot Planning and Engineering Guide* (555-7101-101)

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.

Overview

Contents

This section contains information on the following topics:

What is the Succession Branch Office?

The Succession Branch Office extends Succession 1000 or Succession 1000M features from a Main Office to one or more remote Branch Offices.

A Succession Branch Office is an H.323 WAN Gateway connected to an IP PBX at the Main Office over a WAN. This enables a secondary location to centralize the call processing of its IP-based communications network. The Succession Call Server at the Main Office provides the call processing for the Internet Telephones in both the Main Office and Branch Offices. The Branch Office H.323 WAN Gateway provides call processing functionality to local digital telephones and analog devices. The Branch Office H.323 WAN Gateway also provides 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). More than one Branch Office can be associated with a single Main Office. In addition, 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 properly.

A Succession Branch Office network is shown in Figure 1 on .

Figure 1
Succession Branch Office network (with a Succession 1000 Main Office)

553-AAA0134
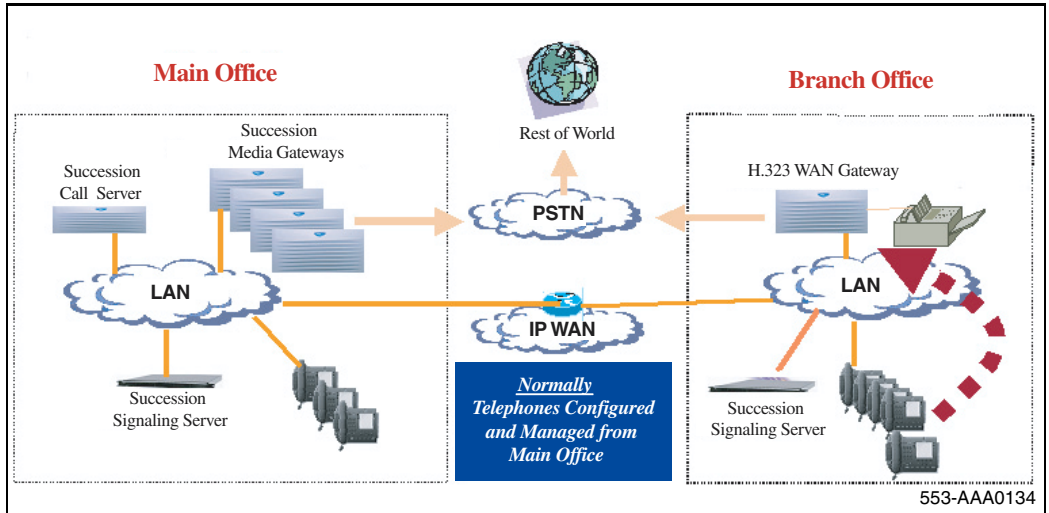
Main Office hardware description

The Main Office must be one of the following systems:

- Succession 1000 (as shown in Figure 1)

- Succession 1000M Cabinet

- Succession 1000M Chassis

- Succession 1000M Half Group

- Succession 1000M Single Group

- Succession 1000M Multi Group

The diagrams throughout this document show a Succession 1000 Main Office. Both the Succession 1000 and Succession 1000M systems perform identical Main Office functions as far as the Branch Office is concerned.

Branch Office hardware description

The basic hardware of a Succession Branch Office includes the H.323 WAN Gateway and the Succession Signaling Server.

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 digital telephones and analog devices, such as fax machines or analog (500/2500-type) telephones in the Branch Office.

Where required, the Branch Office H.323 WAN Gateway is connected by copper wire to the Branch Office H.323 WAN Gateway Expansion Chassis for added capacity.

The Branch Office H.323 WAN Gateway must contain a Succession System Controller (SSC). The SSC provides telephony services to the Branch Office H.323 WAN Gateway elements, such as digital telephones, analog devices, digital trunks, and analog trunks. It also provides Call Processing services to Internet Telephones in Local Mode. The Branch Office H.323 WAN Gateway provides a dedicated slot (slot 0) for the SSC card. The feature set of the software on the SSC may differ from that of the Succession Call Server at the Main Office.

The 10/100BaseT connection for the Embedded Local Area Network (ELAN) and Telephony Local Area Network (TLAN), where the WAN gateway exists, is on the back of the Branch Office H.323 WAN Gateway chassis.

The Branch Office H.323 WAN Gateway chassis has four "usable" slots, plus one for the SSC, with the following characteristics:

- The slots are numbered from 0 to 4. Slot 0 is dedicated to the SSC card, leaving the four "usable" slots 1 to 4.

- No "usable" slot (1 to 4) is dedicated to a specific card type.

- The following circuit cards can be installed in any "usable" slot (1 to 4):

  — Succession Media Cards

— Digital Trunk Cards

— Analog Trunk Cards

— Analog Line Cards

— Digital Line Cards

— Meridian Integrated RAN (MIRAN) Card

— Meridian Integrated Conference Bridge (MICB) Card

— cards to support CallPilot Mini or CallPilot 201i

Note 1: The legacy 24-port ITG-P card, when upgraded to IP Line 3.1 software, provides the same service as the Succession Media Card. In this document, unless otherwise noted, the ITG-P card can be substituted for the Succession Media Card.

Note 2: The Succession Media Cards act exclusively as Voice Gateway Media Cards (VGMCs) in the Branch Office.

Figure 2 shows the Branch Office H.323 WAN Gateway.

Figure 2
Branch Office H.323 WAN Gateway/H.323 WAN Gateway Expansion chassis

553-AAA0186

H.323 WAN Gateway Expansion

The H.323 WAN Gateway Expansion chassis is identical to the H.323 WAN Gateway, with the following exceptions:

- The slots are numbered from 7 to 10. Use any double-slot card in slot 10.

- No slot is dedicated to a specific card type.

- Digital trunk cards are not supported in the Expansion chassis.

- There is no Ethernet port on the back of the Expansion chassis, since the Expansion chassis is connected to the H.323 WAN Gateway with copper wire.

Succession Signaling Server

The Succession Signaling Server is a required piece of equipment at the Branch Office. It provides the following functions:

- IP Peer Networking, incorporating the H.323 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 Succession Signaling Server can be used to provide redundancy in the case of a failure in the other (primary) Succession Signaling Server in the Branch Office.

For more information on the Succession Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Telephones

The Branch Office supports the i2002 and i2004 Internet Telephones and the i2050 Software Telephone. Analog (500/2500-type) and digital telephones are also supported.

Note: Throughout this document, the i2002 and i2004 Internet Telephones and the i2050 Software Telephone are referred to collectively as "Internet Telephones".

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

Internet Telephones must be running firmware version 1.39 or later.

Succession Media Card – Voice Gateway

The Succession Media Card acts as a Voice Gateway Media Card (VGMC), providing a pool of Digital Signaling Processor (DSP) ports for media transcoding between IP voice packets and circuit-switched resources. The card comes equipped with DSP modules. Each call between an Internet Telephone and an analog (500/2500-type) or digital telephone or the PSTN uses one DSP port. Calls between two Internet Telephones do not require any DSP ports, as there is no need for IP-to-circuit-switched transcoding.

Succession Media Cards provide echo cancellation, compression, and decompression of voice streams.

Note: The ITG-P card uses two card slots in the chassis, whereas the Succession Media Card uses one card slot.

Analog or digital trunk cards

All analog and digital trunk interfaces supported on Succession 1000 and Succession 1000M are also supported in the Branch Office. Analog and digital trunk cards interface with the PSTN. For information on trunk cards, refer to *Circuit Card: Description and Installation* (553-3001-211).

Analog or digital line cards

Analog (500/2500-type) or digital telephones and devices are supported in the Branch Office H.323 WAN Gateway. For information about line cards, refer to *Circuit Card: Description and Installation* (553-3001-211).

When additional digital and analog (500/2500-type) telephones are located in the Branch Office, additional DSP resources are required. Refer to *Succession 1000 System: Planning and Engineering* (553-3031-120).

Capacity

Each Succession 1000 or Succession 1000M Main Office can support up to 255 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).

The hardware configuration of the Branch Office depends on:

- the number of line and trunk cards being provisioned

- the number of Succession Media Cards required to provide a sufficient number of DSP channels

Succession Media Card DSP capacity

The number of DSP ports to provision depends on the trunk-to-telephone ratio. A rule-of-thumb is to have the number of ports greater than or equal to the number of trunks configured. See *Succession 1000 System: Planning and Engineering* (553-3031-120) for more information.

If digital telephones and analog (500/2500-type) telephones are equipped at the Branch Office, additional DSP ports are needed for digital-to-Internet Telephone and analog-to-Internet Telephone connections. The number of additional DSP ports must be equal to or greater than the expected number of simultaneous connections of these types. The user can engineer fewer DSP ports depending on their desired blocking ratio.

Hardware configuration overview

In each Branch Office H.323 WAN Gateway, one SSC is required, as well as at least one Succession Media Card with the Voice Gateway application (IP Line 3.1). This leaves three slots remaining, which can contain analog line cards, analog trunk cards, digital line cards, or digital trunk cards.

Note: Each Branch Office H.323 WAN Gateway with a digital trunk card must have a clock controller. See *Circuit Card: Description and Installation* (553-3001-211).

There are two configurations for the Branch Office:

• without an H.323 WAN Gateway Expansion chassis

• with an H.323 WAN Gateway Expansion chassis

A Branch Office configuration without an H.323 WAN Gateway Expansion chassis is shown in Figure 3. It has a single Branch Office H.323 WAN Gateway.

Figure 3
Branch Office with one H.323 WAN Gateway
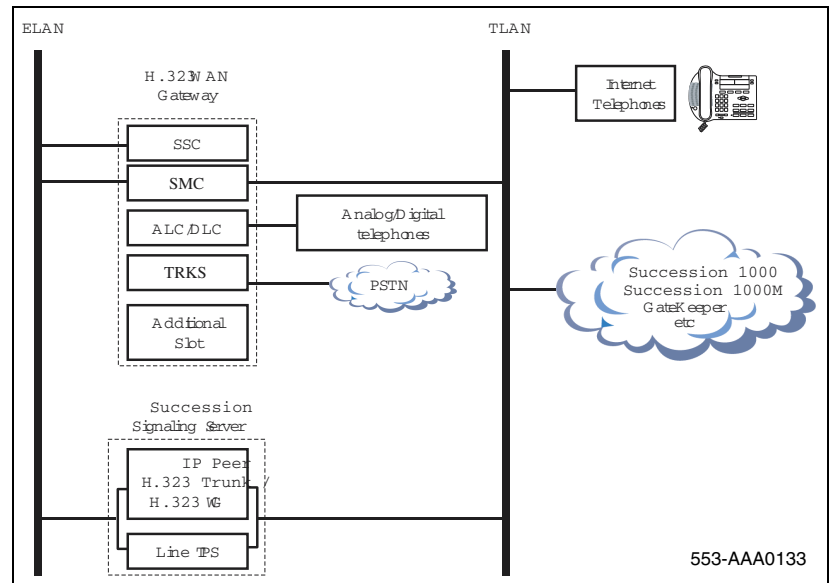
This Branch Office configuration requires at least one Succession Media Card. The additional slots can be used for any combination of the following:

• trunk card

• analog or digital line card

- second Succession Media Card

- Meridian Integrated Conference Bridge (MICB) card

- Meridian Integrated RAN (MIRAN) card

- cards to support CallPilot Mini or CallPilot 201i

For more information on the Succession Media Card configuration, refer to *IP Line: Description, Installation, and Operation* (553-3001-365). For more information on MICB, refer to *Meridian Integrated Conference Bridge: Service Implementation Guide* (553-3001-358).

A Branch Office configuration with an H.323 WAN Gateway Expansion chassis is shown in Figure 4 on . With the addition of an H.323 WAN Gateway Expansion chassis, you have eight usable slots. There must be at least one Succession Media Card (8- or 32-port cards with IP Line 3.1) for the Branch Office H.323 WAN Gateway. If more than one SMC card is used, the cards may all be located in one chassis or distributed among them.

> *Note:* The Branch Office H.323 WAN Gateway Expansion does not support digital trunks.

Figure 4
Branch Office with H.323 WAN Gateway Expansion for maximum capacity

553-AAA0135
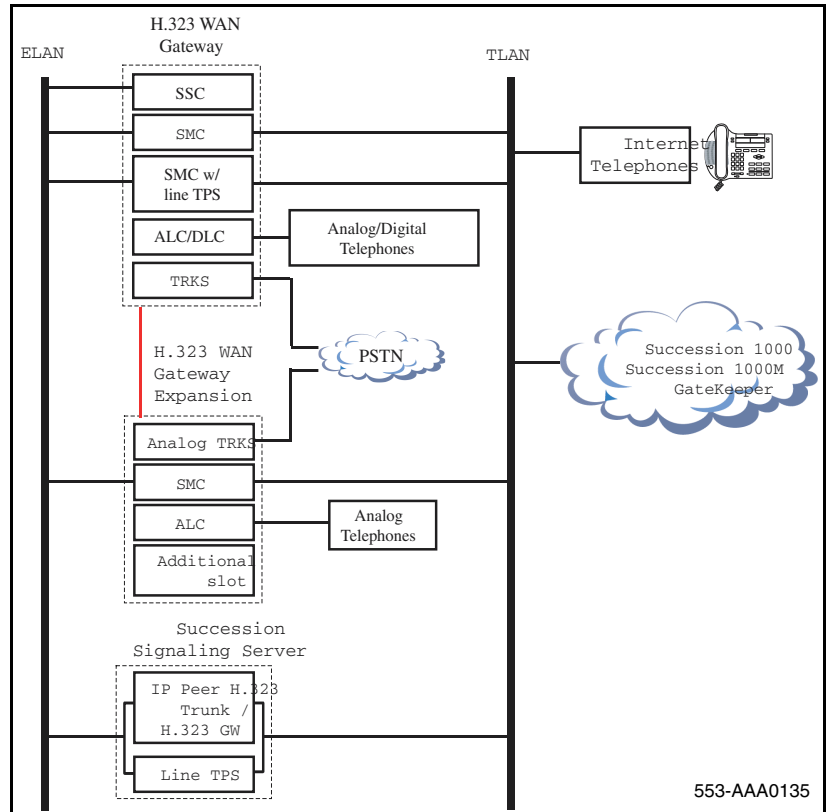
Mixed software operation between Main Office and Branch Office

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.

For information on upgrading software, refer to "Upgrading to Succession 3.0 Software" on .

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 Internet Telephone 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 "Telephones" on .

If you choose to upgrade only the Internet Telephone firmware, you must upgrade the Internet Telephone firmware at the existing Branch Offices first. The Main Office may or not require a Internet Telephone firmware upgrade, depending on its current version.

Refer to "Firmware downloads" on for more information on upgrading firmware for i2002 and i2004 Internet Telephones.

Survivability

The Succession Branch Office provides survivability against WAN failure, Main Office Succession Call Server failure, Succession Signaling Server failure, and Gatekeeper failure. Survivability is also provided during Main Office upgrade, including Succession Signaling Server and Succession Call Server upgrade.

In the event of a WAN failure, the Branch Office Internet Telephones lose communication with the Main Office TPS. This causes the Internet Telephones to reset and register with the Branch Office TPS and the SSC in the Branch Office H.323 WAN Gateway. The Internet Telephones operate in Local Mode, and receive call processing services from the SSC. In Local Mode, the Branch Office TPS tries to communicate with the Main Office TPS once every five minutes. Once communication is established with the Main Office TPS, the Branch Office Internet Telephones are redirected to the Main Office.

If the Main Office Succession Call Server fails and call processing services are provided by an alternate Succession Call Server, the Branch Office Internet Telephones register with the alternate Succession Call Server and receive call processing services from it. If no alternate Succession Call Server

is available, the Branch Office Internet Telephones stay registered with the Main Office TPS for ten minutes. At the end of the ten minutes, the Internet Telephones reset and register with the Branch Office SSC. If a key on a particular Internet Telephone is pressed before the end of the ten minutes, that telephone resets and registers with the Branch Office SSC immediately after the key is pressed.

When the Main Office Succession Signaling Server fails and an Alternate Succession Signaling Server is available, the Branch Office Internet Telephones reset and reregister with the Main Office Succession Call Server through the Alternate Succession Signaling Server, and continue to receive call processing services from the Main Office Succession Call Server. If no Alternate Succession Signaling Server is available, the Branch Office Internet Telephones reset and register with the Branch Office SSC. Internet Telephones that were registered with the Branch Office SSC before the Gatekeeper detected the Main Office Signaling Server failure are then redirected back to the Main Office and register with the Succession Media Card. These telephones stay in Normal Mode. Internet Telephones that registered with the Branch Office SSC after the Gatekeeper discovered the Main Office Signaling Server failure stay registered at the Branch Office.

When a Branch Office Internet Telephone powers up, it registers first with the Branch Office TPS, and second with the Branch Office H.323 WAN Gateway SSC. It is then redirected to the Main Office by the SSC. The Branch Office TPS queries the Primary Gatekeeper for the Main Office Virtual Trunk node IP address to redirect the Internet Telephone. If the Primary Gatekeeper is down or unreachable, the Branch Office TPS queries the Alternate Gatekeeper. If it receives a positive response, the Branch Office Internet Telephone is redirected to the Main Office. If the Alternate Gatekeeper is also down or unreachable, the Branch Office TPS queries the Failsafe Gatekeeper. If a successful response is received from the Failsafe Gatekeeper, the Internet Telephone registers with the Main Office. Otherwise, or if neither an Alternate Gatekeeper nor a Failsafe Gatekeeper is available, the Branch Office Internet Telephone remains in the Branch Office in Local Mode, and receives its call processing services from the Branch Office SSC.

Branch Office Internet Telephones in Normal Mode remain registered with the Main Office when the Primary Gatekeeper fails and no Alternate or Failsafe Gatekeeper is available. They can call any Main Office telephone or

other Branch Office Internet Telephones in Normal Mode. However, they cannot call any Branch Office digital telephones, analog (500/2500-type) telephones, or any external number through the Branch Office trunks in the normal way, because the Virtual Trunks are not available. (Branch Office digital or analog (500/2500-type) telephones are accessible if alternate routing is available through the PSTN.) The user has the option of staying in Normal Mode, or going to Local Mode manually by resetting the telephone or using Test Local Mode. In Local Mode, the Internet Telephones can make local calls to other Internet Telephones, digital telephones, and analog (500/2500-type) telephones at the Branch Office. They can also be used to make outgoing PSTN calls as usual.

>   *Note 1:* You must plan for, and obtain, the Primary and optional Alternate Gatekeeper addresses for installing the Branch Office software. Determine the Gatekeeper role, that is the Alternate or Failsafe configuration, for the Branch Office Succession Signaling Server.

>   *Note 2:* For CallPilot Mini and Call Pilot 201i applications, 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.

Network Bandwidth Management

Succession 1000 and Succession 1000M provides support for bandwidth management on a network-wide basis so that voice quality can be managed between multiple Succession Call Servers using IP Peer Networking in certain scenarios. The Network Bandwidth Management feature allows bandwidth zones to be configured on a network basis so that codec selection and bandwidth allocation software can identify whether Internet Telephones or gateways are physically co-located (in the same bandwidth zone) even though they are controlled by different Succession Call Servers.

For example, bandwidth zones can be configured on a network basis if Internet Telephones at the Branch Office are controlled by a Main Office Succession Call Server. In this configuration, all TDM devices, such as digital and analog (500/2500-type) telephones and trunks to the local PSTN, are under the control of the Branch Office SSC. In this case, calls from Internet Telephones to these TDM devices do not use any WAN (Interzone) bandwidth for media, and should, therefore, use the Intrazone algorithms for

bandwidth allocation and codec selection policy. Network Bandwidth Management provides a mechanism to identify this configuration and adjust the algorithms accordingly.

IMPORTANT!

Once all bandwidth is used, any additional calls will be blocked. Keep this in mind when designing and implementing Network Bandwidth Management.

To implement this feature, the Virtual Private Network Identifier (VPNI) prompt exists in LD 15. This enables the bandwidth management feature and expands the number of bandwidth zones beyond the current maximum of 256. When VPNI is set to its default value of 0, Network Bandwidth Management is disabled.

Network Bandwidth Management is implemented as follows:

1   The network-wide zone number, which is transported via MCDN within the SETUP message, must be captured and stored against the Virtual Trunk TN of the incoming call if the Virtual Private Network Identifier (VPNI) is the same as the terminating system. The combination of the VPNI and the zone is the Network Zone (Network Identifier + zone).

    After this point, all bandwidth management zone-based codec decisions should use the Network Zone, if it exists, instead of the protected zone that is configured against the Virtual Trunk TN.

    If the VPNI does not match (that is, the call is not from the same zone) or the Network Zone is not present (that is, VPNI is not configured or there is no third-party H.323 Gateway), then the zone configured in the protected Virtual Trunk TN block should be used. This ensures that all bandwidth usage and codec selection will be based on the Network Zone of the H.323 Gateways and stations involved in the call.

2   The H.323 protocol specifies that the 'Master', in terms of codec selection, is the terminator in the case of Fast Start (used with outgoing calls). The Master selects the codec and sends a list of preferences to the Slave, which uses what the Master prefers. This ensures that the terminating Succession Call Server knows both the originator's zone

(which it gets in the SETUP message) and the terminator's zone (which it gets from the local TN involved).

This should be changed so that the terminating Succession Call Server, which always knows the ZONEs involved, will always act as Master and the originating Succession Call Server will always act as Slave during any media path modifications. This ensures that the decisions are consistent at both ends and based upon the policy configured at the terminating Succession Call Server for the Network Zones involved.

3   At this point, the Succession Call Server has all the information about bandwidth usage at all Branch Offices. The bandwidth usage on the Branch Office side only gets updated for the first establish call. Any further call transfer or media redirection is not updated in the zone table.

For example, to manage bandwidth and codec selection between a Main Office Succession Call Server and a Branch Office, the following can be configured:

1   Assuming that a VPNI of 1 has been assigned to the area, the Main Office Customer Data Block would be configured with a VPNI of 1 in the Network section.

2   Assuming that a Branch Office ZONE of 5 has been assigned to the Branch Office location, the Internet Telephones would be configured at the Main Office with a ZONE of 5.

3   At the Branch Office, the Customer Data Block would also be configured with a VPNI of 1, and ZONE 5 would be configured on all VGMC DSP ports.

Using this configuration, calls from the Internet Telephone in ZONE 5 at the Main Office that terminate on the PSTN of the Branch Office using VGMC channels configured with ZONE 5 would be treated as Intrazone calls. Bandwidth usage at both the Main Office Call Server and Branch Office SSC would add to the Intrazone usage variables, and the codec selected according to the Intrazone policy (for example, typically Best Quality/G.711).

The Bandwidth Management policies of a Branch Office zone must be the same in the Main Office and in the Branch Office. Furthermore, matching codecs must be selected for resources in the Main Office and in the Branch Office to support the policies. If no matching codecs are selected for

the resources in the Main Office and the Branch Office for a policy, a speech path cannot be set up. As a result, no speech paths may occur in certain call scenarios. For more information, refer to "Zone parameters" on page 82 and page 156.

For example, assume the Virtual Trunks in the Main Office and the Branch Office do not have matching codecs for Best Bandwidth, and the policy for interzone bandwidth management is Best Bandwidth. In this case, a call between digital telephone in the Main Office and a digital telephone in the Branch Office will have no speech path.

Media redirection scenarios

In addition to basic call scenarios, Network Bandwidth Management also supports the following media redirection scenarios:

- Scenario 1: Codec switches correctly during media redirection. See Table 2 on page 35.

- Scenario 2: Call transfer works correctly with Branch Office:

  — Scenario 2.1: Call Transfer from Branch Office Internet Telephone in Normal Mode to Main Office Internet Telephone. See Table 3 on page 35.

  — Scenario 2.2: Call Transfer from Main Office Internet Telephone to Branch Office Internet Telephone in Normal Mode. See Table 4 on page 36.

- Scenario 3: Conference Call works correctly with Branch Office:

  — Scenario 3.1: Conference call between Branch Office and Main Office, initiated by Branch Office Internet Telephone in Normal Mode. See Table 5 on page 37.

Note 1: Scenario 3.2: Conference call between Main Office and Branch Office, initiated by Main Office Internet Telephone. See Table 6 on page 38.

Note 2: The zone table is examined using the commands in LD 117. See *Software Input/Output: Maintenance* (553-3001-511) for more information on these commands.

Note 3:   In these scenarios, consult the zone table at the Main Office for accurate bandwidth usage information.

Table 2
Scenario 1: Codec switches correctly during media redirection

Event	Result
1 An incoming DID call to Branch Office uses IP Peer to reach the symposium controller CDN in the Main Office.	1 The external caller hears music and announcements with a G.729 codec. Bandwidth usage in the Main Office indicates the call is an inter- zone call. The external caller is connected to an ACD agent with a G.711 codec. Bandwidth usage in the Main Office indicates the call is an intra-zone call. The ACD agent is a Branch Office Internet Telephone registered to the Main Office.
2 The call is released.	2 The zone table indicates the bandwidth usage for the call is removed correctly on the Main Office Succession Call Server, and in the Branch Office.

Table 3
Scenario 2.1: Call transfer from Branch Office Internet Telephone in Normal Mode to Main Office Internet Telephone (Part 1 of 2)

Event	Result
1 A Branch Office TDM telephone calls a Branch Office Internet Telephone registered to the Main Office.	1 A speech path is established between the Branch Office TDM telephone and the Branch Office Internet Telephone registered to the Main Office. The zone table indicates intra-zone bandwidth usage.

Table 3
Scenario 2.1: Call transfer from Branch Office Internet Telephone in Normal Mode to Main Office Internet Telephone (Part 2 of 2)

Event	Result
2 The Branch Office Internet Telephone registered to the Main Office initiates a call transfer to a Main Office Internet Telephone.	2 The Branch Office TDM telephone is put on hold. A speech path is established between the Branch Office Internet Telephone registered to the Main Office and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.
3 The Call Transfer key on the Branch Office Internet Telephone registered to the Main Office is pressed to complete the call transfer.	3 A speech path is established between the Branch Office TDM telephone and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.
4 The call is released.	4 The zone table indicates bandwidth usage for the call is unreserved correctly.

Table 4
Scenario 2.2: Call transfer from Main Office Internet Telephone to Branch Office Internet Telephone in Normal Mode (Part 1 of 2)

Event	Result
1 A Branch Office TDM telephone calls a Main Office Internet Telephone.	1 A speech path is established between the Branch Office TDM telephone and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.
2 The Main Office Internet Telephone initiates a call transfer to a Branch Office Internet Telephone registered to the Main Office.	2 The Branch Office TDM telephone is put on hold. A speech path is established between the Main Office Internet Telephone and the Branch Office Internet Telephone registered to the Main Office. The zone table indicates inter-zone bandwidth usage.

Table 4
Scenario 2.2: Call transfer from Main Office Internet Telephone to Branch Office Internet Telephone in Normal Mode (Part 2 of 2)

Event	Result
3 The Call Transfer key on the Main Office Internet Telephone is pressed to complete the call transfer.	3 A speech path is established between the Branch Office Internet Telephone registered to the Main Office and the Branch Office TDM telephone. The zone table indicates intra-zone bandwidth usage.
4 The call is released.	4 The zone table indicates bandwidth usage for the call is unreserved correctly.

Table 5
Scenario 3.1: Conference call between Branch Office and Main Office, initiated by Branch Office Internet Telephone in Normal Mode (Part 1 of 2)

Event	Result
1 A Branch Office TDM telephone calls a Branch Office Internet Telephone registered to the Main Office.	1 A speech path is established between the Branch Office TDM telephone and the Branch Office Internet Telephone registered to the Main Office. The zone table indicates intra-zone bandwidth usage.
2 The Branch Office Internet Telephone registered to the Main Office initiates a conference call to a Main Office Internet Telephone.	2 The Branch Office TDM telephone is put on hold. A speech path is established between the Branch Office Internet Telephone registered to the Main Office and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.

Table 5
Scenario 3.1: Conference call between Branch Office and Main Office, initiated by Branch Office Internet Telephone in Normal Mode (Part 2 of 2)

Event	Result
3 The Conference key on the Branch Office Internet Telephone registered to the Main Office is pressed to complete the conference call.	3 Speech paths are established among the Branch Office TDM telephone, the Branch Office Internet Telephone registered to the Main Office, and the Main Office Internet Telephone. The zone table indicates inter-zone and intra-zone bandwidth usage.
4 The Branch Office TDM telephone releases the call.	4 A speech path is established between the Main Office Internet Telephone and the Branch Office Internet Telephone registered to the Main Office. The zone table indicates inter-zone bandwidth usage.
5 The call is released.	5 The zone table indicates bandwidth usage for the call is unreserved correctly.

Table 6
Scenario 3.2: Conference call between Main Office and Branch Office, initiated by Main Office Internet Telephone (Part 1 of 2)

Event	Result
1 A Branch Office TDM telephone calls a Main Office Internet Telephone.	1 A speech path is established between the Branch Office TDM telephone and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.

Table 6
Scenario 3.2: Conference call between Main Office and Branch Office, initiated by
Main Office Internet Telephone (Part 2 of 2)

Event	Result
2 The Main Office Internet Telephone initiates a conference call to a Branch Office Internet Telephone registered to the Main Office.	2 The Branch Office TDM telephone is put on hold. A speech path is established between the Main Office Internet Telephone and the Branch Office Internet Telephone registered to the Main Office. The zone table indicates inter-zone bandwidth usage.
3 The Conference key on the Main Office Internet Telephone is pressed to complete the conference call.	3 Speech paths are established among the Branch Office TDM telephone, the Branch Office Internet Telephone registered to the Main Office, and the Main Office Internet Telephone. The zone table indicates inter-zone and intra-zone bandwidth usage.
4 The Branch Office TDM telephone releases the call.	4 A speech path is established between the Branch Office Internet Telephone registered to the Main Office and the Main Office Internet Telephone. The zone table indicates inter-zone bandwidth usage.
5 The call is released.	5 The zone table indicates bandwidth usage for the call is unreserved correctly.

Network Bandwidth Management configuration

Zone configuration considerations

Do not configure Zone 0, the default zone, as a Branch Office zone. Network Bandwidth Management does not support zone 0. If zone 0 is configured as a Branch Office zone, the Bandwidth Management feature will not be activated.

Configure available bandwidth for a zone with LD 117 or Element Manager. In the Main Office, configure actual inter-zone and intra-zone available bandwidth. In the Branch Office, set the inter-zone and intra-zone bandwidth parameters to their maximum configurable value.

Configure preferred strategy for a zone with LD 117 or Element Manager. For zones in the Main and Branch Offices associated with Virtual Trunks, set the inter-zone and intra-zone preferred strategies to Best Quality (BQ).

Data configuration example

This example outlines how Network Bandwidth Management zones is configured.

1   At the Main Office:

   a   Define a VPNI number in LD 15

   b   Configure the following in LD 117:

   • Main Office zone with the following properties:

      — Intra-zone Preferred Strategy = Best Quality (BQ)

      — Intra-zone Bandwidth = default (10 000)

      — Inter-zone Preferred Strategy = Best Bandwidth (BB)

      — Inter-zone Bandwidth = maximum bandwidth usage allowed between the Main Office and the Branch Office(s).

   • Branch Office zone with the following properties:

      — Intra-zone Preferred Strategy = Best Quality (BQ)

      — Intra-zone Bandwidth = default (10 000)

      — Inter-zone Preferred Strategy = Best Bandwidth (BB)

      — Inter-zone Bandwidth = maximum bandwidth usage allowed between the Succession Call Server and the Branch Office

   • DSP zone with the following properties:

      — Intra-zone Preferred Strategy = Best Quality (BQ)

— Intra-zone Bandwidth = default (10 000)

— Inter-zone Preferred Strategy = Best Bandwidth (BB)

— Inter-zone Bandwidth = default (10 000)

- Virtual Trunk zone with the following properties:

— Intra-zone Preferred Strategy = Best Quality (BQ)

— Intra-zone Bandwidth = default (10 000)

— Inter-zone Preferred Strategy = Best Quality (BQ)

— Inter-zone Bandwidth = default (10 000)

  c Configure the Internet Telephone, DSP and Virtual Trunk data with the corresponding zone numbers defined in LD 117.

2 At the Branch Office:

  a Define the same VPNI number in LD 15 as defined in the Main Office.

  b Configure the following in LD 117:

- Branch Office zone associated with the Main Office with the following properties:

— Zone number = Zone number defined in Main Office

— Intra-zone Preferred Strategy = Best Quality (BQ)

— Intra-zone Bandwidth = maximum allowable configurable (1 000 000)

— Inter-zone Preferred Strategy = Best Bandwidth (BB)

— Inter-zone Bandwidth = maximum allowable configurable (1 000 000)

Note: The DSP uses the same Branch Office zone number.

- Virtual Trunk zone associated with the Main Office with the following properties:

— Intra-zone Preferred Strategy = Best Quality (BQ)

— Intra-zone Bandwidth = default (10 000)

> — Inter-zone Preferred Strategy = Best Quality (BQ)

> — Inter-zone Bandwidth = Inter-zone Bandwidth defined for the corresponding Branch Office zone at the Main Office

c Configure the Internet Telephone and DSP data with the Branch Office zone number, and the Virtual Trunk with the corresponding zone number defined in LD 117.

How the Branch Office works

The Branch Office connects to the Main Office using Virtual Trunks over the WAN. Virtual Trunks are software components that provide the trunking features of the Meridian Customer-Defined Networking (MCDN) feature set. The Main Office and the Branch Office are configured as Electronic Switched Network (ESN) nodes, connected by Virtual Trunks. The Branch Office H.323 WAN Gateway provides a trunk gateway to the PSTN. Access to PSTN digital or analog trunks at the Branch Office H.323 WAN Gateway occurs through the MCDN Virtual Trunk.

For more information on Virtual Trunks, refer to *IP Peer Networking* (553-3001-213). For more information about Electronic Switched Networking (ESN), refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180).

H.323 WAN Gateway interoperability

H.323 WAN Gateway to H.323 WAN Gateway interoperability is fully supported between Succession 1000 and Multimedia Communications Server (MCS) 5100. 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 MCS5100 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 MCS5100 H.323 Gatekeeper and the Succession 1000 H.323 Gatekeeper.

Normal Mode operation

The Main Office provides centralized call processing for the Branch Office Internet Telephones in Normal Mode. The Branch Office Internet Telephones are configured at the Main Office Succession Call Server. These telephones are registered to the Main Office TPS and are controlled by the Succession Call Server at the Main Office.

Users of the Internet Telephones in the Branch Office (that is, Branch Users) receive the features, key layout, and tones of the Main Office Succession Call Server. This provides feature and application transparency between Branch Office and the Main Office.

Internet Telephone calls

When an Internet Telephone calls another Internet Telephone, each telephone receives the address of the other to exchange media directly between the telephones. Also note that when in Normal Mode, a Branch Office Internet Telephone calling a Main Office Internet telephone does not require any trunking to setup the call. However, WAN bandwidth is used to provide a media path for the call. For more information on Direct IP media path functionality, see *IP Peer Networking* (553-3001-213).

Zones

A zone is a collection of Internet Telephones that:

- share similar IP bandwidth restrictions

- are geographically close to one another

- are all in the same time zone

- are all in the same PSTN dialing plan

For dialing plan purposes, all telephones in the same zone are treated identically. Each Internet Telephone is assigned to a zone during configuration.

Internet Telephones at a Branch Office are configured within a unique zone (a set of zones can also be provisioned, such as for floors of a building). In the Main Office Succession Call Server, Internet Telephones at the Branch Office are assigned to a Branch Office zone to define the numbering plan for local, long distance (optional), and emergency services calls. Zone configuration modifies the dialed digits so a local, long distance (optional) or emergency services call can be sent to an H.323 Gatekeeper as a long distance call. This zone configuration data enables the Main Office Succession Call Server to modify the dialed digits for these types of calls initiated from a Branch Office telephone. The H.323 Gatekeeper then provides the endpoint information to route the call to the Branch Office.

Note: Throughout this document, the term "zone" is defined as a Bandwidth Management Zone, not a Gatekeeper Zone. Refer to "Network Bandwidth Management" on .

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 Virtual 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.

Time of Day

The idle clock on the telephone display must be localized to the correct time for the geographic location of the Internet Telephone (the Succession Call Server updates this information on the telephone). The date and time display

on the Internet Telephone is determined by the Succession Call Server or SSC to which the telephone connects.

Because Branch Offices can be located in regions with a different time zone than the Main Office, the Branch Office supports a feature that enables a different time zone at the Main Office and the Branch Office. The time zone of the Branch Office is configured with the Branch Office zone at the Main Office. The time zone adjusts the Main Office time for display at the Branch Office. Idle Branch Office telephones then display the correct time of the Branch Office, rather than that of the Main Office.

Branch Office Internet Telephone to local PSTN

When a Branch Office Internet Telephone in Normal Mode dials a local PSTN number, the call is processed by the Main Office Succession Call Server. The dialed digits are modified according to the dialing plan information configured in the zone for the Branch Office Internet Telephone.

The call is configured to be routed over the Virtual Trunk to the Branch Office. The Branch Office SSC then tandems the call to the local PSTN.

This implementation can optionally be implemented for long distance calls over PSTN trunks.

IMPORTANT!

If you are using one Access Code for both local and long distance, and that Access Code is associated with a Branch Office zone, all calls (local and long distance) will be routed through that Branch Office.

For more information, see "Dialing plan configuration" on

Internet Telephone to analog (500/2500-type) or digital telephone calls

When a Branch Office Internet Telephone in Normal Mode calls an analog (500/2500-type) or digital telephone in the Branch Office, the call is processed at the Main Office Succession Call Server. A Virtual Trunk route is selected according to the digits dialed. The call is routed over a Virtual

Trunk to the Branch Office. The Branch Office SSC processes the incoming Virtual Trunk call and terminates it to the local analog (500/2500-type) or digital telephone. Since this is a call between IP and circuit-switched devices, a DSP resource on a Succession Media Card is allocated and connected to the analog (500/2500-type) or digital telephone. The IP address of the DSP resource is returned to the Main Office Call Server so a direct media path between the Internet Telephone and the DSP resource can be set up when the call is established. Refer to *IP Peer Networking* (553-3001-213) for details.

Incoming calls from the local PSTN

The Vacant Number Routing (VNR) feature must be configured on the Branch Office SSC to route all vacant numbers to the Main Office. An incoming Central Office trunk call can be configured to terminate at the local attendant console, an analog (500/2500-type) telephone, or a digital telephone. It can also be routed to a remote attendant console, a Branch Office Internet Telephone, or an analog (500/2500-type) or digital telephone in the Main Office. Direct-Inward-Dial (DID) calls from local PSTN trunks are routed according to the destination DNs. Incoming calls to Branch Office Internet Telephones in Normal Mode are routed to the Main Office Succession Call Server over the Virtual Trunks. Calls to local analog or digital devices are terminated locally.

Conference calls

When a conference call is initiated by a Branch Office user, the conference facilities of the Main Office are used. This means that in a conference among three Branch Users, the WAN bandwidth of three media paths is used. The Main Office is where the calls are controlled, except in Local Mode where local resources are used instead.

In sites with limited WAN bandwidth between the Main Office and the Branch Office, and with heavy conference traffic among Branch Users, the Meridian Integrated Conference Bridge (MICB) card can be installed in the Branch Office H.323 WAN Gateway or the Branch Office H.323 WAN Gateway Expansion. This configuration provides a "meet-me" conference facility, and reduces WAN bandwidth usage requirements.

Local Mode

Note: Also see "Survivability" on .

Operation—survivability of Internet Telephones

If the Branch Office Internet Telephone loses communication with the Main Office, the SSC in the Branch Office H.323 WAN Gateway provides the call processing for the telephone. While the Branch Office Internet Telephones are being provided with service at the Branch Office, the telephone display shows "Local Mode".

When a Branch Office telephone is in Local Mode, the user has full access to services configured at the Branch Office (analog or digital devices, analog or digital trunks) and to other Internet Telephones registered to the Branch Office. With proper ESN configuration, the Branch Office user can also access Internet Telephones at the Main Office or other Branch Offices by routing through the local PSTN.

IMPORTANT!

When a telephone or trunk in the Main Office calls a Branch Office Internet Telephone in Local Mode, the call is treated according to the Main Office call redirection configuration (such as forwarding to voice mail or continuous ringback).

When the telephone detects that it has lost communication with the Main Office, it reboots and registers to the TPS at the Branch Office. This means that, depending on the network configuration (or the point of failure in the network), not all Branch Office Internet Telephones go into Local Mode at the same time. Calls are not maintained during switchover from Normal Mode to Local Mode.

Internet Telephones that are in Local Mode due to a network or Main Office failure are automatically redirected to the Main Office when connectivity is restored. Established calls are completed before the switchback from Local Mode to Normal Mode.

To provide survivability for the Internet Telephones, the Branch Office Internet Telephones must be provisioned on both the Succession Call Server at the Main Office and the SSC in the Branch Office. See "Installing and configuring Internet Telephones" on .

If a Branch Office is running a software release prior to Succession 3.0 Software, and it is associated with more than one Main Office, a lost connection to one of the Main Offices does not automatically lose the connections to the other Main Offices. However, new redirections to those other functional Main Offices may not be successful.

Features supported in Local Mode

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 different 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.

A user can attempt a Virtual Office Login to a Branch User from a Branch Office Internet Telephone in Local Mode. If the Virtual Office Login is successful, the Virtual Office user will be registered with either the Branch Office or Main Office.

If the network is using CDP, the Network Ring Again (NRGN) feature does not work for a Branch User in Local Mode. In the CDP environment, the Gatekeeper database configures the Main Office as the endpoint for the Branch User DN. The Virtual Trunk obtains the endpoint of NRGN response messages from the Gatekeeper. It sends admission requests to the Gatekeeper with the Branch User DN. The Gatekeeper returns the address associated with the destination DN. In this case, the returned address is that of the Main Office.

The following are not available in a Branch Office running a software release prior to Succession 3.0:

- automatic redirection to the Main Office following an MOTN or BUID configuration change for a Branch User in Local Mode

- when the Main Office is a Succession 1000 or a Succession 1000M Small System, the Main Office TN differs from the Branch Office TN for a given Branch User

- Abbreviated Dialing – see "Dialing plan configuration" on

- enhancements to the ISS and ISSP prompts in LD 22 to indicate the Branch Office – see "Branch Office software and system information" on

Licensing

There is a licensing feature for the Internet Telephones in the Branch Office that notifies Branch Office administrators of a license violation—the extended use of a Branch Office Internet Telephone in Local Mode.

Operation of Internet Telephones in Local Mode is meant to provide survivability during conditions of network failure only. It is not intended for prolonged operations. Therefore, a License Period of 30 days is allowed for Internet Telephones in a Branch Office to stay in Local Mode. When the License Period expires, a BUG0103 system message is written to the Branch Office SSC log file. The message is also printed on the teletype terminal (TTY). The Internet Telephones are reset at the end of every call, and try to register with the Main Office.

When nine or fewer days remain on the licensing feature, Internet Telephones display a "Licensed days left: n" message to indicate how many days you can use the Branch Office in Local Mode. This message also appears as a banner when the technician logs into a maintenance terminal. After the license has expired, Internet Telephones in Local Mode display "Beyond Licensed Period".

The license feature is based on a debit and credit system for the amount of time the Internet Telephones have been registered to the Main Office or Branch Office. Credits are in two-hour units. After a software upgrade, 360 initial credits, equivalent to a 30-day period, are provided. The total credits

are reduced by one every time one or more Internet Telephones stay in Local Mode for two hours. The total credits are increased by one for every two hours that one or more Internet Telephones are registered with the Main Office. Total credits cannot exceed 360 credits, or 30 days.

Testing the telephone in Local Mode

From Normal Mode, a Branch Office user can use Test Local Mode to test telephone functionality in Local Mode. It can be performed by the user at any time and does not require a password. This test is invoked from the Internet Telephone.

Nortel Networks recommends testing Local Mode operation after changing the provisioning for a telephone on the Branch Office SSC.

To ensure that users do not forget to resume Normal Mode operation, the Branch Office TPS redirects the telephone to the Main Office to return the telephone to Normal mode. This occurs if the telephone remains registered to the Branch Office in Test Local Mode for ten minutes. Alternatively, the user can select Resume Normal Mode from the Options menu.

Internet Telephones with the same DN at the Branch Office

When the Branch Office SSC processes incoming calls from a local trunk or from an analog (500/2500-type) or digital telephone, the SSC determines if the dialed DN is a Multiple Appearance DN (MADN). If any telephone in an MADN arrangement is analog or digital, or if one or more Internet Telephones are registered in Local Mode at the Branch Office, the call terminates at the Branch Office. In this case, the analog (500/2500-type) or digital telephones, and the Internet Telephones registered to the Branch Office, ring. Internet Telephones registered to the Main Office do not ring.

In other words, if the Branch Office SSC can terminate the call to any telephone in the Branch Office that belongs to the MADN arrangement, the call does not reroute to the Main Office.

Internet Telephones with the same DN at the Main Office

If a call is made to an MADN at the Main Office, all MADN appearances, including those on Branch Office Internet Telephones in Normal Mode, ring. Any appearance can answer the call. MADN appearances on Branch Office Internet Telephones in Local Mode do not ring.

Emergency services

Support for access to emergency services by a Branch Office user in Normal Mode is configured at the Main Office.

The key difference between the Main Office user and the Branch Office user is the route selected for the emergency call. An emergency call must be handed off to the PSTN over a trunk at the central office that is geographically closest to the caller—this means that there is normally an emergency trunk in the Main Office, and one in each of the Branch Offices. An emergency call originating from an Internet Telephone in the Branch Office must route from the Main Office Succession Call Server to the Branch Office Succession System Controller so that the call can be sent on the Branch Office PSTN.

IMPORTANT!

In Normal Mode, an Internet Telephone must have a Virtual Trunk available and configured between the Main Office and Branch Office in order to complete an emergency services call.

There are two general methods to specify which digit string results in a call to emergency services:

- Use the Emergency Services Access (ESA) feature. This is the preferred method in North America. ESA provides specific features and capabilities required by legislation in North American jurisdictions.

- Use a special dialing sequence, such as a Special Number (SPN) in the Network Alternate Route Selection (NARS) data block.

Configuring ESA for emergency services

The ESA configuration specifies the digit sequence (a DN) that the user dials to start an emergency call, known as the ESDN. There can only be one ESA configuration per customer and thus only one ESDN per customer, which means that all telephones on the same network must be in the same numbering plan.

If the Branch Office and the Main Office do not use the same digits for emergency calls, it is not possible to use ESA at both locations. Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for complete information.

With all sites using the same ESDN, there is a conflict in the Gatekeeper. This is resolved by using a unique prefix for each site, which the Main Office adds as it routes the call. The suggested prefix is the ESN home location code of the Branch Office Succession Call Server, or alternately, the Number Plan Area (NPA) code of the Branch Office Succession Call Server if there is not more than one Succession Call Server in the NPA. Virtually any unique string can be used as a prefix because the call is sent to the Gatekeeper as an SPN. In the Gatekeeper, SPNs have their own separate numbering plan.

The Automatic Number Identification (ANI) data sent to the Public Safety Answering Point (PSAP) identifies the location of the caller. In some constituencies, legislation requires one DID per fixed number of square feet, so the physical location of the emergency can be approximated based on the telephone number delivered to the PSAP. The ESA feature has a comprehensive scheme that can be used to convert an extension into an appropriate DID.

If the Branch Office is relatively small, it can be easier to use a single, fixed DID number for the Branch Office. This can be configured using the CHG ZESA command in LD 117, where the <ESALocator> parameter is the DID telephone number to be sent for use by the PSAP to locate the source of the emergency call. For more information on this command, refer to *Software Input/Output: Maintenance* (553-3001-511).

Configuring SPN for emergency services

Using an SPN for access to emergency services uses the digit manipulation capabilities configured for the Branch Office zone as follows:

• For a Branch Office Internet Telephone in Normal Mode, the user dials the Access Code for the local PSTN and the normal DN for emergency services.

  If the Main Office and Branch Office use the same DN for accessing emergency services, there is a conflict in the Gatekeeper. This is resolved by using the Zone Dialing Plan (ZDP) configured in the Branch Office. The digits specified by the ZDP are prefixed to the dialed digits, and the call is then sent to the Gatekeeper as an SPN. In the Gatekeeper, the SPNs have their own separate numbering plan, so the call is routed to the Branch Office SSC so that it can be sent out to the Branch Office PSTN.

• For a Branch Office user in Local Mode (or an analog (500/2500-type) or digital telephone at the Branch Office), the user dials the Access Code for the local PSTN and the normal DN for emergency services access. This selects the appropriate trunk for local PSTN access.

Abbreviated Dialing

The Abbreviated Dialing feature allows users in the same geographic location—the Main Office or the Branch Office—to call one another with a DN shorter than the configured DN. Existing pretranslation capability inserts the digits that are not dialed, and the call is processed as usual.

This feature is implemented with a pretranslation group assigned to every telephone. All Internet Telephones in the same bandwidth management zone use the same pretranslation group. TDM telephones, which share the same dialing plan with Internet Telephones in a bandwidth management zone, also use the same pretranslation group.The pretranslation group assignment is more easily and quickly done using the OTM global change functionality.

gives some sample values to help explain the functionality of Abbreviated Dialing.

Table 7
Sample values for Abbreviated Dialing

	Main Office	**Branch Office**
Location code	70	71
DN	703000	713000

Using the sample values from Table 7, Abbreviated Dialing works as follows:

- An Internet Telephone or TDM telephone in the Main Office can call another telephone in the Main Office by dialing only the last four digits of the called party's DN (for example, "3000" to reach "703000").

- An Internet Telephone in the Branch Office, in Normal or Local Mode, or a TDM telephone in the Branch Office can call another telephone in the Branch Office by dialing only the last four digits of the called party's DN (for example, "3000" to reach "713000").

- An Internet Telephone or TDM telephone in the Main Office can call a telephone in the Branch Office by dialing all six digits of the called party's DN (for example, "713000").

- An Internet Telephone in the Branch Office, in Normal or Local Mode, or a TDM telephone in the Branch Office can call a telephone in the Main Office by dialing all six digits of the called party's DN (for example, "703000").

- An incoming call to a Main Office telephone has a four-digit DN, such as "3000". The Main Office location code (in this example, "70") is added to the front of the DN, and the call terminates as indicated by the full-length DN (in this case, "703000").

- An incoming call to a Branch Office telephone has a four-digit DN, such as "3000". The Branch Office location code (in this example, "71") is added to the front of the DN, and the call terminates as indicated by the full-length DN, in this case "713000". In Local Mode, the call is terminated locally. In Normal Mode, the call is routed to the Main Office using VNR.

- CLID on outgoing PSTN calls from the Main Office or the Branch Office are modified from four to six digits. Additional digits can be added using the capabilities of CLID.

- The calling party display always shows the full-length DN of the originating party.

- The display on the calling telephone shows the called DN as dialed. After the call is established or modified, the display changes in accordance with existing features.

Supported applications

OTM 2.1, MICB 3.xx, MIRAN, CallPilot Mini, and CallPilot 201i are supported in the Branch Office.

Planning and management

Contents

This section contains information on the following topics:

Data network planning

Verify compliance with network requirements for system expansions. Refer to *Data Networking for Voice over IP* (553-3001-160). In particular, concentrate on the following:

- delay

- packet loss

- jitter

CAUTION — Service Interruption

If the network is planned so Internet Telephones use a different route to the Main Office than the Branch Office TPS, a fault condition can occur. When the Branch Office TPS can "ping" the Main Office but the Internet Telephone cannot "ping" the Main Office due to a network outage, an Internet Telephone registration can force the telephone into a cycle of registering locally, being redirected to the Main Office, rebooting and then registering locally again. When this cycle occurs, further diagnose the network outage.

WAN bandwidth requirements

The WAN bandwidth requirement between the Main Office and Branch Office consists of two components —one for the media path and the other for signaling and background tasks.

The WAN bandwidth requirement for the media path depends on the following factors:

- traffic pattern at the Branch Office

- chosen packetization delay

- Voice Activity Detect

- codec

- Link type

Detailed information about traffic information is contained in
Succession 1000 System: Planning and Engineering (553-3031-120). An
example for the Branch Office is given in "Branch Office engineering
example" on .

Signaling and background tasks that use WAN bandwidth include:

- Gatekeeper polling

- Gatekeeper database synchronization

- Endpoint registration requests to Gatekeeper

- Lamp Audit

- Internet Telephone Keep Alive messages

- Call signaling to and from Internet Telephones

The maximum bandwidth required for these activities is approximately
13 Kbps. This is insignificant when compared to the bandwidth requirement
for the expected voice traffic.

Therefore, when determining the WAN bandwidth requirement for a
Branch Office, expected voice traffic should be the major factor.

Branch Office dialing plan

Since Internet Telephone users can be located at a Branch Office equipped
with an H.323 WAN Gateway, the routing of calls to the local gateway is
important (especially when toll charges apply to calls made from the central
Succession Call Server that controls the telephone). The administrator can
configure digit manipulation through zone attributes for Internet Telephones
to select a Main Office or Branch Office gateway that provides PSTN access
local to the destination of the call.

> *Note:* The Branch Office supports the various PSTN interfaces. Refer to
> *Electronic Switched Network: Signaling and Transmission Guidelines*
> (553-3001-180) for further information.

Calls from the PSTN to users within the network can be routed with the
various ESN numbering plan configurations or the Vacant Number Routing

(VNR) feature. This enables small sites, such as the Branch Office, to require minimal configuration to route calls through other Succession Call Servers or through the Gatekeeper.

To access local PSTN resources, outgoing calls can be routed using ESN as well as zone parameters that enable digit insertion. The zone parameters force calls made by a Branch Office user to be routed to the desired local PSTN facilities.

> *Note:* Outgoing calls can include local and, optionally, long-distance calls.

For more information about PSTN configuration, see "Configuration example for PSTN resources at the Branch Office" on .

Nortel Networks recommends that the Branch Office user ID be the same at the Branch Office as the DN at the Main Office. A Branch Office user ID has a maximum of 15 digits. Under the recommended Coordinated Dialing Plan (CDP), it can be an extension (for example, 4567). Under the Uniform Dialing Plan (UDP), it is the user's Main Office DN, the Location Code (LOC), plus the Access Code (for example, 6 343-5555).

> *Note:* The Main Office DN must be an Electronic Switched Network (ESN)-compliant DN. See "ESN access or location codes" on .

For more information about CDP, refer to *Dialing Plans: Description* (553-3001-183). For details on other Numbering Plan options, refer to *Succession 1000 System: Overview* (553-3031-010). For more information on ESN, refer to "ESN access or location codes" on .

Emergency Services

To understand Emergency Service Access (ESA), see "Emergency services" on . The Main Office Succession Call Server supports only one Emergency Service DN (ESDN). If the ESDN is different at the Branch Office and at the Main Office, or if there is more than one emergency number, then a Special Number (SPN) must be configured to route ESA calls from the Branch Office telephone to the Branch Office PSTN. Refer to "Emergency Services configuration" on .

Zones

The Branch Office feature enables Internet Telephones to be located in more than one geographic location to have dialing plan behaviors that are localized to the location of the telephone rather than the location of the Main Office Succession Call Server. Use different zone numbers for different Branch Offices. Refer to *Succession 1000 System: Planning and Engineering* (553-3031-120).

Music on Hold

For Branch Office users in Normal Mode, the Main Office provides music to the user if Music on Hold is provisioned. The use of the G.729A/AB and G.723 codecs between the Main Office and the Branch Office impacts the music quality.

ESN access or location codes

ESN data is configured with two Access Codes called AC1 and AC2. AC1 normally applies to long distance calls, whether placed on or off the customer's private network (for example, dialing "6"). AC2 normally applies to local calls (for example, dialing "9"). For more information, refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180).

Provisioning the Internet Telephones

Users must provision the Internet Telephone on any Succession Call Server or SSC that provides service to that telephone. There is no automatic data synchronization between the Main Office Succession Call Server and the Branch Office SSC.

There is a procedure in OTM to transfer Internet Telephone data from the Main Office to the Branch Office. See "Transferring Internet Telephone data using OTM" on .

Configuration example for PSTN resources at the Branch Office

Internet Telephones registered to the Main Office Succession Call Server can be grouped into one of two categories:

- those configured with a Main Office dialing plan, similar to any other non-Internet Telephone at the Main Office

- those configured with a Branch Office dialing plan because the telephone is physically located in a Branch Office

Customer data must first be configured to recognize numbers that are local to each location (a standard NARS configuration issue). This example specifically focuses on the additional changes necessary to physically enable a Branch Office telephone, registered with the Main Office Succession Call Server, to reach PSTN resources in the Branch Office.

Note: Assume that the Main Office and Branch Office have been configured with local numbers, such as 555-1212 or 967-1111.

Table 8 uses the following configuration at the Main Office for Branch Office telephones to reach the PSTN.

Table 8
Example dialing string, area codes, and Access Codes (Part 1 of 2)

	At the Main Office node	**At the Branch Office node**
Local dialing string	Local calls use 7-digit dialing	Local calls use 7-digit dialing
Area code (NPA)	The NPA is 613	The NPA is 506
Country code	The Main Office Node Country Code is 1	The Branch Office Node Country Code is 1
NARS configuration	Local calls use AC2, which is "9" Long distance calls use AC1, which is "6"	Local calls use AC2, which is "9" Long distance calls use AC1, which is "6"

Table 8
Example dialing string, area codes, and Access Codes (Part 2 of 2)

	At the Main Office node	**At the Branch Office node**
The Public National (E.164) entry points to...	"506" points to Branch Office node	"613" points to Main Office node

At the Main Office, the following items must be configured:

- Long distance numbers in the same area code, such as 1-613-531-1234 or 1-613-320-1234.

- Long distance numbers at the Branch Office are configured to go over the Virtual Trunk and use PSTN trunks at the Branch Office, such as 1-506-555-1212 or 1-506-472-1234.

- All other long distance numbers have other routing as appropriate (1-NPA-NXX-XXXX).

At the Branch Office, the following items must be configured:

- Long distance numbers in the same area code, such as 1-506-234-1234 or 1-506-675-1234.

- Long distance numbers at the Main Office are configured to go over the Virtual Trunk and use PSTN trunks at the Main Office, such as 1-613-967-1111 or 1-613-555-1212.

- All other long distance numbers have other routing as appropriate (1-NPA-NXX-XXXX), but most are routed through the Main Office.

If a Main Office telephone goes off-hook and dials "9 555-1212", the Call Server assumes the user intends to reach the number 555-1212 in the local NPA. The fully-qualified number (E.164) is 1-613-555-1212.

If a Branch Office Internet Telephone goes off hook and dials "9 555-1212", the Branch Office Succession System Controller (SSC) assumes that the user intends to reach the number 555-1212 in the NPA that is local to the Branch Office, and thus the fully qualified number (E.164) is 1-506-555-1212.

Since the Main Office must reach the Branch Office PSTN resources (through the Branch Office H.323 WAN Gateway), the call is treated like a PSTN toll-avoidance call. (This is a private-network-routed call with public network termination.)

For other examples, such as calls between different NPAs within the same city, refer to the "Dialing plan configuration" on .

Zone configuration description

Configuration Branch Office features on the Internet Telephones using the Branch Office zone characteristics in LD 117 at the Main Office. For example, assuming that telephones in the Branch Office are in zone 10, use the commands given in LD 117 – Zone configuration example.

LD 117 – Zone configuration example. (Part 1 of 2)

Command	Description
CHG ZBRN 10 YES	
	Sets the flag that shows (literally, in the PRT ZONE output) whether the zone is a Main Office or Branch Office zone.
CHG ZACB 10 AC2 AC1	
	Tells the system the NARS Access Codes for local dialing and the NARS Access Code to convert the call into a long distance call, to route the call to the Branch Office. In this case we are converting a call, such as "9 555-1212" into the call "6 1 506 555-1212", a conversion from AC2 to AC1.
CHG ZDP 10 1 506	
	Specifies the additional digits needed to convert a local call to a long distance call. In this case, insert the PSTN Access Code for long distance (which also happens to be the country code in North America) and the NPA into the digit string. The system can recognize when these values are already present, so if the user were to dial "9 506 555-1212" only the "1" would be added when the conversion to "6 1 506 555-1212" is performed.

LD 117 – Zone configuration example. (Part 2 of 2)

Command	Description
ENL ZBR 10 LOC	
	Enables the Branch Office zone behaviors. Other options can be enabled or disabled separately. For instance, the LOC command turns on the local dialing option, also called "dial 9 for outside line". This can also be applied to long distance calls originating in the Branch Office.

The dialed digits can now be converted to a long distance format. It is up to NARS to partially route the number over the private network to take advantage of any long distance benefits.

Management

The following sections pertain to Branch Office management. Refer to *System Management* (553-3001-300).

Remote Access

Remote Access to the Branch Office SSC is available through Ethernet connection or remote login through a dial-up modem.

Element Manager

The Element Manager application:

- configures the Succession Media Card for IP Line 3.1

- configures the Internet Telephone Terminal Proxy Server (TPS)

- configures the Virtual Trunks

- upgrades the Succession Media Card

- upgrades the Internet Telephone firmware

- manages Succession 1000 and Succession 1000M information, such as:

    — customer data

— routes

— trunks

— the IP telephony node

— Electronic Switched Network (ESN) data

— Digital Signal Processing (DSP) channels

— Branch Office zone features

— Emergency Services Access at the Branch Office

— Daylight Savings Time at the Branch Office

For configuration procedures, refer to *Succession 1000 System: Installation and Configuration* (553-3031-210), *Large System: Installation and Configuration* (553-3021-210), or *Small System: Installation and Configuration* (553-3011-210).

For upgrade procedures, 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).

OTM 2.1

Optivity Telephony Manager (OTM) Release 2.1 supports all Windows and web-based applications for Branch Office, similar to the Succession 1000 and Succession 1000M systems. OTM allows customers to configure Internet Telephone data for use in survivable mode.

When using OTM Station Administration for Internet Telephones, it is possible to copy and paste an Internet Telephone from one system to another. Refer to Procedure 20 on page 176 and Procedure 21 on page 180. This can be useful for provisioning the Internet Telephone data on both the Main Office and Branch Office.

Set-Based Installation for Internet Telephones

Nortel Networks recommends using Set-Based Installation for Branch Office Internet Telephones. Set-Based Installation takes less time than traditional telephone installation.

The procedure for Set-Based Installation enables the delegation of telephone installation to trusted users. To have a trusted user perform this function, configure a Temporary Internet Telephone Installer's Password for the system. See "Internet Telephone passwords and parameters" on . To proceed with Set-Based Installation, see Procedure 18 "Using Set-Based Installation" on .

Automatic Set Removal

The Automatic Set Removal feature enables the technician or a trusted user to remove the Internet Telephone configuration from the system. This feature requires a Flexible Feature Code (FFC) and a set relocation password. The FFC code is the Automatic Set Removal (AREM) in LD 57, and the set relocation password is the Set Relocation Security Code (SRCD) in LD 15.

Traffic measurement

Traffic measurement at the Branch Office includes calls involving local trunks, Virtual Trunks, and analog and digital devices. It does not include calls of Branch Office Internet Telephones in Normal Mode with any terminal at the Main Office, or any other Branch Office in the network. However, Internet Telephones calls to devices or local trunks at the Branch Office are counted as incoming Virtual Trunk calls to the analog or digital devices or local trunks.

When an Internet Telephone is in Local Mode, any calls to or from the Internet Telephone are included in the traffic measurement at the Branch Office.

Call Detail Recording

There is no change to the existing Call Detail Recording (CDR) format.

CDR at the Branch Office reports calls processed at the Succession Media Gateway SSC. CDR includes:

*   incoming Virtual Trunk calls to local devices

*   incoming Virtual Trunk calls to outgoing local analog and digital trunks

*   incoming local trunks (analog and digital) to outgoing Virtual Trunks

- incoming local trunk calls to local devices

- local device calls (Internet Telephones in Local Mode, analog (500/ 2500-type) telephones and digital telephones) to outgoing local trunks

- local device calls to outgoing Virtual Trunks

Calls from Branch Office Internet Telephones in Normal Mode generate CDR records at the Main Office for the following call types involving Branch Office Internet Telephones:

- Incoming Virtual Trunks – CDR records are generated when a call from another Succession Call Server in the network over a Virtual Trunk terminates at a Branch Office Internet Telephone.

- Incoming local (analog and digital) trunks – CDR records are generated when a call from the local PSTN terminates at a Branch Office Internet Telephone.

- Outgoing Virtual Trunks – Such records are generated when a Branch Office Internet Telephone makes a call to another Succession Call Server in the network over a Virtual Trunk, to a device at the Branch Office, or to a destination over the local trunks at the Branch Office. An associated CDR record is also generated at the Branch Office when the call involves Branch Office facilities. When the call goes out on the local trunks at the Branch Office, the CDR record shows the user as having made a long distance call to the PSTN at the Branch Office.

- Outgoing local trunks (analog and digital).

The identifying digits in the Main Office Succession Call Server's CDR log are the manipulated string as specified by the Branch Office zone. For example, the Branch Office user dialed "9, 555-1212", but the Main Office Succession Call Server changes it to "6, 1-613-555-1212". CDR records the dial string as "1-613-555-1212". In other words, the Main Office Succession Call Server produces a CDR record indicating that the user dialed a "long distance" digit string because the feature converts the call from a local dialing pattern to a long distance dialing pattern.

System security

Succession 1000 and Succession 1000M system security is explained in detail in *System Management* (553-3001-300). This is required reading for any Branch Office administrator.

Nortel Networks recommends that the Station Control Password (SCPW) be longer than four characters. This recommendation is not enforced by the software.

Unauthorized access

When using Branch User Config during the installation phase, a Branch Office password and a Main Office password are required. The Branch Office password is the Internet Telephone Installer Password or the Temporary Internet Telephone Installer Password. If the required password is not configured, an error message (or otherwise failure to login) results. Three failed attempts lock that particular user ID from logging in for one hour. The lock is recorded in the TPS system log, and is printed to the Teletype Terminal (TTY). The system administrator can clear the lockout. Also, rebooting or reregistering the telephone to the TPS node can also clear the lock. See "Succession Signaling Server commands" on .

Three failed attempts to enter the Main Office password also locks the user out, this time at the Main Office Succession Call Server. The Main Office Succession Call Server lock can be removed only by an administrator using a LD 32 command to disable and re-enable that TN (terminal number) at the Main Office. Refer to *Succession 1000 System: Maintenance* (553-3031-500) for more information.

Adding a Branch Office

Contents

This section contains information on the following topics:

Introduction

To install a Branch Office, first upgrade the Main Office to Succession 3.0 software. For more information, 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). Then configure the Branch Office implementation parameters at the Main Office before installing the Branch Office. These parameters are the dialing plan, zone parameters, Internet Telephone parameters, and passwords. For more information, see *Succession 1000 System: Installation and Configuration* (553-3031-210).

A Succession 3.0 Branch Office can only be added to a Succession 1000 or 1000M Main Office running Succession 3.0 software. However,

Branch Offices already existing in the network can be running a previous release of software. In this case, you must choose whether or not to upgrade the set firmware for the 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 "Telephones" on page 22.

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 "Firmware downloads" on page 245 for more information on upgrading firmware for i2002 and i2004 Internet Telephones.

Main Office requirements

For the Branch Office to work, the Main Office requires the following:

- Succession 1000 or Succession 1000M hardware, running Succession 3.0 Software

- Network Alternate Route Selection (NARS) package 58. Refer to *Basic Network Features* (553-3001-379).

- H323 Virtual Trunk (H323_VTRK) package 399

- Emergency Service Access (ESA) package 329. This package is optional, and is required only to get 911/ESA features in North American and some Caribbean and Latin American (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.

The Main Office must have a Service Level of 2 or higher to interwork with the Branch Office.

Branch Office requirements

The Branch Office requires the hardware described in "Branch Office hardware description" on page 20. The Branch Office SSC also requires the following software packages:

- Flexible Numbering Plan (FNP) software package 160. Refer to *Dialing Plans: Description* (553-3001-183)

- Emergency Services Access (ESA) package 329

- 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.

- Succession Branch Office (SBO) package 390

- H323 Virtual Trunk (H323_VTRK) package 399

  Note: These packages are automatically enabled in the Branch Office software.

When using Set-Based Installation at the Branch Office, install the following:

- Set Relocation (SR) package 53

- Flexible Feature Code (FFC) package 139

- Automatic Installation (AINS) 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.

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. See Procedure 1 on page 82.

   d Configure the Branch Office dialing plan.See "Dialing plan configuration" on page 195.

   e Configure the Internet Telephone passwords. See Procedure 3 on page 91.

   f Use Gatekeeper Management to add the System Host Name of the Branch Office Succession Signaling Server to the Primary Gatekeeper H.323 endpoint list as "H323AliasName". 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. See "Installing an H.323 WAN Gateway" on page 95.

   b Install the Branch Office Succession Signaling Server. See "Installing a Succession Signaling Server" on page 104.

   c Install the Branch Office software, starting with "Branch Office SSC software installation" on page 144.

   Software for the Branch Office SSC comes with preprogrammed data that can be selected during the installation procedure. For more information, see "Preprogrammed data" on page 263.

   d Configure the Branch Office (Customer Data Block and ELAN). See Procedure 17 on page 157.

   e Configure the Branch Office dialing plan. See "Dialing plan configuration" on page 195.

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. The zone number must match that at the Main Office. 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. See "Abbreviated Dialing configuration" on .

i Provision the Virtual Trunks. Refer to *IP Peer Networking* (553-3001-213).

j Install Branch Office telephones, starting with "Installing and configuring Internet Telephones" on .

Adding a Succession 3.0 Branch Office to an existing Succession 1000 Release 2.0 Branch Office 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 growth in an existing Succession 1000 Release 2.0 Main Office and Branch Office network requires the addition of a new Branch Office. These options are:

1 Upgrade the entire network to Succession 3.0, and then add the new Branch Office (see "Option 1 – Upgrade the entire network to Succession 3.0 Software" on).

2 Upgrade only the Main Office to Succession 3.0, and then add the new Branch Office (see "Option 2 – Upgrade only the Main Office to Succession 3.0 Software (limited time only)" on).

For further information on upgrading the Internet Telephone firmware and Succession Signaling Server software, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Option 1 – Upgrade the entire network to Succession 3.0 Software

To upgrade the entire network to Succession 3.0 Software:

1   At the Main Office:

    a   Upgrade the Succession Call Server software to Succession 3.0 Software.

    b   Upgrade the Main Office Succession Signaling Server(s) software to Succession 3.0 Software with the Automatic Firmware Upgrade set.

    c   Upgrade the Main Office Voice Gateway Media Card(s) to Succession 3.0 Software.

2   At each existing Succession 1000 Release 2.0 Branch Office:

    a   Upgrade the Succession System Controller software to Succession 3.0 Software.

    b   Upgrade the Branch Office Succession Signaling Server software to Succession 3.0 Software with the Automatic Firmware Upgrade set.

    c   Upgrade the Branch Office Voice Gateway Media Card(s) to Succession 3.0 Software.

3   Execute the `umsUpgradeAll` command on the Main Office Succession Signaling Server(s), or VGMC(s), if necessary.

4   Install the new Succession 3.0 Branch Office as described in "Implementation summary" on .

Option 2 – Upgrade only the Main Office to Succession 3.0 Software (limited time only)

IMPORTANT!

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.

If you choose to upgrade only the Main Office to Succession 3.0 Software, you have the choice of upgrading the Internet Telephone firmware. Specifically, the options are:

a Upgrade the Internet Telephone firmware in the existing Succession 1000 Release 2.0 Branch Offices (see "Option 2a – Upgrade Main Office with Internet Telephone firmware upgrade" on).

b Do not upgrade the Internet Telephone firmware in the existing Succession 1000 Release 2.0 Branch Offices (see "Option 2b – Upgrade Main Office without Internet Telephone firmware upgrade" on).

Option 2a – Upgrade Main Office with Internet Telephone firmware upgrade

To upgrade the Main Office to Succession 3.0 Software and upgrade the Internet Telephone firmware in Succession 1000 Release 2.0 Branch Offices to Succession 3.0:

1 At the Main Office:

a Upgrade the Succession Call Server software to Succession 3.0 Software.

b Upgrade the Main Office Succession Signaling Server(s) software to Succession 3.0 Software with the Automatic Firmware Upgrade set.

c Upgrade the Main Office Voice Gateway Media Cards to Succession 3.0 Software.

---

   d   If necessary, execute the `umsUpgradeAll` command on the
           Main Office Succession Signaling Server(s) or VGMC(s).

2   At each existing Succession 1000 Release 2.0 Branch Office:

   a   Upgrade the Internet Telephone firmware to Succession 3.0 Internet
           Telephone firmware.

3   Execute the `umsUpgradeAll` command on the Main Office
         Succession Signaling Server(s), or VGMC(s) if necessary.

4   Install the new Succession 3.0 Branch Office as described in
         "Implementation summary" on .

Option 2b – Upgrade Main Office without Internet Telephone firmware upgrade

To upgrade the Main Office to Succession 3.0 Software without upgrading
the Internet Telephone firmware in the existing Succession 1000 Release 2.0
Branch Offices:

1   At the Main Office:

   a   Upgrade the Succession Call Server software to Succession 3.0
           Software.

   b   Upgrade the Main Office Succession Signaling Server software to
           Succession 3.0 Software with the Automatic Firmware Upgrade set.

   c   Upgrade the Main Office Voice Gateway Media Cards to
           Succession 3.0 Software.

2   At each existing Succession 1000 Release 2.0 Branch Office:

   a   If necessary, execute the `isetResetAll` command on the
           Branch Office Succession Signaling Server(s) or VGMC(s).

3   Install the new Succession 3.0 Branch Office, as described in
         "Implementation summary" on .

Upgrading to Succession 3.0 Software

Contents

This section contains information on the following topics:

Introduction

This chapter describes upgrading an existing Main Office and its associated Branch Offices from Succession 1000 Release 2.0 to Succession 3.0 Software.

When the Branch Office is being upgraded, the following components are not affected:

• telephone services between Branch Office Internet Telephones in Normal Mode

• telephone services between Branch Office Internet Telephones in Normal Mode and Main Office telephones or trunks other than those to the Branch Office

Upgrading to Succession 3.0 Software

If the Main Office has not already been upgraded to Succession 3.0 Software, begin with step 1. If the Main Office has been upgraded to Succession 3.0 Software, skip to step 2.

1   At the Main Office:

    a   Upgrade the Succession Call Server software to Succession 3.0 Software.

    b   Upgrade the Main Office Succession Signaling Server(s) software to Succession 3.0 Software with the Automatic Firmware Upgrade set.

    c   Upgrade the Main Office Voice Gateway Media Card(s) to Succession 3.0 Software.

2   At each existing Succession 1000 Release 2.0 Branch Office:

    a   Upgrade the Succession System Controller software to Succession 3.0 Software.

    b   Upgrade the Branch Office Succession Signaling Server software to Succession 3.0 Software with the Automatic Firmware Upgrade set.

    c   Upgrade the Branch Office Voice Gateway Media Card(s) to Succession 3.0 Software.

3   Execute the `umsUpgradeAll` command on the Main Office Succession Signaling Server(s), or VGMC(s), if necessary.

Main Office configuration

Contents

This section contains information on the following topics:

Introduction

This section describes the configuration of zones, Internet Telephone passwords and parameters, and Branch Office Internet Telephones at the Main Office.

Branch Office configuration procedures are discussed separately in "Branch Office configuration" on .

Dialing plan configuration in the Main and Branch Offices is described in "Dialing plan configuration" on .

For more information on Main Office configuration, refer to *IP Peer Networking* (553-3001-213). Also refer to *Succession 1000 System: Installation and Configuration* (553-3031-210), *Large System: Installation and Configuration* (553-3021-210), or *Small System: Installation and Configuration* (553-3011-210) as appropriate for the system.

Zone parameters

Zone parameters must be configured at both the Main Office Succession Call Server and Branch Office SSC. The Main Office procedure is similar to a Peer Network configuration with the Branch Office-specific configuration outlined in this chapter.

Zone parameters are defined at the Main Office in LD 117 (Procedure 1 on page 82) and applied to Internet Telephones in LD 11 (Procedure 23 on page 182).

Time adjustments for zones are configured in LD 117 and defined relative to the time set in LD 2.

ESA configuration in the dialing plan is discussed for both the Main Office and Branch Office in "Emergency Services configuration" on page 223.

Procedure 1
Configuring ESN and Branch Office zones

WARNING

Before *and* after an upgrade, perform a data dump (using LD 43 EDD or through Element Manager) on the Succession Call Server or SSC to back up the existing data.

1   Configure the Home Location Code, and the Virtual Private Network Identifier.

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

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 2 of 2)

Prompt	Response	Description
CUST		Customer number
	0-99	For Succession 1000M Large Systems
	0-31	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

2   Configure the Branch Office zone.

Configure the zone properties for IP telephony bandwidth management. Use LD 117 or Element Manager. Refer to *IP Peer Networking* (553-3001-213).

Note: The Branch Office zone number and zone bandwidth management parameters at the Main Office must match the corresponding Branch Office zone number and zone bandwidth management parameters at the Branch Office.

IMPORTANT!

Zone 0, the default zone, must not be configured as a Branch Office zone. Network Bandwidth Management does not support zone 0. If zone 0 is configured as a Branch Office zone, the Bandwidth Management feature will not be activated.

LD 117 – Define zone properties for 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 86) 0-1 000 000 Kbps • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 86) • interZoneBandwidth = Interzone available bandwidth (see Note 1 on page 86) 0-1 000 000 Kbps • interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) (see Note 2 on page 86) • 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 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 Internet Telephone is configured 2. any available channel from the pool of shared zones' channels

LD 117 – Define zone properties for 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 31.	
Note 2: If the Network Bandwidth Management feature is going to be used, and the 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 31.	

> **3**   Define the zone parameters at the Branch Office. Use LD 117 or Element Manager. Refer to *IP Peer Networking* (553-3001-213).

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.

4   Enable the features for the Branch Office zone in LD 117.

LD 117 – Enable features for Branch Office zone.

Command	Description
ENL ZBR <zone> ALL	Enables features for Branch Office <zone>.

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

Element Manager zone configuration

From Element Manager, you can configure the Branch-specific zone properties and time difference.

The Zone List window (see Figure 5) is the main window used for zone configuration in Element Manager. Select **Configuration | Zone** from the Element Manager navigation tree to open this window.

Figure 5
Branch-specific zone configuration

In the Zone List window, select the zone to be configured. The following properties can be configured:

- Basic Property and Bandwidth Management - see Figure 6

- Dialing Plan and Access Codes - see Figure 76 on

- Emergency Service Information - see Figure 77 on

- Time Difference and Daylight Saving Time Property - see Figure 7 on

Figure 6
Branch-specific Zone Basic Property and Bandwidth Management

Figure 7
Zone Time Difference and time zone

Internet Telephone passwords and parameters

This procedure enables any trusted user to install a telephone from its keypad interface. Both Main Office and Branch Office passwords are required.

Procedure 2
Setting the Internet Telephone Installer's Password

The Internet Telephone Installer's Password is configured on one Succession Signaling Server or Voice Gateway Media Card in a node. The passwords are applied to all components in the node.

Users must use the Temporary Internet Telephone Installer's Password if the SCPW is not configured.

1   From a computer terminal connected to the Succession Signaling Server, open a command line shell at the Main Office TPS node.

2   For a permanent Internet Telephone Installer's Password, enter the CLI command `nodePwdSet`. For a Temporary Internet Telephone Installer's Password, enter the command `nodeTempPwdSet`. The command, related commands, and explanations are given in Table 9.

Table 9
Internet Telephone node password

Command	Description
nodePwdSet	Sets the node password. If a non-zero length password is configured, all Internet Telephones that attempt to register after this command is entered display a prompt for node password before the TN can be modified.
nodePwdShow	Shows the node password settings.
nodePwdEnable	Enables node password checking.
nodePwdDisable	Disables node password checking.
nodeTempPwdClear	Deletes the temporary password and resets its uses and time to zero.
nodeTempPwdSet	Sets the node-level TN entry temporary password.

For detailed command-line or Element Manager procedures, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

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

To use the Virtual Office feature, a Station Control Password (SCPW) must be configured at both the Branch and the Main Offices. This procedure enables you to configure the length of the SCPW and the parameters for telephone modification, such as the Set-Based Removal feature prompts SRCD (LD 15) and AREM (LD 57). The actual SCPW password

configuration takes place while configuring the telephone data through the overlays. Telephone data is discussed in "Branch Office telephones" on page 163.

Procedure 3
Setting and changing the Station Control Password Configuration

The following steps are used to configure the SCPW.

1   Configure the length of the password, SCPL, to be of non-zero length in LD 15.

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

2   Assign the Automatic Set Relocation security code.

LD 15 – Assign Automatic Set Relocation security code.

Prompt	Response	Description
REQ:	CHG	Change existing data block
TYPE:	FTR	Customer Features and options
CUST		Customer number
	0-99	For Succession 1000M Large Systems
	0-31	For Succession 1000M Small Systems and Succession 1000 systems
SRCD	(0000)-9999	Automatic Set Relocation security code X removes security code

3   Configure the Flexible Feature Code in LD 57 to enable Station Control
Password Change (SCPC) and Set-Based Removal if desired.

LD 57 – Enable password change and set removal features.

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
CODE	SCPC	Station Control Password Change
- SCPC	xxxx	Code to invoke password change

4   The SCPW itself is configured during Internet Telephone configuration,
either using OTM 2.1 (see "Branch Office Internet Telephone
configuration using OTM" on) or overlays (see Procedure 4 on
).

——————— **End of Procedure** ———————

Branch Office Internet Telephone configuration

After the Branch Office zones and passwords are provisioned, provision the
Internet Telephones at the Main Office. These can be provisioned using OTM
2.0 (see "Branch Office Internet Telephone configuration using OTM" on
) or LD 11 (see Procedure 4 on).

Note: There is no automatic data synchronization between the
Main Office Succession Call Server and Branch Office SSC. The
technician must provision the telephone on all pertinent Succession Call
Servers or SSCs. See Procedure 20 on and Procedure 21 on

for details on easily transferring the data from the Main Office to the Branch Office.

Branch Office Internet Telephone configuration using OTM

At the Main Office, OTM can be used to configure Branch Office Internet Telephones. Use Telephone Pages to configure the telephones to include the following:

- Terminal Type

- TN

- Customer Number

- Branch Office Zone

- Prime DN corresponding to the BUID

Refer to *Succession 1000 Element Manager: System Administration* (553-3001-332) for details.

Branch Office Internet Telephone configuration using LD 11

Use this procedure at the Main Office to configure Branch Office Internet Telephones.

Procedure 4
Configuring Branch Office Internet Telephones at the Main Office using LD 11

1 Configure the Branch Office zones and dialing plan. See Procedure 1 on .

2 Configure the following telephone data:

- Terminal type

- Customer Number

- TN

- Zone

- Prime DN to correspond to BUID

LD 11 – Provision Branch User and SCPW at the Main Office.

Prompt	Response	Description
REQ:	NEW CHG	Add or Change
TYPE:		Terminal type.
	I2002	i2002 Internet Telephones
	I2004	i2004 Internet Telephones
	I2050	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.

——————— **End of Procedure** ———————

Branch Office hardware installation

Contents

This section contains information on the following topics:

Installing an H.323 WAN Gateway

The Branch Office hardware consists of an H.323 WAN Gateway. It must contain a Succession System Controller (SSC) card, and can contain the following interface cards:

- 8-port or 32-port Succession Media Card with IP Line 3.1 voice gateway

- Digital Trunk Card

- Analog Trunk Card

- Analog Line Card

- Digital Line Card

- Meridian Integrated RAN (MIRAN) Card

- Meridian Integrated Conference Bridge (MICB) Card

- cards to support CallPilot Mini or CallPilot 201i

To connect to the PSTN, use one of the following interface cards:

- 1.5 Mb T1 Multi-functional Digital Interface

- Extended Universal Trunk (analog)

- 2.0 Mb Digital Trunk Interface (DTI)

- 2.0 Mb Primary Rate Interface (PRI)

Note 1: The Branch Office H.323 WAN Gateway Expansion does not support digital trunks.

Note 2: Each Branch Office H.323 WAN Gateway with a digital trunk card must have a clock controller. See *Circuit Card: Description and Installation* (553-3001-211).

The Branch Office must have a Succession Signaling Server that can be installed in the same rack as the Branch Office H.323 WAN Gateway and Branch Office H.323 WAN Gateway Expansion chassis. The H.323 WAN Gateway Expansion chassis is optional and follows the same installation procedure as the H.323 WAN Gateway.

Readiness checklist

Before starting the installation, use the checklist in Table 10 to make sure you are ready.

Table 10
Readiness checklist (Part 1 of 2)

Have you:	✓
Read all safety instructions in *Succession 1000 System: Installation and Configuration* (553-3031-210)?	
Received all equipment?	

Table 10
Readiness checklist (Part 2 of 2)

Have you:	✓
Made sure the area meets all environmental requirements?	
Checked for all power requirements?	
Checked for correct grounding facilities?	
Developed an equipment layout plan for the system? This information is provided by your Planning and Engineering group.	
Completed the card slot assignment plan? This information is provided by your Planning and Engineering group.	
Obtained all the tools required to continue with the installation?	
Prepared the network data as suggested in *Data Networking for Voice over IP* (553-3001-160) and *Succession 1000 System: Planning and Engineering* (553-3031-120)?	

After you check off all of these items, you are ready to start Branch Office installation.

Tools checklist

To install the system correctly, make sure that the tools listed in Table 11 are available before assembling the components.

Table 11
Tools checklist (Part 1 of 2)

Tools and components	✓
screwdrivers	
an ECOS 1023 POW-R-MATE or similar type of test meter	
appropriate cable terminating tools	

Table 11
Tools checklist (Part 2 of 2)

Tools and components	✓
a drill for making lead holes	
a computer for connecting directly to the Branch Office H.323 WAN Gateway by a DTE—DTE null modem cable, with: • teletype terminal (ANSI-W emulation, serial port, 19 200 bps) for the Succession Call Server, Branch Office H.323 WAN Gateways, Succession Signaling Server, and Succession Media Cards • a web browser for Element Manager (configure cache settings to check for new pages every time and to empty the cache when the browser is closed)	

Rack-mounting an H.323 WAN Gateway or Gateway Expansion

Items required

To install each H.323 WAN Gateway or H.323 WAN Gateway Expansion in a 19-inch rack, use the following items:

• equipment layout plan (discussed in *Succession 1000 System: Installation and Configuration* (553-3031-210))

• one pair of left and right guide brackets

• one pair of left and right ear brackets

• eight #12-24 screws

• four #8-32 machine screws

The NTTK09 kit contains all of the above items with the exception of the equipment layout plan and screws.

Procedure 5
Mounting the H.323 WAN Gateway or H.323 WAN Gateway Expansion in a 19-inch rack

Note: References to "H.323 WAN Gateway" in the following steps also apply to the H.323 WAN Gateway Expansion.

1 Fasten the right guide bracket to the right rack support.

    a. Insert two #12-24 self-tapping screws into the two middle slots in the guide bracket and into the respective holes in the right rack support.

    b. Tighten the screws. See Figure 8.

Figure 8
Guide bracket installed in a rack

Use two screws in the two middle slots.
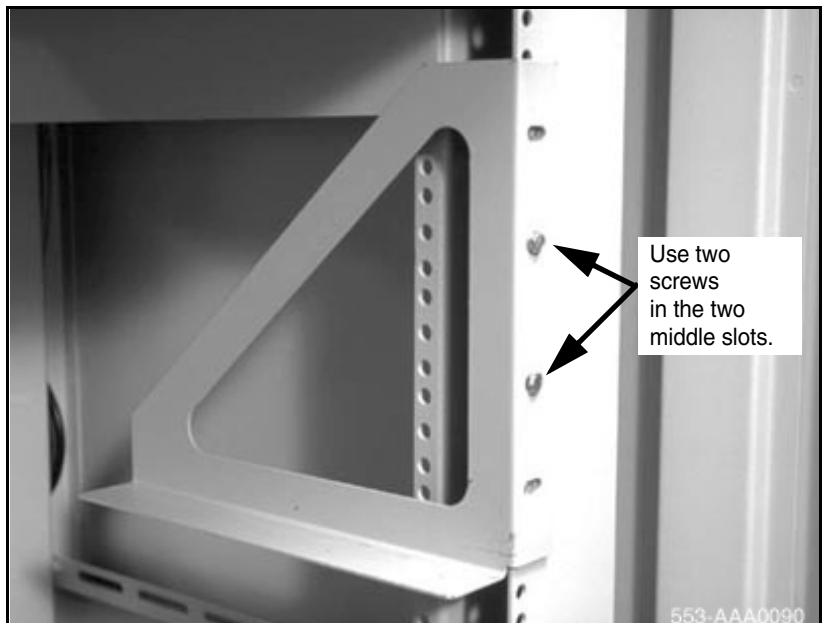
Note: The guide brackets guide the H.323 WAN Gateway into place and enable one person to install the H.323 WAN Gateway in the rack.

2   Fasten the left guide bracket to the left rack support.

   a.   Insert two #12-24 self-tapping screws into the two middle slots in the bracket and into the respective holes in the left rack support.

   b.   Fasten the screws.

3   Attach the right ear bracket (marked with an "R") to the holes on the right side of the H.323 WAN Gateway. See Figure 9.

   a.   Use two #8-32 machine screws.

   b.   Position the ear bracket so that the four holes on the bracket flange are nearer to the back of the H.323 WAN Gateway. To determine the front of the bracket, locate the "R". This "R" must be at the top of the bracket and must face to the front of the H.323 WAN Gateway.

Figure 9
Right ear bracket installed on the H.323 WAN Gateway

Bracket flange marked with an "R". Attach this ear bracket to the right-hand side of the H.323 WAN Gateway.

Attach the ear bracket to these holes.
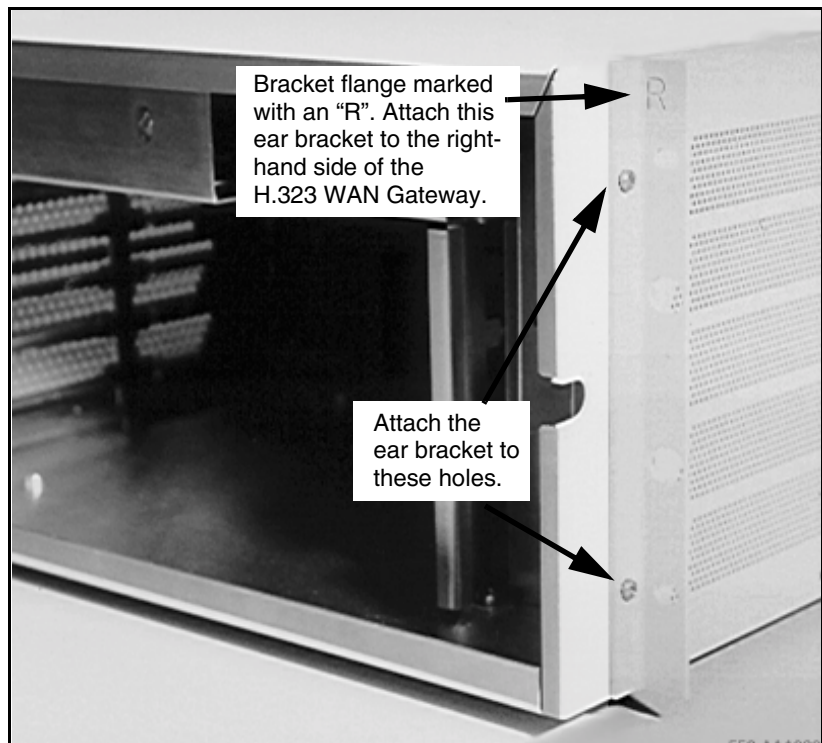
4   Attach the left ear bracket (marked with an "L") to the holes on the left side of the H.323 WAN Gateway (near the front).

   a.   Use two #8-32 machine screws.

   b.   Position the ear bracket so that the four holes on the bracket flange are nearer to the back of the H.323 WAN Gateway. To determine the front of the bracket, locate the "L". This "L" must be at the top of the bracket and must face to the front of the H.323 WAN Gateway.

> **WARNING**
>
> The H.323 WAN Gateway and H.323 WAN Gateway Expansion each weigh approximately 30 lb. (13.5 kg) with circuit cards installed, or 26 lb. (12 kg) without circuit cards installed. If necessary, get assistance when lifting the equipment.

5   Place the H.323 WAN Gateway on the guide brackets. Carefully slide the H.323 WAN Gateway into the rack until the ear brackets come to rest against the rack support.

6   Use the four remaining #12-24 self-tapping screws to fasten the H.323 WAN Gateway to the rack supports (two screws on each side).

7   Make sure that the back of the H.323 WAN Gateway is on the guide brackets. See Figure 10 on .

Figure 10
H.323 WAN Gateway and H.323 WAN Gateway Expansion installed in a rack

Use two screws on each side to fasten the H.323 WAN Gateway to the rack.
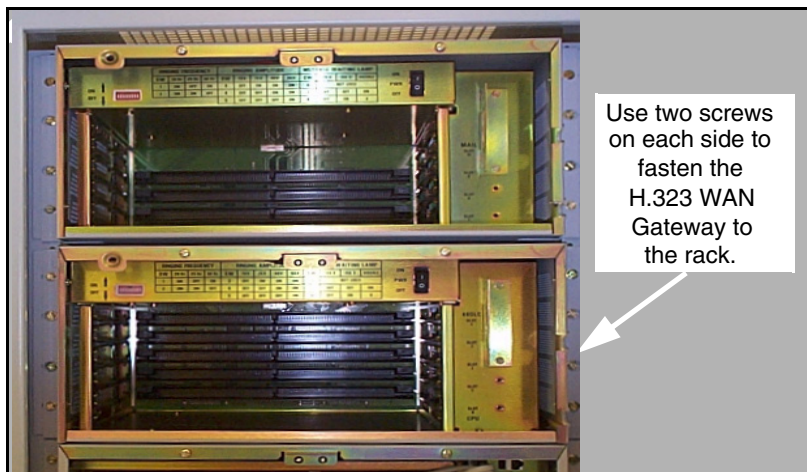
8 Install the equipment ground wires for the H.323 WAN Gateway, H.323 WAN Gateway Expansion, and Succession Signaling Server. See *Succession 1000 System: Installation and Configuration* (553-3031-210).

9 Install a UPS (if required) according to the manufacturer's instructions.

10 Open the H.323 WAN Gateway and install the Software Daughterboard, Security Device, and ground clip as described in *Succession 1000 System: Installation and Configuration* (553-3031-210).

11 Install circuit cards in the H.323 WAN Gateway and the H.323 WAN Gateway Expansion. See *Succession 1000 System: Installation and Configuration* (553-3031-210).

12 Make the Ethernet connections. Configure the Succession Ethernet port to enable OTM and Element Manager connectivity as required.

    a. See Procedure 16 "Connecting the Ethernet ports" on .

    b. Follow the instructions in *Optivity Telephony Manager: Installation and Configuration* (553-3001-230). A sample printout of the Ethernet configuration is provided.

Note: Do not connect a serial port to the AUX connector. It can damage the port.

13 Set DIP switches on the power supply for the desired ringing voltage, ringing frequency, and message waiting voltage. These procedures are in *Succession 1000 System: Installation and Configuration* (553-3031-210).

14 Connect the system to an AC power source. Make sure that the source matches the label on the back of the chassis. Turn the power switch to "ON".

Figure 11
Power switch on front of H.323 WAN Gateway
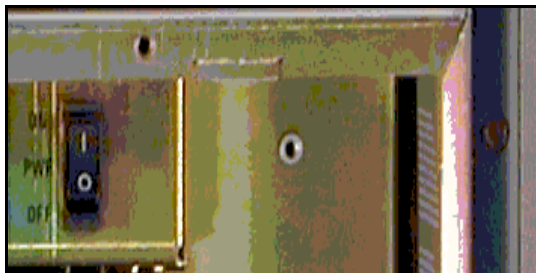
15 Install any remaining equipment, such as alarms. See *Succession 1000 System: Installation and Configuration* (553-3031-210).

16 Reinstall the front covers on the H.323 WAN Gateway and H.323 WAN Gateway Expansion.

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

Installing cards

In the Branch Office, install Succession Media Cards. To install and configure the 8- or 32-port Succession Media Card (Figure 12) or the 24-port ITG-P card, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Figure 12
Succession Media Card

553-AAA0094
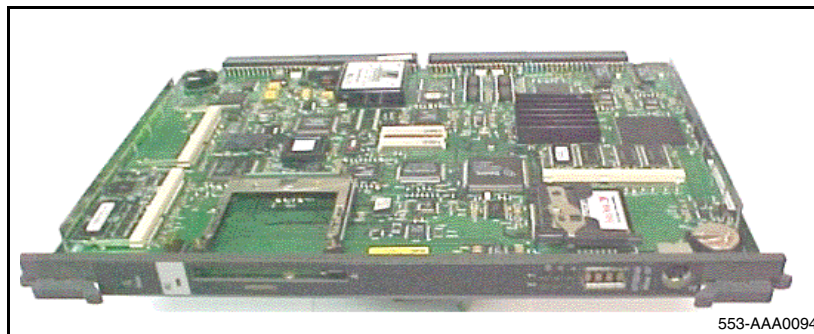
Install a trunk card to connect with the PSTN and an analog or digital line card to connect with local resources. Consult *Succession 1000 System: Installation and Configuration* (553-3031-210) and *Circuit Card: Description and Installation* (553-3001-211) for specific details and installation procedures of the various interface cards of the H.323 WAN Gateway.

Installing a Succession Signaling Server

This section describes how to prepare and install a Succession Signaling Server. For more information on the Succession Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Materials required

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

1   The tools listed in the "Readiness checklist" on page 96.

2   The Succession Signaling Server (see Figure 13 on page 105).

Figure 13
Succession Signaling Server

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

3 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.

4 The serial cable for the Succession Signaling Server.

5 The Ethernet cables for networking.

6 The contents of the accessories pouch to install the Succession Signaling
   Server. The accessories pouch should contain the following items:

   a Two chassis support brackets (A)

   b Two rack-mounting brackets (B)

   c Six rack-mount bracket screws (10-25 x 1/4" panhead Phillips)

   d Two bezel door long rack-mount screws

   Refer to Figure 14 on . If any parts are missing, contact your
   supplier immediately.

Figure 14
Succession Signaling Server brackets (two of each)

> **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 6
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 into an
electrical outlet.

2   Align the end of the rail with the flange (B) toward the back of the
Succession Signaling Server. See Figure 15 on page 107.

Figure 15
Chassis support bracket

553-AAA0097
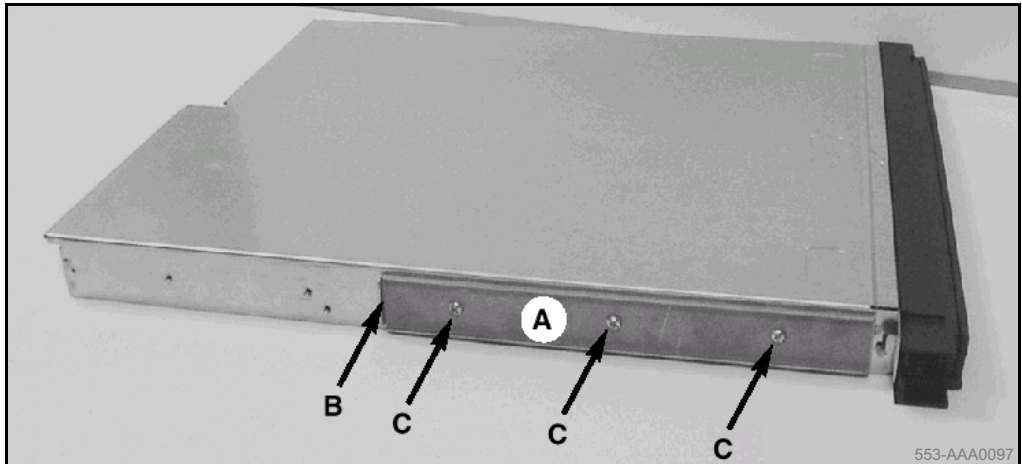
3   Align the screw holes in the rack-mount rail with the mating holes in the side of the Succession Signaling Server chassis. Use three screws (C) on each side.

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 16 and 17 on .

Figure 16
Left hinge mount
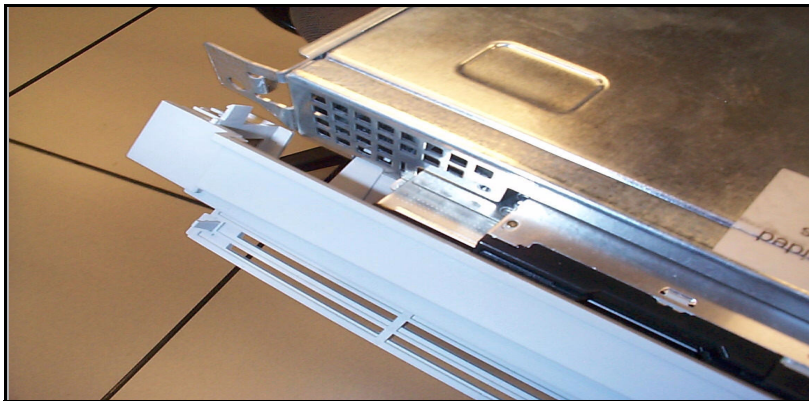
Figure 17
Right hinge mount
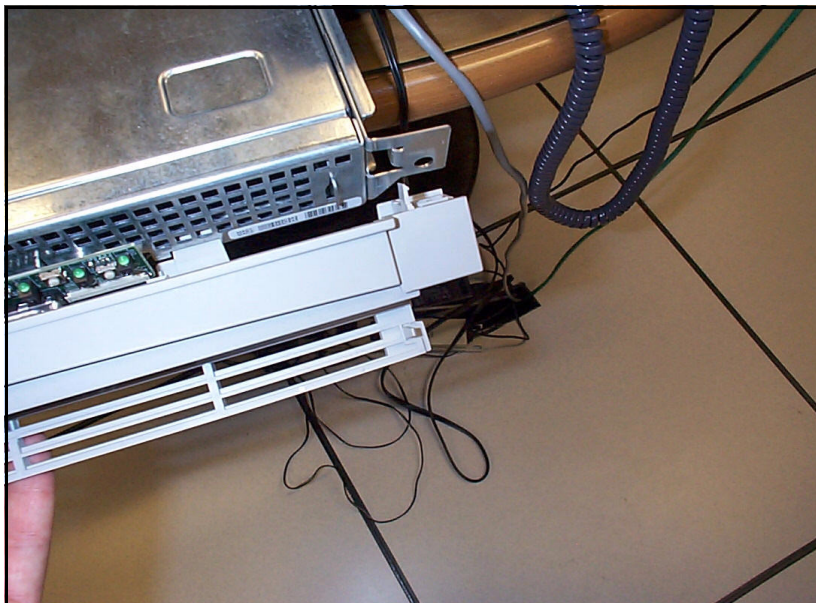
When the door is attached to the Succession Signaling Server and rack-mount apparatus, it appears as shown in Figure 18 on .

Figure 18
Snapped-in bezel door
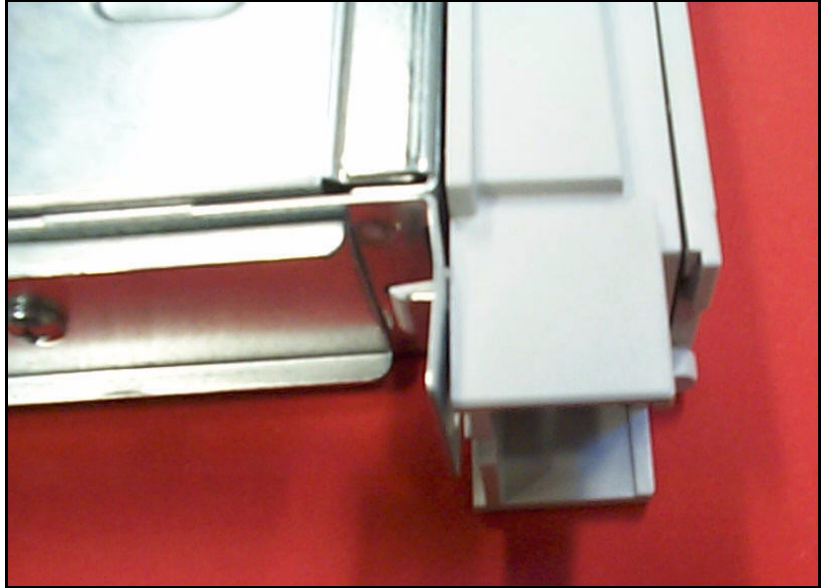
———————— **End of Procedure** ————————

Rack-mounting

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

⚠️	**DANGER OF ELECTRIC SHOCK** DISCONNECT AC POWER: Completely disconnect the the Succession Signaling Server from any AC power source before performing this procedure. Pressing the Power button DOES NOT turn off power to this Succession Signaling Server. Some circuitry in the Succession Signaling Server may continue to operate even though the front panel Power button is off. Failure to disconnect the Succession Signaling Server from its AC power source can result in personal injury or equipment damage.

⚠️	**DANGER OF ELECTRIC SHOCK** GROUNDING THE RACK INSTALLATION: To avoid an electrical shock, include a third wire safety grounding conductor with the rack installation. If Succession Signaling Server power cords are plugged into AC outlets that are part of the rack, provide proper grounding for the rack itself. If Succession Signaling Server power cords are plugged into wall AC outlets, the safety grounding conductor in each power cord provides proper grounding only for the Succession Signaling 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 Succession Signaling Server(s).

> ⚠️ **WARNING**—Damage to Equipment
>
> OVERCURRENT PROTECTION: The Succession Signaling Server is designed for an AC line voltage source with up to 20 amperes (A) of overcurrent protection. If the power system for the equipment rack is installed on a Branch Office circuit with more than 20 A of protection, provide supplemental protection for the Succession Signaling Server. If more than one Succession Signaling Server is installed in the rack, the power source for each Succession Signaling Server must be from a separate Branch Office circuit.

Procedure 7
Rack-mounting the Succession Signaling Server

1   Attach the rack-mount brackets ('B' as shown in Figure 14 on) 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 19
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.

   b.   Slide the Succession Signaling Server into place.

   Refer to Figure 20.

Figure 20
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 Succession 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.
>
> Replace the cord with the correct type. Refer to "Check the Power Cord" in the "Unpack and Inspect the Server" section at the front of this guide for power cord requirements.

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 8
Connecting and powering up the Succession 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 port is the top one of the two Ethernet ports shown in Figure 21 on page 114.

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 port is the bottom one of the two Ethernet ports shown in Figure 21 on page 114.

Figure 21
Back of Succession Signaling Server

Power   **TLAN (P2)**   **ELAN (P1)**   **Admin/Serial Port**
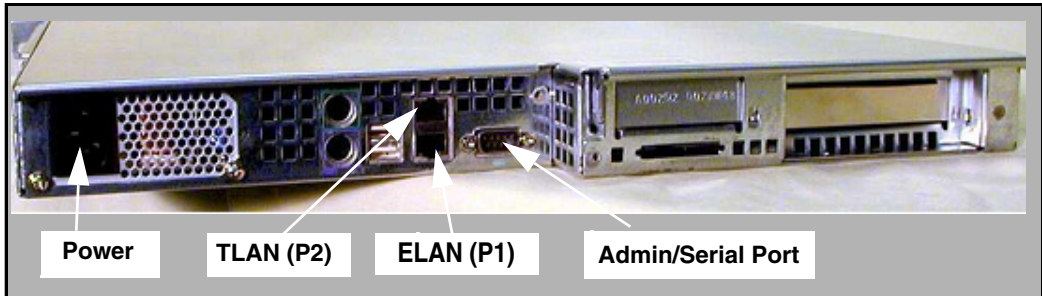
      3   Connect the power cord.

          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 21. Plug the male end of the AC power cord into the AC power source (wall outlet).

      4   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 back of the Succession Signaling Server to a maintenance terminal. The connection looks like that shown in Figure 22.

Figure 22
Maintenance to Succession Signaling Server connection

Serial Cable   Succession
Signaling Server

Maintenance Terminal
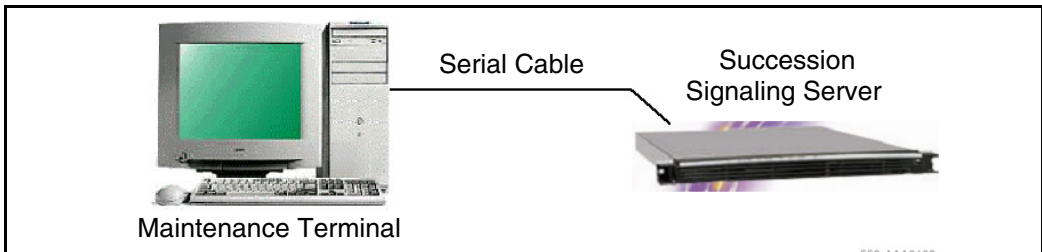
    b. The COM port on the maintenance terminal is set as follows:

- Terminal type: VT100

- Speed: 19 200

- Data bits: 8

- Parity: none

- Stop bits: 1

- Flow control: none

Note: The Succession Signaling Server is shipped with the Admin/Serial port set to 19 200 Bit/s. Other available speeds are 9600, 38 400, and 115 200 Bit/s.

  5 Power up the Succession Signaling Server.

    a. Open the bezel door (Figure 23) 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 swing open the hinged bezel door.

Figure 23
Succession Signaling Server with open bezel door
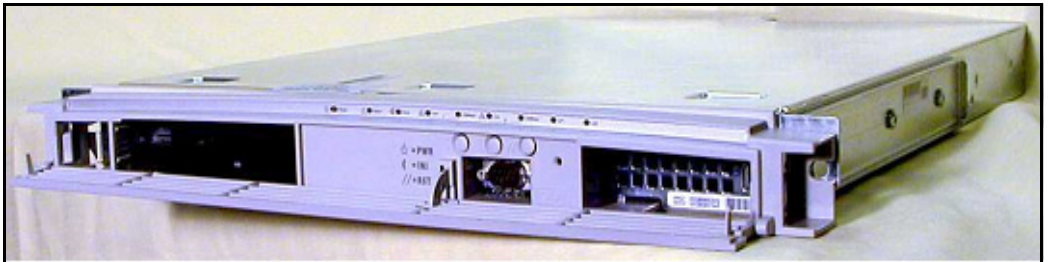
Note 1: The MAC addresses are visible on the lower right-hand side when the bezel door is open. See Figure 24.

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 25 shows the LEDs that correspond to the ELAN and
> TLAN connections.

Figure 24
MAC address

> **b.** Press the Power switch (see Figure 25). Notice that the green LED
> power indicator is lit.

Figure 25
Succession Signaling Server indicators and power switch
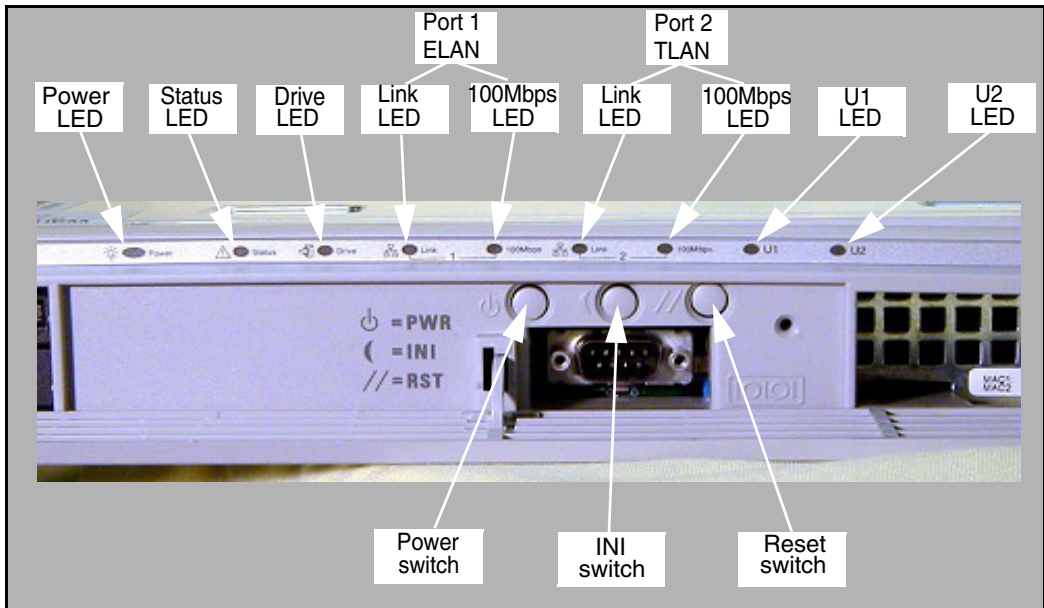
The Succession Signaling Server LED indicators show the following:

- 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.

- 100Mbps – green LED on, Ethernet port running at 100Mbps; LED off, Ethernet port running at 10Mbps.

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.

6 For additional operating information, refer to the Succession Signaling Server Product Guide on the Resource CD-ROM shipped with the Succession Signaling Server.

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

To install the Succession Signaling Server software, see "Succession Signaling Server software installation" on .

Branch Office software installation

Contents

This section contains information on the following topics:

Succession Signaling Server software installation

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 Succession Signaling Server software, including the operating system, applications, and web files. The Install Tool also copies software files for the Voice Gateway Media Cards (VGMCs) 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.

For more information about the Succession Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Materials required

To install the software, you need:

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

2   The Succession Signaling Server Software CD-ROM. Order or download the CD-ROM image from the Nortel Networks Electronic Software Download site if you do not have the latest version in the shipment.

Creating the Succession Signaling Server CD

A single ".iso" file is provided to create the Software CD-ROM. This file is a ready-to-burn ISO9660 CD image that creates a bootable CD that complies to 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 Succession 3.0 Software CD-ROM. See your 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 9
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).

The Software CD-ROM 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, please refer to the CD writer's software documentation.

Once the CD is created, you can use it to install new software or upgrade software on an existing Signaling Server.

Installing the Succession Signaling Server software

Before proceeding, you must complete Procedure 8 "Connecting and powering up the Succession Signaling Server" on .

Procedure 10
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 Signaling Server CD 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 is a software upgrade or a re-installation on an existing system, observe the boot sequence. Enter 'c' at the boot menu shown in Figure 26.

   Note: Entering 'c' at the "ISP 1100" banner speeds up this process, as the keyboard input is buffered.

Figure 26
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 select '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 27 on page 123), press <CR> to perform system checks and begin software installation.

Figure 27
Install Tool banner screen

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

          #####
       #########  ########
      ########``  `#############
     ########       ``     `#############
    #######`          ######```####
    #######      ######``     `###
   #######    #####``        ####         NORTEL NETWORKS
   ####### #####`            ####
   `#########`               ####`     Succession Enterprise Software
    #######`                #####
    `#######                #####'          Copyright 2001 - 2003
   ##########             `###`
   ##``##########          #
  ##    `#######################
  `#      `######################
     #########################``
      ````````  ````####````

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

Verifying filesystems ...
```

The system verifies the file systems.

**a.** When the software runs for the first time on a new system, the hard disk is not partitioned, so the test normally fails. Upon failure, the menu in Figure 28 on appears.

**Figure 28**
**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
```

      i.   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 ...
```

      ii.   The Install Tool banner screen (Figure 27 on)
reappears. Press <CR> to verify the filesystems.

           The disk check reports:

```
Filesystems verification succeeded.
```

      iii. Confirm or enter the date and time (Figure 29 on).

Figure 29
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
```

    b. 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 30 on). Enter 'a' to
continue the installation.

Figure 30
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 31 on .

Figure 31
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 32.

Figure 32
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 33 on .

Figure 33
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 34
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 (see Figure 34), 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 35 on shows actions that can be performed.

Figure 35
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 36 to 40, which start on , appear.

Figure 36
Installation output

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

You have selected to install version x.xx.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 x.xx.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 37
Successful installation

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

Software version x.xx.xx was installed successfully.

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

Figure 38
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 39
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   Configure the Succession Signaling Server as Leader or Follower. See
Figure 40 on page 133.

- If there is not already a Leader Succession Signaling Server in the IP
telephony node, enter 'a' at the prompt to configure this Succession
Signaling Server as Leader. Then go to step 9 on page 133.

- If there is already a Leader Succession Signaling Server in the IP
telephony node, enter 'b' at the prompt to configure this Succession
Signaling Server as Follower. Then go to step 14 on page 137.
Figure 46 on page 137 appears.

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

Figure 40
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>
```

9   Configure the node and data networking parameters. For IP telephony
     node configuration procedures, refer to *Signaling Server: Installation and
     Configuration* (553-3001-212).

     Note: IP addresses shown in Figures 41, 42, and 47 are examples.

Figure 41
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
```

10 Enter the Branch Office H.323 WAN Gateway ELAN IP address for the
Succession Call Server IP address prompt. See Figure 42.

Figure 42
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 Call Server
that this IP telephony node will register to.

Call Server IP  : 192.168.10.10
```

11 Select the Gatekeeper Service to be provided by this Succession
Signaling Server. See Figure 43.

- If there is a Primary and Alternate Gatekeeper in the network, select
  'a' to configure this Succession Signaling Server as a Failsafe
  Gatekeeper.

- If this Succession Signaling Server will be the Primary Gatekeeper,
  select option 'b'.

- If this Succession Signaling Server will be the Alternate Gatekeeper,
  select option 'c'.

- If this Signaling Server will not run the Gatekeeper application, select
  option 'd'.

- If network information is unknown, select option 'd'.

Figure 43
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>
```

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

12 Enter the Primary Gatekeeper IP address, the Alternate Gatekeeper IP address, or both, depending on the option selected in step 11 on . See Figure 44.

- If option 'a' was selected in step 11, you must enter the addresses of both the Primary Gatekeeper and the Alternate Gatekeeper.

- If option 'b' was selected in step 11, you can enter the address of the Alternate Gatekeeper.

- If option 'c' was selected in step 11, you must enter the address of the Primary Gatekeeper.

- If option 'd' was selected in step 11:

   — 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 later using Element Manager.

Figure 44
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 :
```

13 Select 'a' to configure the Succession Signaling Server to run the Gatekeeper, TPS, and Virtual Trunks. See Figure 45 on . Go to Step 15.

Figure 45
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
```

> **14** If this is a Follower Succession Signaling Server, enter the hostname for
> the Follower from the menu in Figure 46.

Figure 46
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
```

> **15** Confirm the parameters. The example in Figure 47 on 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 47
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 also found on the body of the Succession Signaling Server, on the right-hand side of the face behind the bezel door. See Figure 24 on page 116.

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

To complete the installation, the Installation Status Summary screen is displayed as shown in Figure 48 on page 139.

Figure 48
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 x.xx.xx for P2 |
   | loadware       |  yes   |   ok   | copy IP Line x.xx.xx for SA |
   +----------------+--------+--------+-----------------------------+
   | configuration  |  yes   |   ok   | set as Leader/Follower      |
   +----------------+--------+--------+-----------------------------+

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

16 Exit to the Main Menu (see Figure 34 on page 129). Select 'q' from the
Main Menu to quit the installation process. Figure 49 on page 140
appears. Enter 'q' again.

Figure 49
Quit menu

```
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 ...
```

17   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 in an IP
telephony node, there is no BOOTP response. Do not wait for this
response; add the Follower Succession Signaling Server to the IP
telephony node. Refer to *Signaling Server: Installation and Configuration*
(553-3001-212) for details.

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

Succession Signaling Server tools

See Procedure 11 on page 141 to access the options in the Succession Signaling Server Install Tools menu.

Procedure 11
Viewing the Tools Menu

Use this option to set the date and time on the Succession Signaling Server. This is also where you can reset the shell login names and passwords (if you forgot them or simply want to revert to initial defaults).

1 Choose option 't' at the Main Menu to access the Tools menu. The Tools Menu appears as shown in Figure 50.

Figure 50
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:

a. Set the date and time (default).

b. Repartition and reinitialize the hard disk.

c. Delete the Administrator login and password.

    d.   Test the hard disk.

    e.   Change the web server security flag.

Note: Option b, "To partition and initialize the hard disk.", 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 10 on .

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

Succession Signaling Server port speed

Next, change the initial port speed of the Succession Signaling Server for a maintenance terminal connection. This procedure is optional.

Procedure 12
Changing the Succession Signaling Server port speed

1   Make sure the DTE–DTE null modem cable (supplied with the Succession Signaling Server) runs from the back port of the Succession Signaling Server to the maintenance terminal.

2   Press <CR> to see the login prompt. The Succession Signaling Server must boot successfully before the user can log in.

3   Log in to the Succession Signaling Server.

Note: If the Succession Signaling Server has connected to the Succession Call Server (the startup messages indicate whether or not the link is up), use the PWD1 login to access the Succession Signaling Server.

The default Succession Signaling Server Command Line Interface (CLI) login and password is:

- Login = `admin`

- Password = `cseadmin`

The system immediately prompts a change to the default password.

Note: If you forget the password, reset it from the Tools Menu (see Procedure 11 on).

4   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.

5   Change the port speed on the terminal, terminal emulator, or workstation (which can require a terminal emulator reset).

6   Press <CR> several times to make sure the command line prompt is visible at the new speed.

7   Enter the `exit` command to log out of the CLI.

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

After installing software and configuring basic information about the Succession Signaling Server, the Succession Signaling Server components can be configured using the web-based Element Manager interface. See *Succession 1000 Element Manager: System Administration* (553-3001-332).

Verifying a successful configuration

To ensure that the Succession Signaling Server Ethernet connections are configured correctly (ELAN and TLAN), perform a ping test at each interface.

Procedure 13
Verifying successful configuration

1   From the Succession Call Server, in LD 117, enter:

   ping <ip address>

2   From the Media Card, log in to the Media Card and enter:

   ping "ip address",3

3   From the Succession Signaling Server, log in and enter:

   ping "ip address",3

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

Branch Office SSC software installation

After installing the hardware for the Branch Office, connect a computer terminal to the SSC of the Branch Office H.323 WAN Gateway and prepare to install software as for any system.

The Software Installation Program is menu-driven. The main menu provides the core functionality of the program. The Software Installation Program includes the following key functions:

- installation of software in a new system

- upgrade and modification of software in an existing system

- provision of utilities to work with archived databases, review data, back up data, undo an installation, and clear unwanted data

Refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258) for information about these functions and utilities.

During initial software installation on the Branch Office, there is an option to load a default database containing pre-configured data. If necessary, modify the default data at any time to meet the specific requirement of a customer.

> *Note:* Software for the Branch Office SSC comes with preprogrammed data that can be selected during the installation procedure. For more information, see "Preprogrammed data" on .

Procedure 14
Installing and provisioning a Branch Office

This procedure assumes that the hardware installation procedures have been performed and that the system is up and running. It is performed from a TTY connected to the Branch Office H.323 WAN Gateway.

1   Power up the system. See Figure 11 on to see the location of the power switch on the front of the Branch Office H.323 WAN Gateway.

The system displays the Software Installation Main Menu.

```
Branch Office Software Installation Main Menu:
1. New Install or Upgrade from Option 11/11E - From
Software Daughterboard
2. System Upgrade
```

```
3. Utilities
4. New System Installation - From Software Delivery
Card
[q]uit, [p]revious, [m]ain menu,[h] help or [?], <cr>
- redisplay
```

2   Select New Install (item 1) or New System Installation (item 4) from the Software Installation Program.

Note: The following require information from the Keycode data sheet. Please have it available.

```
Succession Enterprise Software Rls 300S will be
installed.
```

3   Select the feature set to be enabled.

Note: The feature set must match the one on the keycode data sheet. The Feature Set names shown in the following list are examples only.

The system displays the following:

```
Select Feature Set You Wish to Enable:
1. AsiaPac Succession Branch Office (ntmp50cd)
2. CALA Succession Branch Office (ntmp50dd)
3. EMEA Succession Branch Office (ntmp50ed)
4. N. America Succession Branch Office (ntmp50fd)
[q]uit, [p]revious, [m]ain menu, [h]elp or [?], <cr> -
redisplay
```

Note: The feature set selected must match that provided with the keycodes.

4   Indicate if there are packages to add.

The system displays the Add Packages prompt, as follows:

```
Do you wish to add packages? (y/n/[a]bort):
```

Select y to add packages.

```
Summary of packages selected (example only):
0-2 4-5 7-14-23-29 32-64 67 70-77 79-81 83 ... 390 ...

Enter additional packages: <cr> to continue
```

Note: The additional packages must match those provided with the keycodes.

If only the feature set and ISM parameters are being upgraded, go to step 7 on .

5   Confirm Feature Set and packages.

```
Your Feature Set Selection is: AsiaPac Succession
Branch Office

Additional Packages selected: 215-235

Summary of Packages selected is:

0-2 4-5 7-14 16-25 28-29 32-64 67 70-77 79-83 86-93 95
100-104 107-111 113-116 118-120 122-125 127-129
131-133 135 137-141 167 ... 390

...

...

215-235

Is this selection correct?
n <cr> (no)
y <cr> (yes)
a <cr> (abort, return to main menu)
```

If the response is NO, go back to step 3 on .
Continue if the response is YES.

6   From the Select Database menu, choose the pre-configured database
(item 1) to install:

Note: The name of the pre-configured shown is an example.

```
1. Pre-Configured database - AsiaPac Succession Branch
Office
2. Basic Configuration
3. Archived database
4. Quick Config for Demo only

[q]uit, [p]revious, [m]ain menu, [h]elp or [?], <cr>
redisplay
```

7   Review and make changes to the ISM parameters, if required.

The system displays the current ISM parameters as shown in the following example:

```
ISM Parameters will be set to:
TNS (5000)
ACDN (300)
AST (400)
LTID (0)
RAN_CON (120)
RAN_RTE (120)
MUS_CON (120)
BRAND (2)
ACD AGENTS (300) -
ANALOGUE TELEPHONES (0)
ATTENDANT CONSOLES(16)
BRI DSL (150)
CLASS TELEPHONES (0)
DATA PORTS (2500)
DIGITAL TELEPHONES (0)
INTERNET TELEPHONES (400)
PHANTOM PORTS (400)
WIRELESS TELEPHONES (0)
WIRELESS VISITORS (0)
ITG ISDN TRUNKS (0)
TRADITIONAL TRUNKS (120)
TMDI D-CHANNELS (64)
SURVIVABILITY (0)
PCA (0)
IP PEER H.323 TRUNKS (30)

Do you wish to change any ISM parameters? (y/n/
[a]bort):
```

Choose one of the following:

- Select 'n' to accept ISM parameter(s).
- Select 'y' to change ISM parameter(s).

Note 1: The Survivability ISM parameter is only used for the Succession Media Gateways in the Main Office. It does not apply to the Branch Office. Therefore, it must always be set to "0" for the Branch Office.

Note 2: If you do not change the feature set, the parameters displayed continue to be the current ISM parameters. The ISM parameters selected must match those provided with the keycodes.

```
Security ID: xxxxxxxx
Current AUX ID: xxxxxxxx
Do you wish to change the AUX ID? (y/n/[a]bort):
```

8   Verify the AUX ID. The default AUX ID is the security ID provided with the system.

9   Select the M3900 Language Set.

The system displays the Select M3900 Language Set menu, as shown in the following example.

```
Select M3900 Language Set:
1. Global 10 languages
2. Western Europe 10 languages
3. Eastern Europe 10 languages
4. North America 6 languages
5. Spare Group A
6. Spare Group B
[q]uit, [p]revious, [m]ain menu,[h] help or [?], <cr>
- redisplay
```

Select item 1 (Global 10 languages).

10   Review and confirm the information entered.

The screen displays the installation summary. Review and confirm the information displayed. You can access this information at any time, using the Current Installation Summary utility, as documented in *Succession 1000 System: Upgrade Procedures* (553-3031-258).

11   Enter the keycodes when prompted.

a.   Enter keycodes instead of x, y, z shown in the following example.

```
Enter new Keycodes:
Key 1:xxxxxxxx
Key 2:yyyyyyyy
Key 3:zzzzzzzz
```

b.   Look for the keycode validation message.

After you enter the last keycode, the system displays a message indicating if the keycodes are successful or not.

Example of a successful screen message:

```
Keycode validation successful
```

```
***WARNING*** A system restart will be invoked as
part of the software installation process".
```

Example of an unsuccessful screen message:

```
Keycode validation unsuccessful
```

c. Choose one of the following:

- If the **successful** message appears, go to Step 12.

- If the **unsuccessful** message appears, repeat Step 11.

  After three unsuccessful keycode validation attempts, the
  following message appears:

  ```
  Keycode validation unsuccessful.
  ```

  ```
  Installation aborted...returning to main menu.
  ```

12 Complete the software installation.

In response to the following message, enter 'y':

```
*** WARNING *** A system restart will be invoked
as part of the software installation process
```

```
Are you sure you wish to perform the installation? (y/
n/[a]bort)
```

The Software Installation Program finishes.

──────── **End of Procedure** ────────

Connecting the Branch Office H.323 WAN Gateway to the network

The Branch Office H.323 WAN Gateway has two 10/100BaseT ports (1 and
2) and one Attachment Unit Interface (AUI) port at the back on the lower
left-hand side. See Figure 51 on .

Figure 51
Back of Branch Office H.323 WAN Gateway
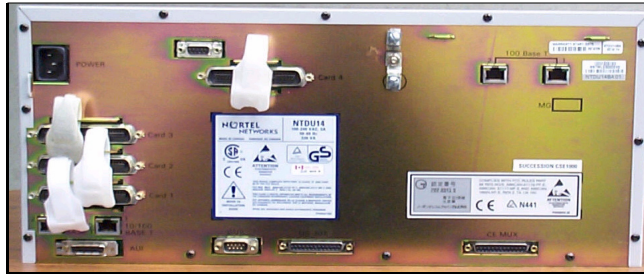
Connect to the 10BaseT ELAN Ethernet port 1, or, in the case of the
NTDK20FA SSC, the AUI port, that is connected to the Ethernet port on the
SSC motherboard.

> *Note 1:* Use the AUI port with an Ethernet Media Attachment Unit
> (MAU) for the NTDK20FA SSC.

> *Note 2:* Port 2 and LED lights on both ports are for future use.

The two 100BaseT ports at the top right corner of the Branch Office
H.323 WAN Gateway are disconnected, as the Branch Office SSC does not
support expansion daughterboards. Therefore, there is no TLAN connection
for the Branch Office H.323 WAN Gateway itself. The TLAN ports of the
Branch Office exist only on the Succession Media Cards, Internet
Telephones, and the Succession Signaling Server, as shown in Figure 3 on
and Figure 4 on .

Refer to LD 117 in *Software Input/Output: Maintenance* (553-3001-511) for
IP connectivity information.

Configure login names and pseudo terminals (PTYs) for OTM and
Element Manager connectivity. You need three PTYs for Element Manager.
For the configuration procedure, see *Optivity Telephony Manager:
Installation and Configuration* (553-3001-230).

The default login is

> User ID: `admin1`
> Password: `0000`

This is a Level 1 password. For more information, refer to *System Management* (553-3001-300).

Procedure 15
Configuring the ELAN IP address

To configure the active ELNK Ethernet interface for the Branch Office:

1   Go into LD 117.

2   Create host entries with IP address on the ELAN subnet. Enter the following command:

`NEW HOST <hostname> <IP_addr>`

3   Configure the ELAN Mask. Enter the following command:

`CHG MASK <maskvalue>`

Where:

<maskvalue> = nnn.nnn.nnn.nnn

4   Configure a new Routing Entry. Enter the following command:

`NEW ROUTE <destination IP> <gateway IP>`

Where:

<destination IP> is the ELAN IP address of the Succession Media Card on the Branch Office H.323 WAN Gateway

<gateway IP> is the ELAN IP address of the Branch Office H.323 WAN Gateway

5   Verify the IP address for the Ethernet link. Enter the following command:

`PRT ELNK`

6   Activate New Host entry. Enter the following command:

`CHG ELNK ACTIVE <hostname>`

7   Save the ELAN configuration. Enter the following command:

`UPDATE DBS`

8 For the changes to take affect, enter the following commands in LD 137 to disable and enable the ELNK:

```
DIS ELNK

ENL ELNK
```

─────────────────── **End of Procedure** ───────────────────

Procedure 16
Connecting the Ethernet ports

To configure TLAN and management support at the Branch Office H.323 WAN Gateway and enable traffic over the WAN, connect the Ethernet cables and configure the data connectivity.

1 Insert the Ethernet cable into the RJ-45 10BaseT Port 1 or Ethernet MAU. Connect the other end of the Ethernet cable to the switch. For more information about the switch, see *Data Networking for Voice over IP* (553-3001-160).

This connects the Branch Office H.323 WAN Gateway to the ELAN. The switch connects to the WAN router.

2 Install and put the Succession Signaling Server into operation, and connect the Succession Signaling Server ELAN and TLAN Ethernet ports to the switch. See *Succession 1000 System: Installation and Configuration* (553-3031-210).

For more detailed information on Succession 1000, switch, and router connections, see *Data Networking for Voice over IP* (553-3001-160).

─────────────────── **End of Procedure** ───────────────────

Using Element Manager to configure the node

In Element Manager (see Figure 52 on), configure the following IP telephony node values that are specific to the Branch Office:

• Primary Gatekeeper IP address

• Alternate Gatekeeper IP address (if equipped)

- default values of the following:

    — Primary Network Connect Server IP address

    — Primary Network Connect Server Port number

    — Alternate Network Connect Server IP address

    — Alternate Network Connect Server Port number

    — Primary Network Connect Server time-out

Figure 52
Confirm IP telephony node values

To configure a Follower Succession Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

To configure an Alternate Gatekeeper, refer to the corresponding procedures in *IP Peer Networking* (553-3001-213).

To configure a Failsafe Gatekeeper, refer to the corresponding procedures in *IP Peer Networking* (553-3001-213).

Branch Office configuration

Contents

This section contains information on the following topics:

Configuring the Branch Office SSC

After connecting the Branch Office H.323 WAN Gateway to the network and configuring the system user names and passwords (see "Branch Office software installation" on), complete the configuration.

Summary of steps

Perform the following steps to configure a Branch Office:

1   Configure ELAN IP address (see Procedure 15 on).

2   Configure the Branch Office dialing plan (see "Dialing plan configuration" on).

3   Configure Succession Media Cards as voice gateways (see "Configuring the Succession Media Cards" on).

4   Configure trunks and lines (see *Succession 1000 System: Installation and Configuration* (553-3031-210)).

5   Configure Internet Telephones (see "Installing and configuring Internet Telephones" on).

Configuring the Succession Media Cards

The Succession Media Cards (see Figure 12 on) arrive at a customer location with pre-installed software. To install and upgrade these cards, you need the latest workfile. The workfile is delivered by the PC card or Element Manager and contains all Succession Media Card operating system and application files. The workfile is a single packed and compressed file.

For more information on configuring the Succession Media Card, see *IP Line: Description, Installation, and Operation* (553-3001-365)

Configuring the trunks and lines

To install the line and trunk cards, refer to *Succession 1000 System: Installation and Configuration* (553-3031-210).

To configure lines on the Branch Office, refer to *Succession 1000 System: Installation and Configuration* (553-3031-210).

To install and configure Virtual Trunks on the Branch Office, refer to *IP Peer Networking* (553-3001-213).

Zone parameters

Zone parameters must be configured at both the Main Office Succession Call Server and Branch Office SSC. The Branch Office procedure is similar to a Peer Network configuration, with the additional Branch Office-specific configuration outlined in this chapter. Refer to *IP Peer Networking* (553-3001-213).

Zones are defined in LD 117 and applied to Internet Telephones in LD 11.

Emergency services configuration in the dialing plan is discussed for both the Main Office and Branch Office in "Emergency Services configuration" on .

Procedure 17
Configuring the Branch Office zone

> **WARNING**
>
> Before *and* after an upgrade, perform a data dump (using LD 43 EDD or through Element Manager) on the Succession Call Server or SSC to back up the existing data.

1 Set the current date and time. See *Software Input/Output: Administration* (553-3001-311).

LD 2 – Define system date.

Command	Description
STAD dd mm yyyy hh mm ss	
	Set the time and date: STAD DAY MONTH YEAR HOUR MINUTE SECOND

2 Configure the Home Location Code and Virtual Private Network Identifier.

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add or Change existing data block
TYPE:	NET	ISDN and ESN Networking options
CUST		Customer number
	0-99	For Succession 1000M Large Systems
	0-31	For Succession 1000M Small Systems and Succession 1000 systems

LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier. (Part 2 of 2)

Prompt	Response	Description
...		
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

3 Configure Vacant Number Routing (VNR).

VNR must be configured at the Branch Office. When a Branch User is in Normal Mode, a call to that user arriving at the Branch Office will be routed to the Main Office. VNR at the Branch Office and the Gatekeeper configuration identifies the Main Office as the endpoint for that user.

VNR is routed through the Virtual Trunk. This enables the Gatekeeper to centralize Numbering Plan definitions. To configure VNR, you must configure a Route List Index (RLI) with the Digit Manipulation Index (DMI in LD 86) set to 0 (no digit manipulation required) on the Virtual Trunk route.

LD 15 – Configure Vacant Number Routing. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add or Change existing data block
TYPE:	NET	Configure networking
VNR	YES	Vacant Number Routing

LD 15 – Configure Vacant Number Routing. (Part 2 of 2)

Prompt	Response	Description
- 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

4   Configure the zone properties for IP telephony bandwidth management. Use LD 117 or Element Manager (refer to Figure 53 on). At the Branch Office, this zone is used only for bandwidth management purposes. It does not have any associated time zone or dialing plan properties.

Note: The Branch Office zone number and zone bandwidth management parameters at the Main Office must match the corresponding Branch Office zone number and zone bandwidth management parameters at the Branch Office.

IMPORTANT!

Zone 0, the default zone, must not be configured as a Branch Office zone. Network Bandwidth Management does not support zone 0. If zone 0 is configured as a Branch Office zone, the Network Bandwidth Management feature will not be activated.

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) 0-1 000 000 Kbps • intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth) • interZoneBandwidth = Interzone available bandwidth (see Note) 0-1 000 000 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 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 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 31.	

5 Configure the parameters for Internet Telephone passwords and modifications. This procedure is outlined in "Internet Telephone passwords and parameters" on .

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

Element Manager Branch Office zone configuration

Figure 53 shows the only zone configuration screen required at the Branch Office. It is an alternative to zone configuration using LD 117.

Figure 53
Branch-specific zone Basic Property and Bandwidth Management

Note: At the Branch Office, the Branch Office Support (ZBRN) parameter must be cleared. This parameter is only applicable to the corresponding zone at the Main Office.

Adding the Branch Office Succession Signaling Server to the node

Add the Succession Signaling Server name to the network H.323 Gatekeeper database using Gatekeeper Management.

Note: If the Succession Signaling Server name is not added to the Gatekeeper database, the Gatekeeper rejects any registration request from the Succession Signaling Server because its name is not in the H.323 ID list. The H.323 ID is case-sensitive.

Refer to *IP Peer Networking* (553-3001-213) for the appropriate procedure.

Branch Office telephones

Contents

This section contains information on the following topics:

Overview

After the Branch Office zones and passwords are provisioned, the Internet Telephones must be provisioned. They can be provisioned using OTM 2.1, LD 11, or Set-Based Installation.

The telephones or devices that are supported in the Branch Office include:

- Internet telephones – See "Installing and configuring Internet Telephones" on page 164.

- Analog (500/2500-type) telephones and devices – See "Analog devices" on page 191.

- Digital telephones and devices – See "Digital devices" on page 192.

This chapter provides information on installing and configuring Internet Telephones, analog devices, and digital devices.

Installing and configuring Internet Telephones

All Branch Office Internet Telephones must be configured in the Main Office on the Main Office Succession Call Server (see "Branch Office Internet Telephone configuration" on page 92). They are also configured in the Branch Office on the Branch Office Succession System Controller (SSC) for survivability purposes. See Procedure 20 on page 176 and Procedure 21 on page 180 for details on transferring the data from the Main Office to the Branch Office in OTM.

Note: Automatic data synchronization is not carried out between the Main Office Succession Call Server and Branch Office SSC. However, refer to "Transferring Internet Telephone data using OTM" on page 176 for procedures to transfer Internet Telephone data from the Main Office to the Branch Office.

Configuring Internet Telephones is done in two stages – Internet Telephone data configuration, and Branch Office user-specific data configuration. The configuration can be done in two ways:

- Set-based installation - Use the keypad interface on the Internet Telephone to enter the data.

  — Enter the Internet Telephone data (follow the procedure "Using Set-Based Installation" on page 167).

  — Enter the Branch Office user-specific data (follow the procedure "Configuring a Branch User" on page 172).

- Use OTM or LD 11 to enter all data.

Alternatively, use any method to install the Internet Telephone and then configure the Branch Office user information.

This section contains instructions for installing Internet Telephones in all three ways: Set-Based, Optivity Telephony Manager (OTM), or overlays.

When the telephone line is inserted into the jack, the telephone tries to contact the Branch Office Internet Telephony Terminal Proxy Server (TPS) for registration, where it receives the firmware and features of the Branch Office.

> **WARNING**
>
> Do not plug the Internet telephone into an ISDN connection. Severe damage can result. Consult the system administrator to ensure that the telephone set is being plugged into a 10/100BaseT Ethernet jack.

At the Branch Office, under a Branch User registration request (plugging a telephone into a jack), the Main Office Succession Call Server checks the configured terminal type against the telephone's type and configuration. This check occurs at the Branch Office.

At the Main Office, under a Branch Office registration request, the Main Office Succession Call Server checks for a match of the configuration to the telephone type. If they do not match, registration is blocked.

Password requirements

To configure Branch Office user-specific data from the Internet Telephone keypad, a Main Office password and a Branch Office password are required.

Note: If you configure an Internet Telephone Installer Password or a Temporary Internet Telephone Installer Password, you can delegate these tasks, and continue to configure the system based on *Succession 1000 System: Installation and Configuration* (553-3031-210).

To install an Internet Telephone at the Branch Office using Set-Based Installation, Nortel Networks strongly recommends that an Internet Telephone Installer Password or a Temporary Internet Telephone Installer

Password be configured on the Branch Office Succession Signaling Server. See "Setting the Internet Telephone Installer's Password" on page 89 for information on configuring the passwords.

To configure the Branch User from an Internet Telephone in the Main Office, one of the following is required:

- Internet Telephone Installer Password or Temporary Internet Telephone Installer Password configured on the Main Office Signaling Server. The Temporary Internet Telephone Installer Password is usually implemented to enable a "trusted" user to install telephones at the Branch Office.

- Station Control Password (SCPW) for the Internet Telephone configured on the Main Office Succession Call Server. This is not the usual option, since usually a trusted user or administrator installs telephones. An SCPW is a user password.

Installing an Internet telephone using the keypad

Before proceeding to install an Internet Telephone using the keypad, be sure to obtain the required passwords, as described in "Password requirements" on page 165.

The procedure to install an Internet Telephone through the telephone interface consists of three steps.

1 Connect the Internet Telephone to an Ethernet jack and configure the S1 IP address (or use DHCP to retrieve the IP address).

The S1 IP address is the IP address of the Branch Office TPS. If it is entered as the Main Office TPS, the Internet Telephones register to the Main Office, but do not behave as Branch Office Internet Telephones.

2 Provision the basic Terminal Number (TN), Directory Number (DN), and node data through the Set-Based Installation procedure (Procedure 18 on page 167). This makes the set operational and provides basic provisioning for survivability. Nortel Networks recommends that the DN be the same at both the Main Office and the Branch Office.

3 Configure the Branch User Identity (BUID) and its Main Office TN through Procedure 19 "Configuring a Branch User" on page 172.

These three steps are easily performed and enable an administrator to install and provision a telephone.

> **WARNING**
>
> After all telephones have been installed, perform a data dump (using LD 43 EDD or through Element Manager) on the Branch Office SSC. Refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258).

If you have already unpacked and connected the Internet Telephone, complete Procedure 18 "Using Set-Based Installation" on . It simplifies configuration of Branch Office Internet Telephones for survivability. Each Branch Office Internet Telephone must also be provisioned at the Main Office.

To use DHCP addressing (using the automatic installation procedure, see *Succession 1000 System: Installation and Configuration* (553-3031-210) for more detail), verify that the network has DHCP enabled. Refer to *Data Networking for Voice over IP* (553-3001-160) for more information.

Procedure 18
Using Set-Based Installation

This procedure installs Internet Telephones at the Branch Office and Main Office. If necessary, the administrator can perform a Set-Based Installation when the Branch Office is in Local Mode.

1   To configure the S1 (primary connect server) on the Internet Telephone, choose DHCP, or manually enter the IP address of the local (Branch Office) TPS node. Enter the Branch Office node number and password, as shown in Figure 54 on .

Figure 54
Set-Based Installation Step 1

```
┌─────────────────────────────────────────┐
│                                         │
│ Connect SVC          an 01 12:17am  J   │
├─────────────────────────────────────────┤
│  Node : _____                           │
│                                         │
│  Password : _____                   │
├─────────────────────────────────────────┤
│  OK          BKSpace            Cle     │
└─────────────────────────────────────────┘
```

2   Enter the TN and press the OK softkey, as shown in Figure 55.

Figure 55
Set-Based Installation Step 2

```
┌─────────────────────────────────────────┐
│                                         │
│ Connect SVC          an 01 12:17am  J   │
├─────────────────────────────────────────┤
│  TN : _____                           │
│                                         │
│                                         │
├─────────────────────────────────────────┤
│  OK          BKSpace            Cle     │
└─────────────────────────────────────────┘
```

3   Wait for the default key map to download. The screen appears as shown in Figure 56.

Figure 56
Set-Based Installation Step 3

```
┌─────────────────────────────────────────┐
│ Succession                              │
├─────────────────────────────────────────┤
│  Invalid TN: 61.0                       │
│  Reason: Unequipped                     │
│  Go offhook to do SBI                   │
├─────────────────────────────────────────┤
│  Reset                                  │
└─────────────────────────────────────────┘
```

4   Lift the handset and listen for the continuous dial tone. The Model prompt is displayed as shown in Figure 57.

Figure 57
Set-Based Installation Step 4

```
Succession

   Model? (20)


```

5   Press the # key to select the default model, or enter the model number and press #.

6   Listen for a special tone. The prompt appears as shown in Figure 58. Enter the zone number as assigned in the Branch Office zone data at the Main Office. Press #.

Figure 58
Set-Based Installation Step 6

```
Succession

   OK, ZONE?(0)


```

7   Enter the extension number as prompted by the screen shown in Figure 59 on , and press #.

Figure 59
Set-Based Installation Step 7

```
 ┌─────────────────────────────────────────┐
 │                                         │
 │ Succession                              │
 │                                         │
 ├─────────────────────────────────────────┤
 │    OK, EXTENSION? 2244                   │
 │                                         │
 │                                         │
 ├─────────────────────────────────────────┤
 │                                         │
 └─────────────────────────────────────────┘
```

8 Replace the handset when you hear a relocation tone and see "OK" on the screen display.

9 The telephone is now registered with the SSC. Wait approximately 10 seconds for key map download to complete. The telephone is now fully operational in Local Mode. The screen appears as shown in Figure 60.

Figure 60
Set-Based Installation complete

```
 ┌─────────────────────────────────────────┐
 │                                         │
 │ Succession                              │
 │                                         │
 ├─────────────────────────────────────────┤
 │    Local Mode                           │
 │                                         │
 │                                         │
 ├─────────────────────────────────────────┤
 │ Trans          Conf rward        . F.   │
 └─────────────────────────────────────────┘
```

10 Test for survival functionality by making and receiving a call on the telephone.

11 The telephone is now configured for basic operation and survivability. To configure the Branch User, see "Branch User configuration" on .

───────────────────── **End of Procedure** ─────────────────────

Note: You must also configure the Set-Based Removal feature prompts SRCD (LD 15) and AREM (LD 57) by following Procedure 3 on .

Branch User configuration

To complete the interface-based configuration of the Branch User telephone, the administrator or a trusted user can configure the telephone with the Branch User Config command. Before proceeding, be sure to obtain the required passwords as described in "Password requirements" on page 165.

If the Branch User ID (BUID) is not configured, the Internet Telephone registers at the Branch Office SSC and stays in Local Mode. If the telephone is configured with a BUID and/or an Main Office TN (MOTN), it is automatically redirected to the Main Office TPS and then to the Main Office Succession Call Server. Redirection may not be successful - refer to Table 12 on page 249.

Branch User Config is the telephone-based mechanism to enter the BUID so that the Internet Telephone can be redirected to the Main Office to run in Normal Mode. Branch User Config is an option on the option menu display that is available to the Branch User.

The menu option for Branch User Config is shown in Figure 61.

Figure 61
Options menu

```
Options

    Telephone Option
    Virtual Office Login
    Branch User Config

  Select
```

To register an Internet Telephone to the Main Office, Branch User Config uses the following:

- Branch User ID (BUID)

- Branch Office password—Internet Telephone Installer's Password or Temporary Internet Telephone Installer's Password

- Main Office TN (MOTN), in either Large System format (four fields) or Small System format (two fields). This defaults to the TN at the Branch Office.

- Main Office password—Internet Telephone Installer's Password, Temporary Internet Telephone Installer's Password, or SCPW.

  Note: For information on setting up passwords, see "Internet Telephone passwords and parameters" on .

Branch User Config is used for configuration. Once the telephone is configured at the Branch Office, its parameters redirect the telephone to the Main Office. This means that configuration is not required a second time unless the Branch User parameters change on that Internet Telephone.

  Note: Attempting to perform a Branch User Config to a TN of a different set type at the Main Office results in a Permission Denied (4) error message on the display of the Internet Telephone. See Figure 12 on for more information on error messages.

Whenever a valid change is made to BUID/MOTN in LD 11, the Internet Telephone, if in Local Mode, is automatically redirected to the Main Office. A service change to BUID/MOTN does not affect Internet Telephones in Normal Mode. If the BUID of an Internet Telephone is deleted in a service change, no attempt is made to redirect the telephone to the Main Office.

⚠ WARNING

Do not delete the BUID/MOTN. If they are subsequently deleted, the association between the Main Office and the Branch Office will be lost, and any Internet Telephones which are in, or go into, Local Mode, will remain in Local Mode.

Procedure 19
Configuring a Branch User

1   To invoke the login and configuration operation for a Branch User, press the Services key (the key with the Globe icon) on an idle Internet Telephone. If the Branch Office package is equipped, the Virtual Office Login and Branch User Config options are displayed.

2 Select Branch User Config, as shown in Figure 61 on .

3 Enter the Branch User ID, that is a dialable DN of the Main Office. See Figure 62.

Note: For a CDP dialing plan, the Access Code is not required. For example, xxx-xxxx. For a UDP dialing plan, this DN includes the Access Code. For example, 6-xxx-xxxx.

Figure 62
Branch User ID

```
 ┌─────────────────────────────────────────┐
 │ Succession                              │
 │ ─────────────────────────────────────── │
 │    Enter Branch User ID:                │
 │                                         │
 │                                         │
 │ ─────────────────────────────────────── │
 │  Select          Delete                 │
 └─────────────────────────────────────────┘
```

4 Enter the Branch Office password, that is the Internet Telephone Installer's Password or Temporary Internet Telephone Installer's Password for the TPS node at the Branch Office. See Figure 63.

Figure 63
Branch Office Password

```
 ┌─────────────────────────────────────────┐
 │ Succession                              │
 │ ─────────────────────────────────────── │
 │    Enter Branch Password:               │
 │                                         │
 │ ─────────────────────────────────────── │
 │  Select          Delete                 │
 └─────────────────────────────────────────┘
```

5 Enter the Main Office TN in one of the following two ways:

- Choose SELECT to accept the default Main Office TN on the display.

- Enter the Main Office TN in either Small System format (two fields) or Large System format (four fields), and press SELECT.

The default value is the Branch Office TN in Small System format (two fields). See Figure 64, which shows an example of the display of a TN in Small System format.

Figure 64
Main Office terminal number

```
┌─────────────────────────────────────────┐
│                                          │
│  Succession                              │
│                                          │
├──────────────────────────────────────────┤
│     Enter Main Office TN:                │
│     6 2   1 0                            │
│     ─                                    │
│                                          │
├──────────────────────────────────────────┤
│  Select          Delete                  │
└─────────────────────────────────────────┘
```

6   Enter the Internet Telephone Installer's Password, Temporary Internet Installer's Password for the Main Office, or the SCPW for the Main Office TN. See Figure 65.

Figure 65
Main Office password

```
┌─────────────────────────────────────────┐
│                                          │
│  Succession                              │
│                                          │
├──────────────────────────────────────────┤
│     Enter Main Office Passw              │
│                                          │
│                                          │
├──────────────────────────────────────────┤
│  Select          Delete                  │
└─────────────────────────────────────────┘
```

Following entry of this data, the telephone is taken offline and the display shows "Locating Remote Server". The telephone registers with the Main Office and becomes operational.

WARNING

Network Problems During Installation:

Setup:
The Internet telephone in the Branch Office is on a different subnet to the Branch Office TPS and has a different route to the Main Office. The Branch Office TPS can connect to the Main Office but the Internet telephone cannot.

Symptom:
The terminal registers to the Branch Office TPS and is redirected to the Main Office (displaying the "Locating Remote Server" message). When it does not successfully register at the Main Office, it returns to the Branch Office (displaying "Server Unreachable"). The terminal keeps repeating the pattern.

Consequence:
The Internet telephone does not successfully provide call service.

Diagnosis:
When this behavior is observed, check whether a ping succeeds from the Internet terminal's subnet to the Main Office TPS subnet.

WARNING

After all telephones have been installed, perform a data dump (using LD 43 EDD or through Element Manager) on the Branch Office SSC. Refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258).

7   Execute the `EDD` command in LD 43.

─────────────── **End of Procedure** ───────────────

Transferring Internet Telephone data using OTM

Provisioned data for Internet Telephones at the Branch Office can be transferred directly from the Main Office to the Branch Office using OTM. BUID and MOTN values are then added. This transfer can be done in two ways:

- using the Import/Export facility in OTM – see Procedure 20

- using the Copy/Paste facility in OTM – see Procedure 21 on

This section describes both methods.

Procedure 20
Using the Import/Export facility in OTM

1   Create a report file to contain the exported station data:

    a. In OTM Navigator, select **Utilities | Corporate Directory**.

    b. In the Corporate Directory window, select **Configuration | Add Report**.

2   Configure the report file in the New Report window:

    a. Under the General tab:

        i. Type a file name, such as "ExportStation", in the Report Name text box.

        ii. In the Directory Members list box, select the Main Office(s) from which the data is to be exported.

    b. Under the Data Fields tab, in the Data field information list box, select the data field(s) to be exported. To select all the fields, click **Include All**.

    c. Under the Output tab:

        i. Select a data field and use the Move Up and Move Down buttons to rearrange the order of the selected field.

        ii. Enter or select a name and path for the report file in the Export File Name text box.

        The file must be saved with a .csv extension.

    d. Click **OK** in the New Report window to save the report configuration.

3 Generate the report file.

    a. In the Corporate Directory window, select the report and select **File** I **Generate Report**.

    b. In the Generate Report menu, select **Now...**.

    c. In the Generate Report Now dialog box, select **Generate report only** and click **OK**.

An example of a generated report file, as displayed in a text editor, is shown in Figure 66.

Figure 66
Generated report file


```
ExportStation.csv - Notepad
File  Edit  Format  Help
DN,Location,TN,Last Name,First Name,Instrument,Site\System
"6100","061 0 00 00","061 0 00 00","","","I2050","MainOffice1\MainOffice1"
"6101","061-0-00-01","061 0 00 00","","","I2050","MainOffice1\MainOffice1"
"6102","061-0-00-02","061 0 00 00","","","I2050","MainOffice1\MainOffice1"
```
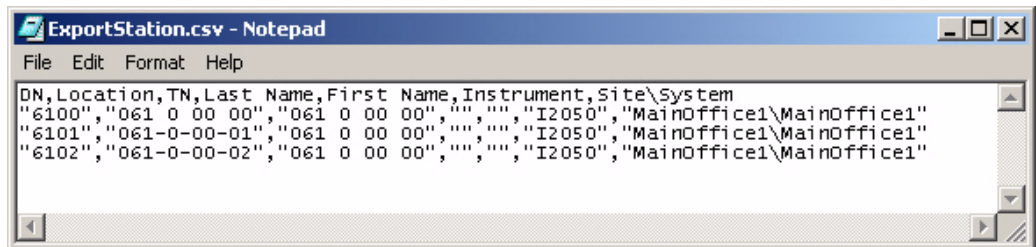
4 Create the field import file

    a. In a text editor, open the report file generated in step 3.

    b. Save the file as a new file with an extension of '.fld' (for example fields.fld).

    c. In the new file (for example, fields.fld), delete all but the first line of text, leaving only the first line listing the data fields. In the example shown in Figure 66, all lines following the first line of text are deleted.

    d. Delete the last field in the remaining lines. In the example shown in Figure 66, the text ",`Site\System`" is deleted.

    e. (Optional) To import data for additional data fields not added in step 2 on , type the name of the additional data field(s) in the line. Fields that can be added include BUID, MOTN, VOUA/VOUD, VOLA/VOLD, and SCPW.

Add the field names in the desired order, either mixing them with the existing fields or adding them at the end. Separate field names with commas.

f.   Save the file.

An example of a completed field import file is shown in Figure 67. This example includes the additional data fields BUID, SCPW, VOUA, and VOLA.

Figure 67
Field import file
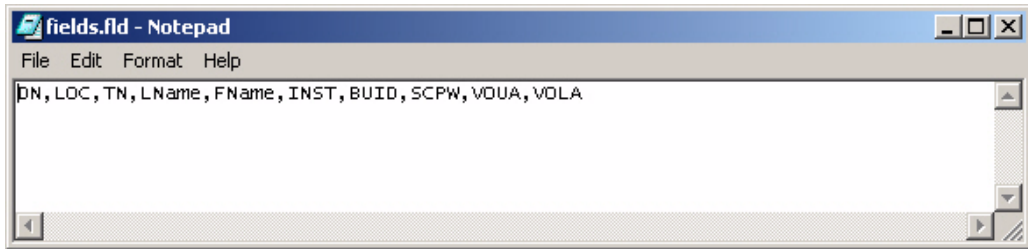
5   Create the data import file

a.   In a text editor, open the report file generated in step 3 on .

b.   Save the file as a new file with an extension of '.txt' (for example data.txt).

c.   In the new file (for example, data.txt), delete the first line of text listing the data fields. In the example shown in Figure 66 on , the line beginning with "`DN,Location,`" is deleted.

d.   Remove the last field in each of the remaining lines. In the example shown in Figure 66 on , the text "; "`MainOffice1\MainOffice1`" is removed from each line.

e.   If additional data fields were added to the field import file in step 4 on , add the corresponding data on each line of the data import file.

Insert the additional data values in each line in the same order as their corresponding field names are listed in the data import file, either mixing them with the existing data or adding them to the end of each line.

Note 1:   Each data item must be enclosed in double quotes ("). Data items must be separated by a semi-colon with no spaces. A data item with no value is given as " ".

Note 2: Each data item in a line corresponds to a field name in the field import file (see step 4 on page 177), and the data must be inserted in the same order on each line.

f. Save the file.

An example of a completed data import file is shown in Figure 68. This example includes data for the additional fields: BUID, SCPW, VOUA, and VOLA.

**Figure 68
Data import file**
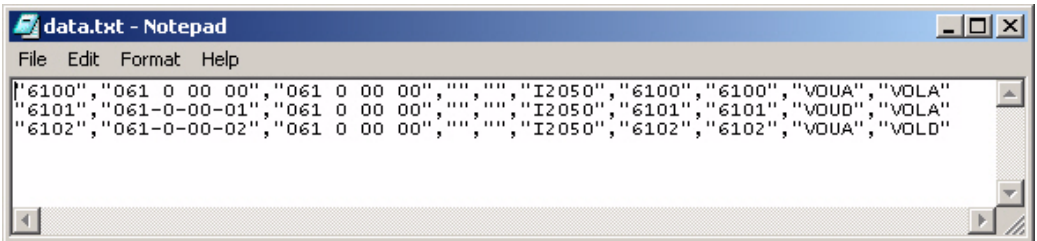
6 Import the data:

a. In OTM Station Administrator, select **File | Conversion Utility**.

b. In the Conversion Utility, select **File | Import | Data files**.

c. Select the field import file created in Procedure 4 on page 177 and click OK.

d. Select the data import file created in Procedure 5 on page 178 and click **OK**.

e. Click **OK** in the Import dialog box when the import process is done.

7 Verify the results:

a. In Branch Office Station Administration, check the attributes of the telephone(s) that have been imported.

b. Transmit the telephone(s) that have been imported to the Branch Office PBX, and test appropriately.

—————— **End of Procedure** ——————

Procedure 21
Copying and Pasting Internet Telephone Data using OTM

1   Copy the station data to be transferred. In OTM Station Administration for the Main Office:

   a.   Select the station which is to be copied to the Branch Office.

   b.   Select **Edit | Copy**.

2   Copy the station data to the Branch Office. Select **Edit | Paste** in OTM Station Administration for the Branch Office.

3   Compare the two stations in OTM Station Administration to confirm that the common properties of the two stations are identical.

4   Set the BUID of the station in OTM Station Administration for the Branch Office:

   a.   Select the station.

   b.   Select **Features**.

   c.   Select **BUID** from the list box.

   d.   Enter the BUID in the BUID text box in the Branch Office features dialog box and click **OK**.

   e.   Click **Done** in the Features dialog.

5   Transmit the telephone(s) that have been imported to the Branch Office PBX, and test appropriately.

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

Survivability test

This section pertains to telephones installed at the Branch Office. When WAN connectivity is lost, the Internet Telephones reboot and are registered at the Branch Office. When WAN connectivity is reestablished, each telephone reregisters at the Main Office.

After the Branch Office Internet Telephones are installed and configured, test the telephone for survivability. This is highly recommended when installing the BUID and MOTN through overlays or OTM. In these cases, the telephones are automatically redirected to the Main Office without the opportunity to test for Local Mode functionality.

Refer to "Test Local Mode" on for details on testing Local Mode functionality.

Procedure 22
Testing the telephone for survivability

Test the survivability of the connections and functions using the Test Local Mode command on the Branch Office Internet Telephone.

1   Press the Services key (the key with a Globe icon) to get the Options menu, and choose Test Local Mode.

This results in the Internet Telephone registering to the Branch Office SSC.

2   Make and receive a call on the telephone.

3   Use the Resume Normal Mode command (under the Services key, Options menu) to redirect the telephone to the Main Office TPS node. This reregisters the telephone at the Main Office. If Resume Normal Mode is not selected, the telephone automatically returns to Normal Mode after ten minutes.

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

Installing telephones through LD 11

To use the Virtual Office feature at the Branch Office in local mode, a Station Control Password must be configured. Refer to Procedure 3 on to provision the Station Control Password on the Branch Office. To prevent user password confusion, Nortel Networks recommends that the same SCPW be used at the Main Office and the Branch Office.

Procedure 23 on describes the general method of installing a Branch User telephone through LD 11.

Note: If the installation technician uses OTM or LD 11 to configure the Branch User ID and Main Office TN for an Internet Telephone, the Internet Telephone is automatically redirected to the Main Office after it is registered to the Branch Office.

Procedure 23
Installing Internet Telephones through overlays

1   Configure the Branch Office zones and dialing plan. See Procedure 17
    "Configuring the Branch Office zone" on page 157. Perform this
    procedure on the Branch Office SSC.

2   Configure the following telephone data:

    •   Terminal type

    •   Customer Number

    •   TN

    •   Zone

    To automatically redirect the telephone to the Main Office, configure a
    BUID and its MOTN. The BUID and MOTN prompts are unique to the
    Branch Office. Leave the MOTN field blank if it has the same value as the
    Branch Office TN. If a BUID is not entered, MOTN is not prompted. In this
    case, Branch User configuration is still required.

The BUID, or primary DN, of a Branch Office Internet Telephone should match
its primary DN at the Main Office, though this is not a requirement. If different
DNs are configured, the dial-in numbers change when the Branch Office is in
local mode.

> **WARNING**
>
> Do not delete the BUID/MOTN. If they are subsequently
> deleted, the association between the Main Office and the
> Branch Office will be lost, and any Internet Telephones
> which are in, or go into, Local Mode, will remain in Local
> Mode.

LD 11 – Provision Branch User and SCPW at the Branch Office. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add or Change

LD 11 – Provision Branch User and SCPW at the Branch Office. (Part 2 of 2)

Prompt	Response	Description
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.
...		
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.

3   (Optional) Disallow usage of Virtual Office. For more information on the Virtual Office feature, refer to *Internet Terminals: Description* (553-3001-368).

LD 11 – Enable/disable Virtual Office (optional).

Prompt	Response	Description
REQ:	NEW CHG	Add or Change
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)

4   Provision the Station Control Password (SCPW) if the Virtual Office feature is desired in Local Mode due to WAN or Main Office failure. See Procedure 3 "Setting and changing the Station Control Password Configuration" on page 91.

5   Perform a manual or automatic installation of the Branch Office Internet Telephone according to instructions in *Internet Terminals: Description* (553-3001-368).

WARNING

After all telephones have been installed, perform a data dump (using LD 43 or through Element Manager) on the Branch Office SSC. Refer to *Succession 1000 System: Upgrade Procedures* (553-3031-258).

6   Test the Internet Telephones for survivability using Procedure 22 "Testing the telephone for survivability" on page 181.

—————— **End of Procedure** ——————

Using the Internet Telephones

A Branch Office Internet Telephone is operational immediately after configuration. You can learn more about its services by referring to "Telephone Options" on and to *Internet Terminals: Description* (553-3001-368). You can also test the telephone. Refer to "Test Local Mode" on .

Changing the SCPW

Use Procedure 23 to change the SCPW of a telephone at any time.

Procedure 24
Changing the SCPW

1   Dial the SCPC code followed by the current Station Control Password. An FFC tone is given at this point.

2   Enter the new password (the new password must be 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. If the new password is not accepted, an overflow tone is given.

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

Telephone Options

The Internet Telephone Options feature is described in *Internet Terminals: Description* (553-3001-368).

Procedure 25
Using the Options feature

This procedure explains how to use Internet Telephone Options 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 (see Figure 69 on). The menu contains the following items:

    •   Telephone Option

    •   Virtual Office Login

    •   Test Local Mode

Figure 69
Options menu

```
 ┌──────────────────────────────────────┐
 │ Options                              │
 ├──────────────────────────────────────┤
 │    Telephone Option                  │
 │    Virtual Office Login              │
 │    Test Local Mode                   │
 ├──────────────────────────────────────┤
 │   Select                             │
 └──────────────────────────────────────┘
```

Note 1: The Options Menu is new to IP Line 3.0. In IP Line 2.0 and previous releases, the Telephone Options menu was presented immediately after pressing the Services key. In IP Line 3.0 and subsequent releases, the Options menu is presented instead. The user must select Telephone Option to access the Telephone Option menu.

Note 2: The Virtual Office Login option only appears if VOLA CLS is configured.

2   Use the Down key to highlight **Telephone Option**.

3   Press the **Select** softkey to activate the feature.

    4   Choose one of the following options:

- Volume adjustment

- Contrast adjustment

- Language

- Date and time

- Display diagnostics

- Local dialpad tone

- Set info

- Ring type

- Call timer

- Onhook default path

- Change Feature Key label

    5   Follow the screen prompts to enter data as required.

    6   Press the **Services** key or the **Cancel** softkey to exit the Services menu.

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

Virtual Office Login on the Branch

The Virtual Office Login feature is described in *Internet Terminals: Description* (553-3001-368).

Procedure 26
Using the Virtual Office Login feature

This procedure explains how to log in to and log out of Virtual Office. The Internet Telephone has been configured using Branch User Config and is operating in Normal Mode or Local Mode.

    1   Press the Services key (the key with the Globe icon) to display the Options menu (see Figure 69 on).

    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 destination Internet Telephone.

"Locating Remote Server" appears on the display.

When logged into Virtual Office, the telephone display appears as shown in Figure 70.

Figure 70
Virtual Office - logged in

```
┌─────────────────────────────────────────┐
│                                          │
│  Succession                              │
│                                          │
├─────────────────────────────────────────┤
│                                          │
│                                          │
│     User: xxx xxxx                       │
├─────────────────────────────────────────┤
│  Trans          Confrward         . F.   │
└─────────────────────────────────────────┘
```

6   To log out, press the Services key to display the Options menu, then use the arrow key to highlight Virtual Office Logout and press Select. See Figure 71.

Figure 71
Virtual Office application menu

```
┌─────────────────────────────────────────┐
│                                          │
│  Options                                 │
├─────────────────────────────────────────┤
│     Telephone Option                     │
│     Virtual Office Log                   │
│                                          │
├─────────────────────────────────────────┤
│  Select                                  │
└─────────────────────────────────────────┘
```

─────────────── **End of Procedure** ───────────────

Feature interactions between Branch User and Virtual Office logins

When an Internet Telephone user at a Branch Office travels to the Main Office or another network location, the user can access their own Main Office TN from an Internet Telephone at the visited location by using the Virtual Office feature. The Internet Telephone at the Branch Office is forced to logout after the feature is activated.

If the telephone has been forced-logout, the Virtual or Branch User softkey shows on the telephone display (see Figure 72 on). The telephone is not operational in this mode. The user must log in to bring the telephone back into service.

Figure 72
Virtual or Branch softkey display

```
┌─────────────────────────────────────┐
│ Succession                          │
│                                     │
│    Logged Out                       │
│                                     │
│                                     │
├─────────────────────────────────────┤
│  Virtual   anch  Br                 │
└─────────────────────────────────────┘
```

The Virtual and Branch softkeys are provided to reset the telephone to operational:

1 Press the Branch softkey to register the telephone to the Main Office.

2 Press the Virtual softkey to activate Virtual Office Login.

In either case, the user is prompted for the User ID and the SCPW.

When a Branch User telephone re-powers, it registers with the Branch Office H.323 WAN Gateway SSC, and is automatically redirected to the Main Office. If another Internet Telephone has already occupied the Main Office TN using the Virtual Office login, the re-powered Internet Telephone is logged out at the Main Office Succession Call Server with the

screen shown in Figure 72. The telephone remains registered to the
Main Office TPS and is listed with the `isetShow` command.

Test Local Mode

A user in Normal Mode can test the survivability functionality by entering the
Test Local Mode command, as shown in Figure 61 on . This results
in the Internet Telephone registering to the Branch Office SSC. The user
should make a call and receive a Branch-based or PSTN-based call in Test
Local Mode to be sure that the telephone works in the event of a WAN failure.

Procedure 27
Using the Test Local Mode feature

This procedure explains how to test the Internet Telephone for Local Mode
operation. The Internet Telephone has been configured using Branch User
Config, overlays, or OTM, and is operating in Normal Mode.

1   Press the Services key (the key with the Globe icon) to bring up the
     Options menu (see Figure 69 on).

2   Use the Down key to highlight **Test Local Mode**.

     The Internet Telephone displays "Local Mode". The Services key displays
     the menu in Figure 73.

Figure 73
Resume Normal Mode

```
┌─────────────────────────────────────────────────┐
│                                                  │
│  Options                              Jan        │
│ ┌───────────────────────────────────────────────┤
│ │   Telephone Option                             │
│ │   Virtual Office Login                         │
│ │   Resume Normal Mode                           │
│ ├───────────────────────────────────────────────┤
│ │  Select                                        │
└─┴───────────────────────────────────────────────┘
```

3   To register again at the Main Office, use the down arrow to select the
     Resume Normal Mode command.

     Note 1: If you fail to resume Normal Mode, Test Local Mode lasts for ten
     minutes, and then automatically redirects the telephone to the Main Office
     Succession Call Server.

Note 2: The Virtual Office Login option only appears if VOLA CLS is configured.

—————— **End of Procedure** ——————

Set-Based Removal

The following procedure can be used by an administrator or a trusted user to remove the system provisioning for an Internet Telephone or analog (500/2500-type) or digital telephone.

Procedure 28
Using the Set-Based Removal feature

When the Automatic Set Removal (AREM) feature is enabled and you have a Set Relocation Security Code (SRCD), follow these steps:

1   Lift the handset or press the DN key of the Internet Telephone to be removed.

2   Key in the AREM code after hearing the dial tone.

3   Enter the SRCD.

4   Hang up, or press the Release key.

—————— **End of Procedure** ——————

Analog and digital devices in the Branch Office

Analog devices

Analog (500/2500-type) telephones are supported in the Branch Office, but are not centrally managed from the Main Office. Instead, they are managed at each Branch Office. When a call is between an analog (500/2500-type) telephone and an Internet Telephone, a DSP resource is required. Therefore, when analog (500/2500-type) telephones are located in the Branch Office, allow for additional voice gateway channels to support IP-TDM connections.

Analog (500/2500-type) telephones at a Branch Office can be configured using:

•   Set-Based Installation

- Overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 23 on .

- OTM

Analog devices supported at the Branch Office include analog (500/2500-type) telephones, fax machines, and modems.

Digital devices

Digital telephones and Attendant Consoles are supported in the Branch Office, but are not centrally managed from the Main Office. Instead, they are managed at each Branch Office. When a call is between a digital telephone and an Internet Telephone, a DSP resource is required. Therefore, when digital telephones are located in the Branch Office, allow for additional voice gateway channels to support IP-TDM connections.

Digital telephones at a Branch Office can be configured using:

- Set-Based Installation (not for M3900-series telephones)

- Overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 23 on .

- OTM

Digital devices at the Branch Office include digital telephones, consoles, and a CallPilot Mini or CallPilot 201i.

M3900-series digital telephones also have a Virtual Office feature. This feature is not network-wide, like the Virtual Office feature on the Internet Telephones. For an M3900-series telephone, a Virtual Office login enables a registration to another TN within the Branch Office SSC.

Activating analog (500/2500-type) and digital telephones

Activate each telephone using the Automatic Set Configuration feature. This feature is described in *Succession 1000 System: Installation and Configuration* (553-3031-210).

To program a telephone with the data feature, configure the Data Class of Service parameter in LD 11. Refer to *Software Input/Output: Administration* (553-3001-311).

Dialing plan configuration

Contents

This section contains information on the following topics:

Overview

Configuring the dialing plan for a Branch Office is done in two stages:

- configuring on-net dialing

- configuring off-net dialing for access to the PSTN

For on-net calls, the configuration of the dialing plan in the Main and
Branch Office is the same as for other Succession 3.0 configurations. The

same is true for off-net calls made by non-Branch users in the Main Office, and by users of TDM telephones and Internet Telephones in Local Mode in the Branch Office.

This section primarily describes the configuration of a dialing plan for off-net calls from Branch Office Internet Telephones in Normal Mode. However, the procedures in this chapter are also applicable when configuring on-net UDP dialing for these telephones, if a single Access Code is used for both UDP and some or all off-net calls.

Introduction

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.

Dialing plans

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. A common configuration might be:

- Branch Office users select the Branch Office PSTN for local calls.

- Main Office users select the Main Office PSTN for local calls.

- All users select either the Main Office or Branch Office PSTN for long distance calls to minimize toll charges.

However, this configuration represents only one way that the dialing plan could be configured. 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.

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.

Examples of on-net configurations are given in Appendix C: "On-net dialing plan configuration examples" on .

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.

An example of a simple off-net configuration is given in Appendix D: "Off-net dialing plan configuration example" on .

Routing

Branch User telephone call to Branch Office PSTN

The Branch User telephone is registered at the Main Office. The Branch User telephones are physically located at the Branch Office, so routing of local PSTN calls back to the Branch Office is essential, even if they are registered with the Main Office.

Branch Office behavior of the Branch User telephones at the Main Office is configured by setting Branch Office zone characteristics through LD 117 at the Main Office.

Routing incoming call from BO PSTN to BO telephone (DID call)

If the DN is valid and can terminate, call termination at the Branch Office is treated differently for Internet telephones and non-Internet telephones, as follows:

- Internet Telephones – If the telephone is registered at the Branch Office (Local Mode), the call is terminated locally. If the telephone is not registered at the Branch Office (Normal Mode), the call is routed through a Virtual Trunk to the Main Office.

- Non-Internet Telephones – Calls are terminated locally (within the Branch Office).

If the DN is not valid, the number is considered vacant by the Branch Office controller and VNR is used to route the call to the Gatekeeper for resolution.

H.323 zones

In an H.323 network, each Gatekeeper controls one H.323 zone. Each zone can consist of many H.323 IP clients and many H.323 Voice Gateways/endpoints. If a call terminates beyond the call originator's own H.323 zone, the Gatekeeper of the called party's zone provides the endpoint information to set up the connection.

It is possible to divide a system into several zones. It is also possible to divide a customer within a system into different zones. It is more common to assign one zone to one system and one customer.

Bandwidth management zones

An IP Peer network is divided into different bandwidth management zones. Each Internet Telephone, Virtual Trunk, or Voice Gateway DSP channel is assigned to a bandwidth management zone. All Internet Telephones, Virtual Trunks, or Voice Gateway DSP channels in a bandwidth management zone:

- share the same IP bandwidth management policies

- are geographically near each other

- are all in the same time zone

- are all in the same PSTN dialing plan

A bandwidth management zone is assigned to each Virtual Trunk and Voice Gateway DS Channel in LD 14. It is assigned in the same way as the ZONE for an Internet Telephone in LD 11. This zone enables the trunk to send a setup message, with a codec list selected according to the Best Bandwidth (BB) or Best Quality (BQ) criteria for that zone.

For dialing plan purposes, all telephones in the same zone can be treated identically. Each Internet Telephone is assigned to a zone during configuration. The Branch Office feature enables Internet Telephones that are located in more than one geographic location to have dialing plan behaviors that are localized to the telephone location rather than the CS location.

Different zone numbers are assigned to different Branch Offices.

Zone-based digit manipulation

For Branch Office users in Normal Mode, it may be desirable to provide routing that is different from that provided to Main Office users. For example, it may be desirable to route certain calls directly to the Branch Office PSTN trunk, rather than receive the same routing as non-Branch users in the Main Office.

To achieve this, the Zone Access Code Behavior (ZACB) and Zone Digit Prefix (ZDP) properties of the Branch Office zone are used to add digits to the digits dialed by the Branch Office user. The resulting digit string is then used to route the call. The net effect of this is that a Branch User's and a Main User's call can be routed differently, even though the dialed digits were the same.

For example, if "1 87654321" is dialed, where "1" is the Access Code, then:

- for a Main Office user, the call is routed based on the dialed digits.

- for a Branch Office user, the digits undergo zone-based digit manipulation (such as inserting "101"), and the call is routed based on the new manipulated digit string (in this example "1 101 87654321").

By performing this zone-based digit manipulation, calls from Main Office users and Branch Office users undergo different routing. Some applications are:

- routing all Branch Office users' calls to the Branch Office PSTN trunk

- routing Branch Office users' local calls to the Branch Office PSTN trunk

- routing all Branch Office users' calls to the Main Office PSTN trunk

- routing Branch Office users' long distance calls to the Main Office PSTN trunk

Special considerations apply in the case where a single Access Code is used for both on-net and off-net calls, especially when UDP is used. Routing of on-net and off-net calls is normally different. The Succession Call Server ESN Special Number provisioning (refer to Notes 1 and 2 on page 210) and Gatekeeper Numbering Plan Entry provisioning (refer to the note on page 214) should be used to provide this different routing.

In the case where a single Access Code is not shared, that is, where one Access Code is exclusively used for UDP on-net dialing, standard procedures should be used. Refer to *Dialing Plans: Description* (553-3001-183).

For a given Branch Office, there may be more than one zone defined at the Main Office. Therefore, different Branch Users may receive different routing treatments.

The combination of zone-based digit manipulation and Succession 3.0 Software routing capabilities can be used to achieve many other routing outcomes for Branch User calls.

Configuring the dialing plan for PSTN access to Branch Office users in Normal Mode

Preparing to configure the dialing plan

Before configuring the dialing plan for PSTN access to Branch Office users in Normal Mode, you must complete the following steps:

- At the Main Office, configure the Virtual Trunk to enable calls originating on Branch Office Internet Telephones in Normal Mode to reach the Branch Office. Refer to *IP Peer Networking* (553-3001-213) for details.

- At the Main Office, configure trunks for access to the PSTN.

- At the Branch Office, configure the Virtual Trunk to enable calls originating on Branch Office Internet Telephones in Normal Mode to reach the Branch Office. Refer to *IP Peer Networking* (553-3001-213) for details.

- At the Branch Office, configure trunks for access to the PSTN.

- At the Main Office, configure the Branch Office zone properties in LD 117, excluding the ZACB and ZDP properties. Refer to *IP Peer Networking* (553-3001-213) for details.

- At the Main Office, configure the routing for PSTN access.

- At the Branch Office, configure the routing to enable calls made from TDM or Internet telephones in Local Mode to access the PSTN.

- At the Branch Office, configure Vacant Number Routing (VNR)

- Configure the Internet Telephones with the same zone number at both the Main Office and the Branch Office. Nortel Networks also recommends that the Prime DNs be the same at both the Main and the Branch Offices. If different DNs are configured, the dial-in numbers change when the Branch Office is in Local Mode.

- Assign unique individual DNs as Branch User Identities (BUID) to Automatic Call Distribution (ACD) telephones.

Configuring the dialing plan

The steps to configure the dialing plan for Branch Office PSTN access are:

- At the Main Office (Procedure 29 on page 204):

    1   Configure the ZACB property for the Branch Office zone.

    2   Configure the ZDP property for the Branch Office zone.

    3   Configure the Route List Index.

    4   Configure the ESN Special Number and Digit Manipulation.

- Configure the Gatekeeper (Procedure 30 on page 213).

    1   Access Element Manager.

    2   Select an endpoint.

    3   Configure the Numbering Plan Entry for the Branch Office.

- At the Branch Office (Procedure 31 on page 215):

    1   Configure the Route List Index.

    2   Configure ESN.

These steps can be done using overlays, as described in this section, or in Element Manager. Refer to *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) or *IP Peer Networking* (553-3001-213) for more details.

A sample configuration is given in Appendix D: "Off-net dialing plan configuration example" on page 317.

Procedure 29
Configuring the Main Office

1   Configure the ZACB property for the Branch Office zone. Refer to *IP Peer Networking* (553-3001-213).

LD 117 – Define the zone Access Code handling for the Branch Office zone.

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.

The ZACB and ZDP (step 2 on) properties are used to configure the digit manipulation behavior of the Branch Office zone.

The ZACB property specifies which calls undergo digit manipulation. The attribute can be configured in the following ways:

- CHG ZACB <zone>

   In this configuration, dialing AC1 or AC2 does not trigger digit manipulation. Branch Office users' calls are treated exactly the same as those for Main Office users.

- CHG ZACB <zone> ALL

   In this configuration, calls dialed with AC1 and calls dialed with AC2 undergo zone-based digit manipulation. All Branch Users' calls can then be routed to the Branch Office PSTN.

   For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a Branch User dials "1 87654321", ZDP is inserted in the dialed digits to form a digit string of "1 101 87654321". If a Branch User dials "2 87654321", ZDP is inserted in the dialed digits to form a digit string of "2 101 87654321".

- CHG ZACB <zone> AC1 AC2

   In this configuration, only calls dialed with AC1 undergo zone-based digit manipulation. All Branch Users' calls dialed with AC1 can then be routed to the Branch Office PSTN.

For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a Branch User dials "1 87654321", ZDP is inserted in the dialed digits to form a digit string of "1 101 87654321". If a Branch User dials "2 87654321", zone-based digit manipulation does not occur and the digit string remains unchanged.

- CHG ZACB <zone> AC2 AC2

    In this configuration, only calls dialed with AC2 undergo zone-based digit manipulation. All Branch User calls dialed with AC2 can then be routed to the Branch Office PSTN.

    For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If a Branch User dials "1 87654321", zone-based digit manipulation does not occur and the digit string remains unchanged. If a Branch User dials "2 87654321", ZDP is inserted in the dialed digits to form a digit string of "2 101 87654321".

Note 1: As part of the ZACB configuration, you can also change the dialed Access Code, so if you dial AC2 it can be changed to AC1, or vice versa. This provides more flexibility in the Main Office NARS configurations. Normally, you do not need to change the Access Code.

Note 2: The Access Code dialed by the user is used internally by the Succession Call Server. It is not sent as part of the outpulsed digits (to the Gatekeeper or to the trunks).

Note 3: If a specified Access Code is used for both local and long distance dialing, then both types of calls will receive the specified routing.

2   Configure the ZDB property for the Branch Office zone in the Main Office. Refer to *IP Peer Networking* (553-3001-213).

LD 117 – Define the 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.

The ZDP and ZACB (step 1 on) properties are used to configure the digit manipulation behavior of the Branch Office zone.

The ZDP property is inserted between the Access Code specified in the ZACB command and the dialed digits. This zone-based digit manipulation allows the Main Office Succession Call Server and the network Gatekeeper to distinguish the Branch Office users' calls from the Main Office users' calls, and route them accordingly. The digit manipulation occurs before any digit processing in the Main Office Succession Call Server or Gatekeeper.

Note: If DialingCode1, DialingCode2 or DialingCode3 are already present in the dialed digits, then they will not be re-inserted.

Nortel Networks recommends that the ZDP attribute for each Branch Office zone be set to a unique non-dialable number within the dialing plan (for example "1019" or "999"). This unique non-dialable number can then be used, when configuring the Main Office ESN Special Number (step 4 of Procedure 29 on) and the Gatekeeper (Procedure 30 on), to route the calls to the Branch Office for connection to the local PSTN.

For example, assume AC1 = 1, AC2 = 2, ZACB = AC1 AC1, and ZDP = 101.

If a Branch Office user dials "1 87654321", zone digit manipulation occurs because AC1 was dialed and ZACB = AC1 AC1. ZDP is inserted in the dialed digits to form a digit string of "1 101 87654321". The call is routed differently than with the digits "1 87654321". ESN configuration at the Main Office Succession Call Server (step 4 on

) routes the call to the Gatekeeper because it recognizes "101 87654321" after the Access Code rather than "87654321". The Access Code ("1") is not included in the digit string that is sent to the Gatekeeper. The Gatekeeper recognizes "101" at the front of the digit string and routes the call to the destination Branch Office. At the Branch Office, the ESN Special Number is configured (step 2 on) to remove "101" from the digit string and route the call based on the digits "87654321".

If a Branch Office user dials "2 87654321", zone-based digit manipulation does not occur because AC2 was dialed and ZACB = AC1 AC1. The digit string remains unchanged "2 101 87654321". The Main Office routes the call using ESN configuration and the dialed digits.

3 Configure the Route List Index at the Main Office.

After configuring zone-based digit manipulation, a specialized route for the call must be configured. To select a trunk to route calls, a Route List Index (RLI) must be configured in the Route List Block (RLB). The RLI uses the route number for the Virtual Trunk to route calls to the Gatekeeper. A Digit Manipulation Index (DMI) is associated with the RLI to allow manipulation of the digits to be outpulsed. For this application the DMI is used to update the call type of the call.

a. Configure the DMI in LD 86 with the DGT feature.

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.
DEL	(0)-19	Number of leading digits to be deleted, usually 0 at the Main Office.

LD 86 – Configure Digit Manipulation Index at the Main Office. (Part 2 of 2)

Prompt	Response	Description
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

b.   Configure the RLI in LD 86 with the RLB feature.

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 (step a on).

For example, assume that the Virtual Trunk is on route 10, and the Customer number is 0:

```
>LD  86
REQ  NEW
CUST 0
FEAT DGT
DMI  10
DEL
INST
CTYP NATL

REQ  NEW
CUST 0
FEAT RLB
RLI  10
ENTR 0
LTER NO
ROUT 10
...
DMI
...
```

4   Configure ESN Special Number and Digit Manipulation.

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

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 2 of 2)

Prompt	Response	Description
TRAN	 AC1 AC2	Translator Access Code 1 (NARS/BARS) Access Code 2 (NARS)
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 (step 4 on page 209)

After configuring the zone-based digit manipulation (step 1 on page 204 and step 2 on page 206) and specialized route (step 3 on page 207), the route must be associated with the ESN Special Number. The Main Office ESN Special Number configuration is based on new digits inserted by zone-based digit manipulation. The digits are processed based on the Access Code, AC1 or AC2, that was dialed

Note 1: For off-net calls the following should be considered:

- If all calls which have undergone Zone-based digit manipulation are to be routed by the Gatekeeper, only one SPN needs to be provisioned to route calls to the Gatekeeper based on the ZDP.

- If some calls are to be routed by the Gatekeeper, and others by the Main Office Succession Call Server, multiple SPNs should be provisioned to route calls based on the ZDP value and one or more dialed digits. Each SPN can then use a different RLI if required.

For example, assume ZDP = 101. It is possible to provision multiple SPNs (1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, and 1010) to route calls based on the ZDP value plus the first dialed digit. However, it may not be necessary to provision all SPN combinations. For example, if calls dialed with a first digit of "3" after the Access Code are invalid, then SPN "1013" does not need to be provisioned.

- Be careful when choosing how many dialed digits to include in the SPN. If one of the dialed digits is included in the SPN (that is, ZDP + one dialed digit), a maximum of ten SPNs need to be configured. Similarly if two dialed digits are included in the SPN (ZDP + two dialed digits), a maximum of one hundred SPNs need to be configured. For each additional dialed digit included in the SPN, the maximum number of SPNs that need to be provisioned is increased by a factor of ten.

Note 2: If a single Access Code that undergoes Zone-based digit manipulation is used for both on-net and off-net calls, then separate DMIs and SPNs must be provisioned to correctly route these calls. The SPN must correctly identify the routing to be used, and it must use a DMI that sets the Call Type correctly.

ESN Special Numbers are configured in LD 90. Respond to the prompts as follows:

- TRAN—Enter the Access Code.

- TYPE—Enter SPN for this configuration, as the ZDP value configured in step 3 on is usually a unique non-dialable number.

- SPN—Enter the ZDP value plus enough digits to distinguish the type of number, such as national, international, or local. There must be enough SPN entries to route all valid dialed numbers (see the example in this section).

- FLEN—Enter the number of digits that are expected for the call type.

- RLI–Enter the RLI configured in LD 86 in step 3b on . The RLI will route the call to the Gatekeeper with the correct type of number.

For example, assume the following:

- AC1 = 1, ZACB = AC1 AC1, and ZDP = 101

- Customer number = 0

- Long distance calls start with "1", have 11 digits, and use RLI = 10 and DMI = 10.

- Local calls start with "5" or "6", are seven digits long, and use RLI = 30 and DMI = 30.

Note: RLI and DMI values do not have to be the same, but for clarity, it may be useful to set them the same.

```
>LD  90
REQ  NEW
CUST 0
FEAT NET
TRAN AC1
TYPE SPN
SPN  1011
FLEN 14          11 digits for long distance + 3 digits for ZDP
...
RLI  10
SPN  1015
FLEN 10          7 digits for long distance + 3 digits for ZDP
...
RLI  30
...

SPN  1016
FLEN 10          7 digits for long distance + 3 digits for ZDP
...
RLI  30
...
```

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

Procedure 30
Configuring the Gatekeeper

After configuring Main Office routing to the Gatekeeper, the Gatekeeper must be provisioned to identify the desired endpoint for the calls. This procedure configures the Gatekeeper with the inserted digits specified by the zone-based digit manipulation configuration.
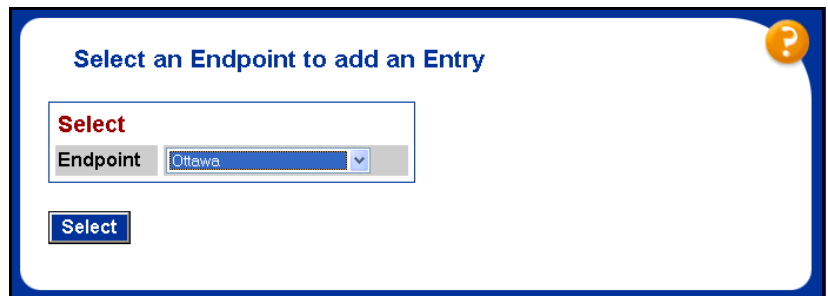
> *Note:* Instead of configuring the Gatekeeper, you can configure a route in the Main Office to directly route the call (see step 4 on).

This procedure provides information specific to the configuration of the Gatekeeper for this application. Refer to *IP Peer Networking* (553-3001-213) for complete details on configuring the Gatekeeper.

1   Select **Gatekeeper Standby Database Admin | Numbering Plan Entries | Create** from the navigation menu on the left-hand side of the Element Manager window.

The Select an Endpoint to add an Entry screen appears, as shown in .

Figure 74
Element Manager—Select an Endpoint to add an Entry

2   Select Branch Office from the Endpoint drop-down menu and click on **Select**.

The Add Entry screen appears, as shown in Figure 75.

Figure 75
Element Manager—Add Entry

3   Configure the Numbering Plan Entries for the Branch Office. This is usually set to the unique non-dialable number that identifies the Branch Office, as configured in the ZDP property of the Branch Office zone in LD 117 at the Main Office (see step 2 of Procedure 29 on).

The type of number configured in the Gatekeeper should be set to match the type of number as configured in Main Office ESN Special Number configuration in step 4 of Procedure 29 on .

Note: If some calls are to be routed differently from others, it is possible to provision the multiple Numbering Plan Entries in the Gatekeeper to achieve this.

For example, if ZDP = 101, it is possible to provision multiple Numbering Plan Entries (101, 1011, and so on) to route calls based on the ZDP value or the ZDP value plus some of the dialed digits.

Unlike on the Succession Call Server, if the ZDP plus additional digits are used to identify routing it is not necessary to provision all of the combinations. For example, if calls with digit strings starting with "1011" are to be routed differently from those starting with "101x" (where "x" is a digit other than "1"), then only "101" and "1011" need to be provisioned as Numbering Plan Entries on the Gatekeeper.

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

Procedure 31
Configuring the Branch Office

1   Configure the Route List Index at the Branch Office.

After the call arrives at the Branch Office, a route must be provisioned to handle the call. In order to be able to select a trunk to route calls, a Route List Index (RLI) must be configured in the Route List Block (RLB). The RLI uses the route number for PSTN trunk to route calls to the PSTN. A Digit Manipulation Index (DMI) can be associated with the RLI to allow manipulation of the digits to be outpulsed. For this application, the DMI is used to remove the ZDP digits that were inserted in the dialed digits at the Main Office.

a.   Configure the DMI in LD 86 with the DGT feature.

LD 86 – Configure Digit Manipulation Index at the Branch 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 Branch Office. (Part 2 of 2)

Prompt	Response	Description
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 (step 2 on page 206).
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.

b. Configure the RLI in LD 86 with the RLB feature.

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

LD 86 – Configure Route List Index. (Part 2 of 2)

Prompt	Response	Description
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 (step a on page 215).

For example, assume that the PSTN trunk is on route 18 and the Customer number = 0.

```
>LD  86
REQ  NEW
CUST 0
FEAT DGT
DMI  18
DEL  3          Set to remove ZDP added in the Main Office
INST
CTYP

REQ  NEW
CUST 0
FEAT RLB
RLI  18
ENTR 0
LTER NO
ROUT 18
...
DMI  18
...
```

2   Configure ESN Special Number and Digit Manipulation.

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 (step 4 on page 209)

After configuring the specialized route for calls that have been routed to the Branch Office by the Gatekeeper, the route must be associated with the ESN Special Number.

The Branch Office will receive the manipulated number as an incoming call, indicating that the ZDP value added at the Main Office is at the beginning of the number. The Branch Office ESN configuration must ensure that the extra digits (the ZDP value) are deleted by using a proper DMI. The call then terminates at the PSTN connection.

Note: The DMI configured in LD 86 in step 1 on is used to remove the digits that were inserted in the dialed number at the Main Office.

For example, assume ZDP at the Main Office = 101, Customer number = 0, and the RLI for the PSTN trunk = 18.

```
>LD  90
REQ  NEW
CUST 0
FEAT NET
TRAN AC1
TYPE SPN
SPN  1011
FLEN 0
...
RLI  18
```

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

Dialing plan configuration using Element Manager

From Element Manager, you can configure the Branch-specific zone dialing plan and Access Codes. From the Zone List window in Element Manager (see Figure 5 on), select the Branch Office Dialing Plan and Access Codes option, and enter the necessary information. Refer to Figure 76 on .

Figure 76
Zone Dial Plan and Access Codes

Site: 47.11.216.167 > Configuration > Zone List > Zone 0 >

Zone Dialing Plan and Access Codes

Input Description	Input Value
Zone Number (ZONE):	0
Prefix (ACB_DC1):	236
Country Code/Trunk Code (ACB_DC2):	345
Destination Network Code (ACB_DC3):	678
Local Access Code (ACB_LOC_AC):	Access Code 1 (AC1)
Long Distance Access Code (ACB_LD_AC):	Access Code 2 (AC2)

Submit   Refresh   Cancel

Testing PSTN access using a Branch Office Internet Telephone

Use Procedure 32 to test that PSTN access is working correctly.

Procedure 32
Testing PSTN access using a Branch Office Internet Telephone

1 From a Branch Office Internet Telephone in Local Mode (use Procedure 27 on if necessary):

   a. Make a local PSTN call.

   b. Make a long distance call.

   The calls must be routed according to the Branch Office ESN configuration.

2 From a Branch Office Internet Telephone in Normal Mode:

   a. Make a call to the local PSTN.

   b. Make a long distance call.

The calls must be routed according to the ESN configuration that was configured in Procedure 29 on .

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

For calls that tandem over the Virtual Trunk to the Branch Office and go out to the PSTN trunk(s) in the Branch Office, the following configuration problems can occur:

•   The call can receive overflow tones. Use LD 96 to view the digits sent to the Virtual Trunk (ENL MSGO {dch#}).

•   If the digits look correct at the Main Office, the Gatekeeper might not be properly configured. If the Gatekeeper rejects the call, a diagnostic message is displayed on the Succession Signaling Server console.

•   If the call makes it to the correct Branch Office (check that it is not going to the wrong node if the Gatekeeper is configured incorrectly) the Branch Office is probably rejecting it because it does not know the digit string. Use LD 96 to view the digits (ENL MSGI {dch#}).

Emergency Services configuration

Contents

This section contains information on the following topics:

Overview

For Branch Office applications, Nortel Networks recommends two alternative general methods to specify which digit string results in a call to emergency services:

- Use of the Emergency Services Access (ESA) feature—this is the preferred method in North America and some Caribbean and Latin American (CALA) markets. ESA provides specific features and capabilities required by legislation in these jurisdictions.

- Use of a special dialing sequence, such as a Special Number (SPN) in the Network Alternate Route Selection (NARS) data block. This method is also used where ESA is available, but the ESDN at the Main Office does not match the ESDN at the Branch Office.

Either of these methods have a Branch Office implementation which triggers the Main Office Succession Call Server to forward emergency services calls

to the Branch Office PSTN. Calls are redirected over a Virtual Trunk using the services of the Gatekeeper.

Emergency Services Access (ESA)

Configuring ESA for the Branch Office

For Emergency Services Access (ESA), the Main Office Succession Call Server forwards the call to the Branch Office for termination. Calls are redirected over a Virtual Trunk using the Gatekeeper services. The Gatekeeper routes the calls using a special number, referred to in this section as the ESA Special Number.

ESA must be configured and tested on each call processor (the Succession Call Server at the Main Office and the SSC at each Branch Office) to differentiate between emergency calls originating from Internet Telephones at each location and calls originating on trunks.

The steps to configure ESA for emergency access at each location are:

1   Determine the dialing plan for ESA calls.

2   Configure the Main Office emergency trunk (CAMA or PRI).

3   Configure the Virtual Trunk at the Main Office.

4   Configure ESN at the Main Office.

5   Configure ESA at the Main Office.

6   Configure the Branch Office zone on the Main Office.

7   Configure the ESA Special Number on the Main Office.

8   Test ESDN using a Main Office telephone.

9   Configure the Branch Office emergency trunk (CAMA or PRI).

10   Configure the Virtual Trunk at the Branch Office.

11   Configure ESN at the Branch Office.

12   Configure ESA at the Branch Office.

13   Configure the Branch Office zone on the Branch Office.

14 Configure the ESN SPN on the Branch Office.

15 Configure the Gatekeeper for the ESA Special Number used.

16 Test ESDN using a Branch Office Internet Telephone.

17 Test ESDN using an analog (500/2500-type) or digital telephone located at the Branch Office.

Determining the dialing plan for ESA calls

In many jurisdictions of the United States and Canada, the emergency number must be "911". The call processor cannot have a DN that conflicts with these digits, but since "9" is often used for NARS AC2 (the local call Access Code), this is not usually a problem.

The basic ESA feature only provides for a single ESA route per system. Since all Internet Telephones are associated with the same Main Office, all ESA calls therefore go to the same Public Safety Answering Point (PSAP) regardless from which Branch Office they originated. This is not satisfactory if the Branch Offices are widely dispersed.

In general, ESA calls should leave the network through a trunk at the Branch Office where the originating telephone is located. To enable this, it is necessary for telephones at each Branch Office to supply a unique identifying prefix to the Gatekeeper when the ESA calls are being routed so that the Gatekeeper can select a distinct route for each Branch Office. This prefix can be configured with the zone data for the Branch Office telephones. The provisioning of this prefix is an enhancement for Branch Office.

While a variety of numbering schemes are available, Nortel Networks recommends that customers use "0" + the ESN location code of the Branch + "911". This 7-digit number, referred to here as the ESA Special Number, is configured as a special number (SPN) in the Gatekeeper so that the Virtual Trunk routes the call to the Branch Office.

Procedure 33
Configuring the Main Office

You can use Element Manager or the Command Line Interface for this procedure. Refer to *IP Peer Networking* (553-3001-213) for details.

1   Configure the Main Office emergency trunk (CAMA or PRI).

Configure either analog CAMA or digital PRI to correctly signal the call identification.

ESA overrides all security features. Configure the trunk with restrictions so that other features cannot access the trunk.

2   Configure the Virtual Trunk using the procedure from *IP Peer Networking* (553-3001-213).

The Virtual Trunk must be configured to enable emergency calls originating from Branch Office Internet Telephones registered at the Main Office to reach the Branch Office.

3   Configure ESN.

ESA uses a route number rather than ESN route list index. However, ESN is required at the Branch Office.

4   Configure Emergency Services Access (ESA) in LD 24.

Configure an ACD number as an Emergency Services Directory Number.

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.

    5   Configure the Branch Office zone on the Main Office.

        a. Configure the Branch Office zone's ESA dialing information in LD 117.

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 Office 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.

        b. Enable the Branch Office zone ESA in LD 117

           ENL ZBR <Zone> ESA

6 Configure the ESA Special Number at the Main Office.

    a. Configure the ESA Special Number in the Gatekeeper. Using Gatekeeper management, configure the ESA Special Number defined for the Branch Office zone. Refer to *IP Peer Networking* (553-3001-213).

       Nortel Networks recommends that customers use "0" + the ESN Location code + ESDN. An example for location code 725 would be 0725911. The zero is recommended to prevent a collision in the ESN data with the HLOC entry.

    b. Configure the ESN Special Number at the Main Office.

        i. Configure the Digit Manipulation Index in LD 86 with the DGT feature.

LD 86 – Configure Digit Manipulation Index. (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	 (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

LD 86 – Configure Digit Manipulation Index. (Part 2 of 2)

Prompt	Response	Description
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.

    ii.   Configure the Route List Index in LD 86 with the RLB feature.

LD 86 – Configure Route List Index.

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
	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 Large Systems
	0-127	For Small Systems and Succession 1000 systems
DMI	(0)-999	Digit Manipulation Index number, as previously defined in LD 86, FEAT = DGT (step i on page 228)

iii. Configure the ESN Special Number and Digit Manipulation in LD 90.

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
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
...		

LD 90 – Configure ESN Special Number and Digit Manipulation. (Part 2 of 2)

Prompt	Response	Description
- 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.

Note: The Branch Office must recognize incoming digits on the Virtual Trunk and remove all but the ESDN.

7 Test ESDN using a Main Office telephone to confirm that Main Office calls go out the Main Office trunks.

If OSDN is used, the ESA route number must be blank to make test calls without using any trunk resources. It the route number has been configured, remove it by entering "x" at the prompt.

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

Procedure 34
Configuring the Branch Office

You can use Element Manager or the Command Line Interface for this procedure. Refer to *IP Peer Networking* (553-3001-213).

1   Configure an emergency trunk (CAMA or PRI).

2   Configure the Virtual Trunk.

   Before a call can come in on the Virtual Trunk, the Virtual Trunk must be configured.

3   Configure ESN.

   A Special Number (SPN) is configured at the Branch Office. The SPN contains the digits sent to the Gatekeeper to route the emergency call from the Main Office to the Branch Office.

   The SPN must use:

   •   A Route List Index (RLI) with local termination

   •   A Digit Manipulation Index (DMI)

      The system deletes the routing digits, leaving only the Emergency Services DN (ESDN).

   When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

4   Configure ESA.

   ESA configuration enables:

   •   telephones to connect to the Branch Office call processor (digital devices, analog devices, attendant consoles) and to dial the ESDN

   •   the Virtual Trunk (and any other trunks) to tandem a call to ESA

─────────────── **End of Procedure** ───────────────

Procedure 35
Configuring the Branch Office zone

1   Configure the Branch Office zone on the Branch Office.

In the Branch Office, only the zone number and bandwidth/codec selection is configured.

Note: Use the same zone number between the Branch Office and Main Office. The Main Office configuration (Procedure 33, step 5 on page 227) provides the Branch Office zone characteristics (local time, local dialing, and ESA).

2   Configure the ESN SPN.

The Branch Office must recognize the incoming digits on the Virtual Trunk and remove all but the ESDN. The call is routed to a local termination. ESA recognizes the call as an emergency call and selects the correct route. Refer to "Dialing plan configuration" on page 195.

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

Configuring the Gatekeeper

The Gatekeeper must be configured for the ESA Special Number (SPN). The Gatekeeper uses the ESA SPN to route the emergency call from the Main Office to the Branch Office.

Nortel Networks recommends that a consistent pattern be followed for all ESA calls. For example, use "0" + ESN Location code of the Branch Office node + the ESDN. An example for location code 725 would be: 0725911. The zero is recommended to prevent a collision in the ESN data with the HLOC entry.

For more information, refer to *IP Peer Networking* (553-3001-213).

Testing the number

Use Procedure 36 to test the ESDN number from any telephone in the
Branch Office.

Procedure 36
Testing ESDN using a Branch Office Telephone

1   For Internet Telephones:

    a. Dial the ESDN on a Branch Office Internet Telephone in Local Mode.
        Use Procedure 27 on to enter Local Mode.

        The calls must go out the emergency trunk(s) in the Branch Office.

    b. Dial the ESDN on a Branch Office Internet Telephone in Normal
        Mode.

        The calls must tandem over the Virtual Trunk to the Branch Office
        and go out the emergency trunk(s) in the Branch Office. The
        following configuration problems can occur:

        •   The call can receive overflow tones. Use LD 96 to view the digits
            sent to the Virtual Trunk (ENL MSGO {dch#}).

        •   If the digits look correct on the Main Office, the Gatekeeper
            might not be properly configured. If the Gatekeeper rejects the
            call, a diagnostic message is displayed on the Gatekeeper
            console.

        •   If the call makes it to the correct Branch Office (check that it is
            not going to the wrong node if the Gatekeeper is configured
            incorrectly) the Branch Office is probably rejecting it because it
            does not know the digit string. Use LD 96 to view the digits (ENL
            MSGI {dch#}).

2   For analog (500/2500-type) or digital telephones, dial the ESDN on a
    Branch Office analog (500/2500-type) or digital telephone.

    The calls must go out the emergency trunk(s) in the Branch Office.

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

Element Manager ESA configuration

From Element Manager, you can configure ESA. From the Zone List window in Element Manager (see Figure 5 on page 87), select the Branch Office Emergency Service option, and enter the necessary information. Refer to Figure 77 on page 235.

Figure 77
Zone Emergency Service Information

Emergency Service using Special Numbers (SPN)

Determining the dialing plan for emergency access calls is critical.

In many jurisdictions, the emergency number is a fixed number (for example, "112" or "999"). The call processor (Main Office Succession Call Server or Branch Office SSC) cannot have a DN that conflicts with these digits. To dial the emergency number in this configuration, a Branch Office user must dial the appropriate Access Code. For example, if AC2 is 9, then the user must dial "9 999" to make a call to emergency services.

Access to Emergency Service using SPN should be configured in the following circumstances:

- When the Emergency Service number at the Branch Office is different from that at the Main Office.

- When there is more than one number used for accessing Emergency Service; for example, when there are different numbers for Police, Fire, and Ambulance services.

- In markets where the ESA feature is not available (outside of North America and CALA).

To configure Emergency Service using SPN, follow the process outlined in "Dialing plan configuration" on . If Branch Office PSTN access is correctly configured, Emergency Service from the Branch Office will already be present.

Branch Office access to Emergency Service using SPN must be configured and tested on each call processor (the Main Office Succession Call Server and each Branch Office Succession System Controller) to differentiate between emergency calls originating from Internet Telephones at each location and emergency calls originating on trunks.

Abbreviated Dialing configuration

Contents

This section contains information on the following topics:

Overview

With Abbreviated Dialing, Internet Telephone users in the same geographic location, either the Main Office or the Branch Office, can call one another using a DN shorter than the configured DN.

This feature is implemented with a pretranslation group assigned to every telephone. All Internet Telephones in the same bandwidth management zone use the same pretranslation group. TDM telephones, which share the same dialing plan with Internet Telephones in a bandwidth management zone, also use the same pretranslation group.The pretranslation group assignment is more easily and quickly done using the OTM global change functionality.

Virtual Office Login always requires that the full DN be entered. In other words, a user cannot use the abbreviated DN to Virtual Login to an Internet Telephone.

The called telephone display always shows the full-length DN of the calling party.

Recommended configuration

Nortel Networks recommends the following configuration of Abbreviated Dialing in the Main and Branch Offices.

- The numbering plan at both the Main Office and Branch Office must have six or seven digits, including Internet Telephones in Local Mode.

- All Branch Office Internet Telephones are in a different bandwidth management zone than the Main Office Internet Telephones.

- Each bandwidth management zone has a unique pretranslation group number assigned to it.

- CLID of calls going to the public network (E.164/PSTN) are converted to the shorter DN by removing the digits added during pretranslation.

- Additional digits can still be added to the outgoing calling party number (the shortened DN) using CLID capabilities.

IMPORTANT!

When designing the numbering plan, make sure that there is no conflict between the long DN and the leading digits of the short DN so no pretranslation is invoked when a long DN is dialed.

For example, assume a long DN of "3623674" and a short DN of "3216". If the leading digit "3" in the short DN is configured to be translated to "3623", the short DN is then translated to "3623623674".

Configuring Abbreviated Dialing

Abbreviated Dialing must be configured at the Main Office and at the Branch Office.

Note: The Main Office and Branch Office must have the same configuration. In other words, the DNs, zones, and Pretranslation Groups must be exactly the same in both offices.

The steps to configure Abbreviated Dialing are:

1   Configure Speed Call Lists – see Procedure 37 on .

2   Configure Pretranslation Groups – see Procedure 38 on .

3   Assign the Pretranslation Group to the telephones – see Procedure 39 on .

4   Configure Incoming DID Digit Conversion – see Procedure 40 on .

Note: The Pretranslation Group number does not need to be the same as the number of the zone to which it is assigned. However, it does make configuration more intuitive if the two values are the same.

Procedure 37
Configuring Speed Call List (SCL)

1   In LD 18, configure the SCL for each Main Office zone.

LD 18 – Configure Speed Call Lists (SCL) for each zone.

Prompt	Response	Description
REQ	NEW	New
TYPE	SCL	Speed Call List
LSNO	1-8190	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.
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.		

2   Repeat step 1 to configure the SCL for each Branch Office zone.

3   In LD 18, configure the default 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.

─────────────── **End of Procedure** ───────────────

Procedure 38
Configuring Pretranslation Groups

While not required, it is recommended that the Pretranslation Group number (XLAT) be the same as the number of the zone to which it is assigned.

1   In LD 18, configure the Pretranslation Group for each Main Office zone.

LD 18 – Configure Pretranslation Group for each zone. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	New
TYPE	PRE	Pretranslation Group
XLAT	1-8191	Group number. Correlates Pretranslation Group to Speed Call List.

LD 18 – Configure Pretranslation Group for each zone. (Part 2 of 2)

Prompt	Response	Description
- PRE	1-8190	Pretranslation Speed Call List Number. Corresponds to LSNO defined in LD 18, TYPE=SCL

2   Repeat step 1 to configure the Pretranslation Group for each Branch Office zone.

3   In LD 18, configure the default Pretranslation Group at the Main Office.

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

4   In LD 15, activate the Pretranslation feature.

LD 15 – Activate Pretranslation feature.

Prompt	Response	Description
REQ:	CHG	Change
TYPE:	FTR	Features and options
...		
PREO	1	Activate Pretranslation feature
...		

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

Procedure 39
Assigning Pretranslation Groups to the telephones

The Pretranslation Group must be assigned to all Internet Telephones and TDM telephones. This procedure describes how to configure a single telephone, and it must be repeated for each telephone in the group. The global change utility in OTM can be used to configure all TDM telephones in the group at one time. For details, see *Optivity Telephony Manager: System Administration* (553-3001-330).

1   In LD 11, assign the Pretranslation Group to Internet Telephones and TDM telephones.

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.
...		

2   Repeat step 1 for each telephone in the group.

──────── **End of Procedure** ────────

Procedure 40
Configuring Incoming DID Digit Conversion (IDC)

1   In LD 15, configure Flexible Code Restriction for IDC.

LD 15 – Configure Flexible Code Restriction (FCR) for Incoming DID Digit Conversion. (Part 1 of 2)

Prompt	Response	Description
REQ:	CHG	Change

LD 15 – Configure Flexible Code Restriction (FCR) for Incoming DID Digit Conversion. (Part 2 of 2)

Prompt	Response	Description
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.

2   In LD 49, configure IDC.

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

3   In LD 49, configure Flexible Code Restriction to allow all codes.

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
...		

4   In LD 16, configure the Route Data Block to enable IDC on this route.

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
...		

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

Maintenance

Contents

This section contains information on the following topics:

Maintenance and diagnostics

This section outlines messages and commands specific to the Branch Office.

Firmware downloads

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 "Required firmware <version> is displayed on the telephone screen (see Figure 78 on).

Figure 78
Required firmware version

```
┌─────────────────────────────────────────┐
│                                         │
│ Succession                              │
├─────────────────────────────────────────┤
│                                         │
│   Required FW Vers xxxxxxx              │
│                                         │
│                                         │
├─────────────────────────────────────────┤
│                              Cancel     │
└─────────────────────────────────────────┘
```

This display can only be cleared by pressing the Cancel key. While this display appears, the user can only receive calls; they 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.

Procedure 41
Upgrading firmware

Upgrade procedures are generally found in *Succession 1000 System: Upgrade Procedures* (553-3031-258). Relevant information can be found in *IP Line: Description, Installation, and Operation* (553-3001-365).

1   At the Branch Office, upgrade Internet Telephone firmware on the Succession Signaling Server. For instructions, see the chapter "Uploading software upgrade files" in *Succession 1000 System: Upgrade Procedures* (553-3031-258).

2   Issue the CLI command `umsUpgradeAll`. Internet Telephones that are registered in Local Mode are upgraded.

3   At the Main Office, upgrade the firmware on the Succession Signaling Server.

4   Issue the CLI command `umsUpgradeAll`. Internet Telephones registered at-home to the Main Office are upgraded. Branch Office telephones are redirected back to their home TPS with the version number of the firmware required.

Since the Branch Office TPS firmware was upgraded in step 1 on page 247, when the Branch Office telephones are redirected back to the Branch Office in step 2 on page 247, they upgrade to the new firmware. The telephones are automatically redirected back to the Main Office after upgrading.

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

Always upgrade the Branch Office TPS before the Main Office TPS. Otherwise, the Branch Office TPS does not have the required version of firmware for upgrading the telephone. The Internet Telephone stays in Local Mode with the required firmware version displayed (see "Diagnostics" on page 248). The System Administrator has two options:

- Upgrade the firmware at the Branch Office, in which case the Internet Telephones are redirected to the Main Office after the upgrade.

- Issue the isetResetAll command on the Branch Office Signaling Server Maintenance terminal to redirect the Internet Telephones to the Main Office.

Diagnostics

Several cases involve automatic Main Office registration. This occurs, for example:

- if the telephone is under Test Local Test

- if a Branch User was either forced to logout by another login, or the telephone was used for a Virtual Office login and the login has subsequently logged out <under development>

- if the telephone rebooted and the logout status is lost

When a login is attempted and one of the following messages appears on the telephone display, there are a number of reasons. Tables 12 through 14, starting on page 249, provide error messages and troubleshooting parameters for Internet Telephone operation.

Table 12
Normal Operation troubleshooting (Part 1 of 2)

Message	Probable Cause	Actions
Local Mode	Test Local mode	Press Services key (key with Globe icon), and select Resume Normal Mode. Use the STAT c u command in LD 32 to show the reason why the Branch User stays in Local Mode.
Local Mode Server Unreachable (1)	Incorrect Primary or Alternate Gatekeeper IP address configured	Correct Primary or Alternate Gatekeeper IP address.
	Primary or Alternate Gatekeeper IP address unreachable from this endpoint.	Check network configuration, and update as required.
	NCS port number is not properly configured.	Correct Main Office and Branch Office NCS port numbers.
	Gatekeeper is down	Restore Gatekeeper.
	Link to gatekeeper is down	Restore Link to Gatekeeper.
Local Mode Server Unreachable (2)	Main Office TPS is unreachable from the Branch Office TPS	Check network configuration, and update as required.
	Main Office TPS is down	Restore Main Office Succession Signaling Server.
	Link to Main Office TPS is down	Restore Link to Main Office TPS.
	Main Office Succession Call Server is down	Restore Main Office Succession Call Server.
	Main Office node is not registered as an H.323 endpoint to the Gatekeeper.	Register the Main Office node to the Gatekeeper.

Table 12
Normal Operation troubleshooting (Part 2 of 2)

Message	Probable Cause	Actions
Local Mode Invalid ID (1)	Branch User ID endpoint is not in Gatekeeper database	Check Gatekeeper database and update as required.
	Incorrect Branch User ID configured	Correct Branch User ID configuration in Branch Office TN.
Local Mode Invalid ID (2)	Branch User ID not found in any equipped TN	Check Main Office Branch User configuration, and update as required.
	Incorrect Branch User ID configured	Correct Branch User ID configuration in Branch Office TN.
Local Mode Invalid ID (3)	Gatekeeper database has Branch Office as endpoint for Branch User ID	Correct Gatekeeper database configuration to have Main Office as Branch User ID endpoint.
	Incorrect Branch User ID configured	Correct Branch User ID configuration in Branch Office TN.
Required FW Vers	Firmware incompatible with Main Office TPS	Upgrade Internet telephone firmware at the Branch Office TPS. *Note:* Nortel Networks recommends that customers upgrade all Branch Office TPSs before they upgrade the Main Office TPS during firmware upgrade. The Internet Telephones are directed to the Branch Office for firmware upgrade, and then redirected to the Main Office automatically.

Table 13
Legend for LD 32 STAT command Login status (Part 1 of 3)

Number	Description
0	Initialize status
1	Branch User Login

Table 13
Legend for LD 32 STAT command Login status (Part 2 of 3)

Number	Description
2	Branch User Local Mode Test
3	Branch User Config
5	Branch User Forced Logout (F/W Download)
6	Branch User No Branch Office Password Provisioned
7	Branch User Locked from Branch Office Password Retry
10	Branch User Gatekeeper Unreachable
11	Branch User Gatekeeper User Unknown (user id - TN combination unknown)
12	Branch User Main Office unreachable, or Main Office is not registered with the Gatekeeper as an endpoint.
13	Branch User Main Office User ID Unknown, or Branch User Main Office User ID and Main Office TN Combination does not exist, or Internet Telephone telephone type and Main Office TN telephone type do not match.
14	Branch User Firmware Out of Sync
15	Another Branch User already logged in the User ID at the Main Office and active on a call
16	Branch User ID entry in Gatekeeper database has Branch Office as endpoint

Table 13
Legend for LD 32 STAT command Login status (Part 3 of 3)

Number	Description
30	Virtual Office Login
32	Virtual Office Locked from Login

Table 14
Branch User Config troubleshooting (Part 1 of 5)

Message	Probable Cause	Actions
Busy, try again	Main Office TN already equipped and active on a call.	Identify duplicate Branch User ID allocation, and correct the configuration accordingly.
	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
Invalid ID (1)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Branch User ID not in Gatekeeper database.	Update Gatekeeper database to include Branch User ID.
Invalid ID (2)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	No Main Office TN associated with Branch User ID configured.	Configure Main Office TN to associate with Branch User ID.
	Main Office TN associated with the Branch User ID and the programmed TN on the Internet telephone does not match.	Configure a Main Office TN to match the Internet telephone TN, or configure a new Branch Office TN and Internet telephone TN to match the Main Office TN.

Table 14
Branch User Config troubleshooting (Part 2 of 5)

Message	Probable Cause	Actions
Invalid ID (3)	Gatekeeper database has Branch Office as endpoint for Branch User ID.	Correct Gatekeeper database configuration to have Main Office as Branch User ID endpoint.
	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
Locked from Login	Incorrect Branch Office TPS Internet Telephone Installer Password, or Temporary Internet Telephone Installer Password entered three times.	Wait one hour for the lock to clear automatically, or use the clearLockout command on the Branch Office IPL maintenance terminal to clear the lockout.
	Incorrect Main Office TN Station Control Password, Main Office Internet Telephone Installer Password, or Main Office Temporary Telephone Installer Password entered three times.	Wait one hour for the lock to clear automatically, or disable and enable the Main Office TN in LD 32 to clear the lockout.
Permission Denied (1)	Internet Telephone Installer Password or Temporary Internet Telephone Installer Password at the Branch Office TPS not configured or disabled.	Set or enable the Internet Telephone Installer Password or Temporary Internet Telephone Installer Password at the Branch Office TPS.

Table 14
Branch User Config troubleshooting (Part 3 of 5)

Message	Probable Cause	Actions
Permission Denied (2)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Internet Telephone Installer Password at the Main Office TPS not configured or disabled and the Branch User ID is already assigned to a user in another Branch Office.	Identify duplicate Branch User ID allocation, and make correction.
Permission Denied (3)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Incorrect Internet Telephone Installer Password at the Main Office TPS entered.	Retry with correct Internet Telephone Installer Password at the Main Office TPS.
	Station Control Password not configured in Main Office TN.	Add Station Control Password to the Main Office TN.
Permission Denied (4)	Terminal type configured in the Main Office TN does not match the type of the Branch Office Internet telephone.	Change the terminal type in the Main Office TN to match the type of the Branch Office Internet Telephone, or change the terminal type in the Branch Office TN to match the type in the Main Office TN, and replace the Branch Office Internet Telephone with the correct type.

Table 14
Branch User Config troubleshooting (Part 4 of 5)

Message	Probable Cause	Actions
Permission Denied (6)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Incorrect Branch Office Internet Telephone Installer Password, or Temporary Branch Office Internet Telephone Installer Password entered.	Retry with correct Branch Office Internet Telephone Installer Password, or Temporary Branch Office Internet Telephone Installer Password.
	Incorrect Main Office Internet Telephone Installer Password or incorrect Station Control Password entered.	Retry with correct Main Office Internet Telephone Installer Password or correct Station Control Password.
Server Unreachable (1)	Incorrect Primary or Alternate Gatekeeper IP address configured	Correct Primary or Alternate Gatekeeper IP address.
	Primary or Alternate Gatekeeper IP address unreachable from this endpoint.	Check network configuration, and update as required.
	NCS port number is not properly configured.	Correct Main Office and Branch Office NCS port numbers.
	Gatekeeper is down	Bring Gatekeeper into service.
	Link to gatekeeper is down	Restore Link to Gatekeeper.

Table 14
Branch User Config troubleshooting (Part 5 of 5)

Message	Probable Cause	Actions
Server Unreachable (2)	Main Office TPS is unreachable from the Branch Office TPS	Check network configuration, and update as required.
	Main Office TPS is down.	Bring Main Office Succession Signaling Server into service.
	Link to Main Office TPS is down.	Restore link to Main Office TPS.
	Main Office Succession Call Server is down.	Bring Main Office Succession Call Server into service.
	Main Office node is not registered as an H.323 endpoint to the Gatekeeper.	Register the Main Office node to the Gatekeeper.

Table 15
Virtual Office Login Troubleshooting (Part 1 of 3)

Message	Probable Cause	Actions
Busy, try again	Remote telephone is active on a call.	Wait for remote telephone to become idle and try again.
	Automatic Call Distribution (ACD) telephone to login is logged in.	Log out ACD telephone from a queue before a Virtual Office login to it from another telephone.
	Make-Set-Busy is inactive on ACD telephone to log in.	Set Make-Set-Busy active on ACD telephone to log in.

Table 15
Virtual Office Login Troubleshooting (Part 2 of 3)

Message	Probable Cause	Actions
Invalid ID (1)	Incorrect User ID entered.	Enter correct User ID.
	User ID not in Gatekeeper database.	Update Gatekeeper database to include User ID.
Invalid ID (2)	Incorrect User ID entered.	Enter correct User ID.
Locked from Login	Incorrect Station Control Password entered three times.	Wait one hour for the lock to clear automatically, or disable and enable the remote telephone in LD 32 at the remote Succession Call Server to clear the lock.
Permission Denied (3)	Incorrect User ID entered.	Retry with correct User ID.
	Remote telephone has no Station Control Password.	Configure the remote telephone with Station Control Password.
Permission Denied (4)	Incorrect User ID entered.	Retry with correct User ID.
	Attempt to Login to a remote i2004 or i2050 telephone from an i2002 telephone.	Go to an i2004 or i2050 telephone and try again.
Permission Denied (5)	Incorrect User ID entered.	Retry with correct User ID.
	Remote telephone does not have VOUA Class of Service.	Configure the remote telephone with VOUA Class of Service.

Table 15
Virtual Office Login Troubleshooting (Part 3 of 3)

Message	Probable Cause	Actions
Permission Denied (6)	Incorrect User ID entered.	Retry with correct User ID.
	Incorrect Station Control Password entered.	Select Retry, and try again with the correct Station Control Password.
Server Unreachable (1)	Incorrect Primary or Alternate Gatekeeper IP address configured	Correct Primary or Alternate Gatekeeper IP address.
	Primary or Alternate Gatekeeper IP address unreachable from this endpoint.	Check network configuration, and update as required.
	NCS port number is not properly configured.	Correct NCS port number.
	Gatekeeper is down	Bring Gatekeeper up.
	Link to gatekeeper is down	Restore Link to Gatekeeper.
Server Unreachable (2)	Remote TPS is down.	Bring remote Succession Signaling Server up.
	Link to remote TPS is down.	Restore link to Remote TPS.
	Remote Succession Call Server is down.	Bring remote Succession Call Server up.

Succession Signaling Server commands

This section describes new and changed Branch Office-specific Command Line Interface (CLI) commands on the IP Line Succession Media Card.

isetShow

The isetShow command is enhanced to provide the type of Internet Telephone registration and the new registration status. The result prints out as shown in Figure 79.

Figure 79
isetShow report

```
Set Information
---------------
 IP Address    Type  RegType State  Up   Time    Set-TN  Regd-TN        HWID         FWVsn  UNIStimVsn SrcPort DstPort
------------- ----- ------- ------ -- -------- ------- ------- ----------------- ------- ---------- ------- -------
47.11.249.202 i2004 Regular online  1 01:54:09  062-03  062-03 18006038763e996600 0602B44     2.5        5100    5000
47.11.249.199 i2004 Regular online  1 01:53:33  062-02  062-02 180060387639156600 0602B44     2.5        5100    5000
47.11.249.205 i2002 Branch  online  0 21:30:06  062-11  062-11 18006038dd001c6600 0603B44     2.5        5100    5000
47.11.239.52  i2004 Branch  online  0 01:26:09  062-01  062-01 180060387634c16600 0602B50     2.5        5100    5000

Total sets = 4
value = 0 = 0x0
```

clearLockout "TN" or "IP"

A registration lock is placed at the TPS after three consecutive failed attempts to enter either the Internet Telephone Installer Password or the Temporary Internet Telephone Installer Password.

The lockout affects the Virtual Office login or Branch User Config and lasts for one hour. This lockout does not survive re-registration of the Internet Telephone. However, the installation technician can issue the clearLockout command to clear the lockout for a particular telephone.

This command has one parameter – the TN or IP address of the telephone.

Succession Call Server commands

Print

LD 117 contains commands to view Branch Office zones at the Main Office Succession Call Server.

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 Office 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.

Enable/disable Branch Office zone features

LD 117 contains commands to enable and disable features for the
Branch Office zones.

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.

Status

LD 117 contains commands to view the status of Branch Office zones at the
Main Office Succession Call Server.

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)

Inventory

The inventory (generated in LD 117) is for all Internet Telephones registered
to the Succession Call Server or Succession System Controller (SSC). This
includes Internet Telephones registered by a Virtual Office and
Branch Office login at the Main Office Succession Call Server. At the SSC,

inventory only includes Internet Telephones registered at the Branch Office, not all the Internet Telephones physically located at the Branch Office.

To get an inventory of all Internet Telephones at a Branch Office, execute the `INV GENERATE` command at the Branch Office with Branch Users in Local Mode.

> *Note:* Do this only during a maintenance window.

To register all Internet Telephones at the SSC, disconnect the WAN connection to the Main Office (not recommended) or individually logout the Internet Telephones from the Main Office. See "Test Local Mode" on .

LD 117 contains inventory commands. These commands include the registered Internet Telephones.

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.

Branch Office software and system information

When the Succession Branch Office (SBO) package is equipped, the `ISS` and `ISSP` commands in LD 22 display system and software information for the Branch Office. If the SBO package is restricted, the two commands provide information about the Succession Call Server.

LD 22 – Print Branch Office software and system information.

Prompt	Response	Description
REQ	ISS ISSP	Print issue and release Print system and patch information

Appendix A: Preprogrammed data

Contents

This section contains information on the following topics:

Introduction

To install a Succession 1000 system, you must first enter customer data in overlays. For example, you must assign features to the telephone keys.

For software installation, it is not necessary to program data for the SSC card in advance. The SSC card can be programmed with the minimum number of files to enable the Branch Office to operate.

This chapter contains the following procedures:

- "Passwords and codes" on

- "Default numbering plan" on

- "Flexible Feature Codes" on

- "SDI ports" on

- "Trunk routes" on

- "System parameters" on

- "Customer data" on

- "Trunk models" on

- "Telephone models" on

Passwords and codes

Table 16 lists each function and its password or code.

Table 16
Passwords and codes (Part 1 of 2)

Function	Code or extension(s)
TTY password (For access to TTY system overlays)	0000
Level 1 login name access	ADMIN1
Level 1 password access	0000
Level 2 login name access	ADMIN2
Level 2 password access	0000
Administration telephone password	1234
Administration telephone FFC	*41

Table 16
Passwords and codes (Part 2 of 2)

Function	Code or extension(s)
SPRE code	1
Telephone relocation Flexible Feature Code	*40
Telephone Removal Flexible Feature Code	*42
Telephone relocation password (SRCD)	1234

Note: Login name access is required when LNAME_OPTION is set to YES.

Default numbering plan

The default numbering plan for a Branch Office is based on the following guidelines:

- The default numbering plan uses four digits and starts at 2200.

- The prime extension number (DN) for each telephone is in the range 2200-2XXX. The value of "XXX" varies depending on the number of telephones in the system. Secondary extension numbers use numbers outside this range. This arrangement enables the Succession 1000 to automatically configure telephones.

First digits

Table 17 shows the default numbering plan for a Branch Office.

Table 17
Default numbering plan—First digit (Part 1 of 2)

First digit	Preprogrammed use for digit
1	SPRE code
2	Not used
3	Not used

Table 17
Default numbering plan—First digit (Part 2 of 2)

4	Not used
5	Not used
6	Not used
7	COT/TIE/DID/WATS/FEX/RAN/MUS/AWR/Paging Trunk Access Codes and attendant DN, Call park DNs
8	Not used
9	Not used
0	Attendant extension

Note: The first number of the default numbering plan is preprogrammed as 2200. The remaining numbers are assigned in software. These numbers do not become active until you select the numbers during the telephone activation procedure.

The digit "7" in the default numbering plan is programmed with many system features to help you configure the Succession 1000 system.

Important extension numbers

Table 18 lists important extension numbers.

Table 18
Default numbering plan – important extension numbers

Extension	Use
Attendant extension	0
Call park extensions	7900-7919

Flexible Feature Codes

Many administrative procedures use Flexible Feature Code (FFC) data. Table 19 lists the FFCs for the Succession 1000 system.

Table 19
Flexible Feature Codes

FFC Prompt	FFC	Definition
ASRC	*40	Automatic Set Relocation
AREM	*42	Automatic Set Removal Code
ADMN	*41	Administration Set Access Code
CFWA	#1	Call Forward All Calls Activate
CFWD	#1	Call Forward All Calls Deactivate
C6DS	*70	6 Party Conference Code
HOLD	#4	Permanent Call Hold
MNTC	*43	Maintenance Access Code
PUGR	*71	Pick-up Group Code
RDLN	*72	Last Number Redial
RDST	*73	Store Last Number Redial
RGAA	*74	Ring Again Activate
RGAD	*75	Ring Again Deactivate
RGAV	*77	Ring Again Verify
SPCC	#2/*80	Speed Call Controller Code
SPCU	#3/*81	Speed Call User Code
SSPU	*89	System Speed Call User Code

SDI ports

The minimum port configuration for the Branch Office is three SDI ports, all of which are on the NTDK20FA SSC card. Table 20 shows the default SDI port configuration. The value for "XX" is set on the faceplate of the SSC circuit card.

Table 20
Pre-configured SDI ports

TTY Number	Card	Port	Use	Configuration
0	0	0	MTC/SCH/BUG	XX/8/1/NONE
1	0	0	MTC/SCH/BUG	1200/8/1/NONE
2	0	1	CTY	1200/8/1/NONE

Table 21
Pre-configured PTY ports

TTY Number	Card	Port	Use
14	0	0	MTC/SCH/BUG
15	0	1	MTC/SCH/BUG

Modem port

The pre-configured modem port enables the remote maintenance modem to be connected without additional system programming. This port is pre-configured as TTY 0 (port 0 on the SSC card) and programmed for Maintenance (MTC), Service Change (SCH), and BUG messages.

ESDI settings

Table 22 lists the preset ESDI settings.

Table 22
ESDI settings

Setting	Code
BPS	4800
CLOK	EXT
IADR	003
RADR	001
T1	10
T2	002
T3	040
N1	128
N2	08
K	7
RXMT	05
CRC	10
ORUR	005
ABOR	005
USER	CMS
ENL	NO

Telephone tones

The telephone tones in North America are as follows:

• **Dial tone:** A continuous tone.

- **Special dial tone**: Three beeps followed by continuous dial tone.

- **Overflow tone:** Like a busy tone, except faster and higher.

- **Relocation tone:** A short high-pitched beep that continues for 4 seconds, followed by silence.

Trunk routes

Table 23 shows preprogrammed trunk route information that you must have to activate and modify trunks.

Table 23
Preprogrammed trunk route information (Part 1 of 2)

Route	Type	Access Code	Mode	Interface
00 *	COT	7100	IAO	-
01 *	COT	7101	ICT	-
02 *	COT	7102	OGT	-
03	TIE	7103	IAO	-
04	TIE	7104	ICT	-
05	TIE	7105	OGT	-
06	DID	7106	ICT	-
07	WAT	7107	IAO	-
08	WAT	7108	ICT	-
09	WAT	7109	OGT	-
40	MUS	7140	OGT	-
41	AWR	7141	-	AUD
42	RAN	7142	-	DGT
43	RAN	7143	-	AUD
44	PAG	7144	OGT	-

Table 23
Preprogrammed trunk route information (Part 2 of 2)

Route	Type	Access Code	Mode	Interface
50	FEX	7150	IAO	-
51	FEX	7151	ICT	-
52	FEX	7152	OGT	-

Note: Trunk routes marked with an asterisk (*) are configured to support Call Detail Recording (CDR) output. CDR is pre-configured in LD 16 as follows:

```
CDR    YES
INC    YES
OAL    YES
AIA    YES
```

System parameters

The default system parameter values for the Succession 1000 system are given in Table 24.

Table 24
System parameters

Parameter	Value
Low Priority Input Buffers (LPIB)	450
High Priority Input Buffers (HPIB)	450
Number of Call Registers (NCR)	300
Multiple Appearance Redirection Prime (MARP) feature allowed	YES

Refer to "Capacity Engineering" in *Succession 1000 System: Planning and Engineering* (553-3031-120) for further information on buffer sizes.

The preprogrammed data also include virtual superloops 96, 100, 104, 108, and 112.

Customer data

The default customer number used in the preprogrammed data is zero (0).

Trunk models

Do not use the DIP Class of Service for Model 19 of TIE trunk mode. The correct Class of Service for model 19 of TIE trunk mode is DTN.

Note: All trunks are programmed as immediate start/supervision = YES, with the exception of trunks with an asterisk(*). Trunks marked with an asterisk (*) are set for wink start/supervision = YES.

Table 25
Preprogrammed trunk route information (Part 1 of 4)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
COT	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900

Table 25
Preprogrammed trunk route information (Part 2 of 4)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
TIE	XUT	1	OAD	DIP	3COM/600
		2	LDR	DIP	3COM/600
		3	OAD	DTN	3COM/600
		4	LDR	DTN	3COM/600
		5	OAD	DIP	3COM/900
		6	LDR	DIP	3COM/900
		7	OAD	DTN	3COM/900
		8	LDR	DIP	3COM/900
TIE	XEM	16	EAM	DIP	-/600
		17	EM4	DIP	-
		18	EAM	DTN	-/600
		19	EM4	DTN	-

Table 25
Preprogrammed trunk route information (Part 3 of 4)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
DID	XUT	1	LDR Wink Start Supv = YES	DIP	3COM/600
		2	LDR Wink Start Supv = YES	DTN	3COM/600
		3	LDR Wink Start Supv = YES	DIP	3COM/900
		4	LDR Wink Start Supv = YES	DTN	3COM/900
		5*	LDR Wink Start Supv = YES	DIP	3COM/600
		6*	LDR Wink Start Supv = YES	DTN	3COM/600
		7*	LDR Wink Start Supv = YES	DIP	3COM/900
		8*	LDR Wink Start Supv = YES	DTN	3COM/900
WAT	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900
MUS	XUT	1			3COM/600

Table 25
Preprogrammed trunk route information (Part 4 of 4)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
AWR	XUT	1			600/1200
RAN	XUT	1			600/1200
PAG	XUT	1	LDR	DIP	3COM/600
		2	OAD	DIP	3COM/600
		3	LDR	DTN	3COM/600
		4	OAD	DTN	3COM/600
		5	LDR	DIP	3COM/900
		6	OAD	DIP	3COM/900
		7	LDR	DTN	3COM/900
		8	OAD	DTN	3COM/900
PAG	XEM	16	EAM	DIP	-/600
		17	EM4	DIP	-
		18	EAM	DTN	-/600
PAG	XEM	19	EM4	DTN	-
FEX	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900

Telephone models

Define three models (model# 20) for i2002, i2004 and i2050 with KEY 0 SCR, VOLA CLS, and VOUA CLS.

Define model# 20 for analog (500/2500-type) telephones.

Appendix B: Branch Office engineering example

Contents

This section contains information on the following topics:

Introduction

This chapter provides sample engineering calculations for a Branch Office, with either a Succession 1000 or Succession 1000M Main Office.

The following abbreviations are used in formulas:

- IT = Internet Telephone

- AT = analog (500/2500-type) telephone

- SMC = Succession Media Card

Assumptions

Equipment characteristics

Assume the Branch Office has the equipment characteristics given in Table 26.

Table 26
Equipment characteristics

Number	Type
120	Internet Telephones
36	Analog (500/2500-type) telephones

Traffic characteristics

Assume the Branch Office has the traffic characteristics given in Table 27.

Table 27
Traffic characteristics

Number	Comments
6 CCS	For each Internet Telephone, 50% of calls go to other Internet Telephones, and 50% of calls go to analog (500/2500-type) telephones and PRI trunks.
5 CCS	For each analog (500/2500-type) telephone, 40% of calls go to PRI trunks, and 60% of calls go to Internet Telephones.
120 seconds	The average holding time for each call.

Note: Conference traffic is generally not singled out for calculation in traffic engineering. When a Branch Office does not have conference capability, conference call participants must use the WAN to reach the Main Office to join conferences. However, if the traffic is significant (a rough guide is more than 10% of Internet telephone traffic), traffic should be included in the WAN bandwidth calculation.

Required calculations

The following is a summary of the required calculations:

- number of Virtual Trunks to the Main Office

- number of SMCs

- real-time load for the Succession Call Server

- bandwidth for WAN

- bandwidth for LAN

Calculations

Figure 80 on page 280 is a conceptual representation of a Branch Office H.323 WAN Gateway. An actual system could require different types and number of cards.

Traffic

Traffic calculations are based on the traffic flows shown in Figure 80 on page 280.

Figure 80
Branch Office traffic flow

Note: 1. Internet Telephone to Internet Telephone calls do not go through the SMC.
      2. Internet Telephone to Main Office calls do not go through the SMC.
      3. All other calls go through the SMC.

553-AAA0186
553-AAA0126
553-AAA0125
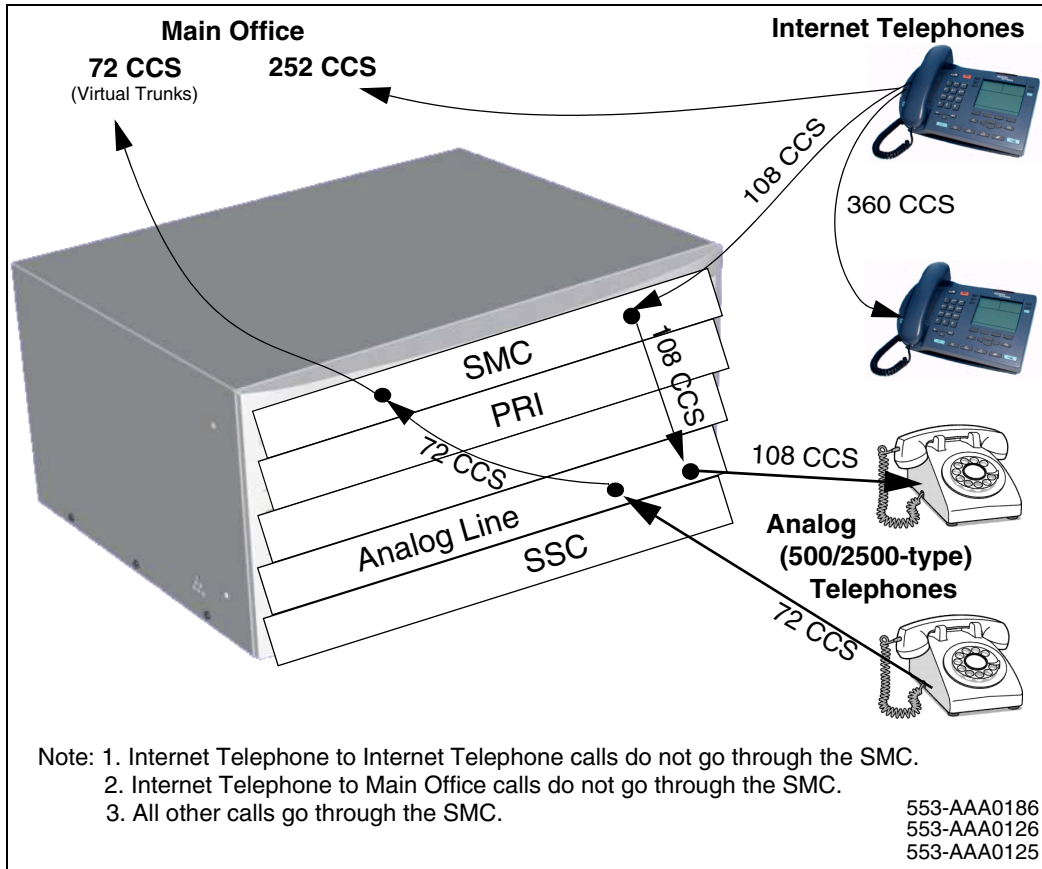
Procedure 42
Calculating traffic

1   Calculate the Internet Telephone to Internet Telephone traffic (intra-Internet Telephone traffic does not go through the SMC):

Total IT x IT CCS x % calls to Intra-IT calls = Intra-IT traffic

120 x 6 x 0.5 = 360 CCS

2   Calculate the Internet Telephone traffic to analog (500/2500-type) telephones:

Number of ATs x CCS for each AT x % of calls to ITs = IT traffic to analog (500/2500-type) telephones

36 x 5 x 0.6 = 108 CCS (this traffic is part of SMC traffic)

3   Calculate the Internet Telephone traffic to Main Office resources (MOR):

Total ITs x IT CCS - Intra-IT traffic - IT traffic to analog (500/2500-type) telephones = IT traffic to MOR

120 x 6 - 360 - 108 = 252 CCS

4   Calculate the analog (500/2500-type) telephone traffic to Virtual Trunks (IPPT):

Number of ATs x CCS for each AT x % of calls to Virtual Trunks = Analog (500/2500-type) traffic to IPPT

36 x 5 x 0.4 = 72 CCS (this traffic is part of SMC traffic)

This is the total IPPT traffic.

5   Calculate total IP traffic to the LAN:

a.   Total ITs x IT CCS + analog traffic to IPPT = Total CCS

120 x 6 + 72 = 792 CCS

b.   Total CCS ÷ 36 = Erlangs

792 ÷ 36 = 22 Erlangs

6   Calculate the SMC traffic from analog (500/2500-type) telephones to Internet Telephones and Virtual Trunks:

IT traffic to analog (500/2500-type) telephones + Analog traffic to IPPT = SMC traffic

108 + 72 = 180 CCS

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

Branch Office H.323 WAN Gateway and Expansion requirements

Table 28 shows the number of cards required and the devices on those cards.

Table 28
Branch Office H.323 WAN Gateway and Gateway Expansion card type, number and devices

Card type	Number of cards	Devices on cards
SMC	1	32 DSP channels
XALC	3	36 Analog (500/2500-type) telephones

One Branch Office H.323 WAN Gateway has four slots available, and an H.323 WAN Gateway Expansion chassis is required for additional cards.

Requirement: one Branch Office H.323 WAN Gateway

Note: An analog line card or digital line card has 16 ports. If 36 digital telephones are used instead of 36 analog (500/2500-type) telephones, the resulting calculation would yield the same number of cards: three XDLC cards, taking the place of three XALCs. The total number of card slots and Branch Office H.323 WAN Gateway requirements are the same.

─────────── **End of Procedure** ───────────

Procedure 43
Calculating Succession Call Server Loading

Only the CCS from one terminating end of a connection is used in the Call Server loading calculation. For example, a call from one Internet Telephone to another includes the CCS from both telephones. The Succession Call Server loading calculation divides the CCS by two.

1   Calculate the Internet Telephone to Internet Telephone calls:

IT to IT CCS x 100 seconds ÷ average hold time ÷ 2 = IT to IT calls

360 x 100 ÷ 120 ÷ 2 = 150 calls

Note: Dividing by 2 is only required for IT-to-IT traffic. Intra-IT CCS is double counted in relation to the number of calls. For example, one call lasting 100 seconds appears as one CCS on the originating telephone, one call on the CPU, and one CCS on the terminating telephone. Two CCS on telephones must be divided by two to get the correct number of calls.

2   Calculate the Internet Telephone to Main Office resources (MOR) calls:

IT to IT CCS x 100 seconds ÷ average hold time = IT to MOR calls

252 x 100 ÷ 120 = 210 calls

3   Calculate the Internet Telephone to analog (500/2500-type) telephones:

IT to AT CCS x 100 seconds ÷ average hold time = IT to AT calls

108 x 100 ÷ 120 = 90 calls

4   Calculate the analog (500/2500-type) telephone to Virtual Trunks (IPPT) calls:

AT to IT CCS x 100 seconds ÷ average hold time = AT to IPPT calls

72 x 100 ÷ 120 = 60 calls

5   Calculate the Succession Call Server loading in EBC:

IT to IT calls x (1+f1) + IT to MOR calls x (1+f2) + IT to AT calls x (1+f3) + AT to IPPT calls x (1+f4) = Succession Call Server EBC

150 x 2.15 + 210 x 1.68 + 90 x 1.48 + 60 x 1.18 = 879.3 EBC

6   Calculate the Succession Call Server loading in percent:

Succession Call Server loading ÷ CS maximum EBC = % loading

879.3 ÷ 35000 = 3%

Requirement: The loading of this configuration for Succession Call Server is very low at 3%. This Succession Call Server can be located at the Branch Office or anywhere within the zone.

——————— **End of Procedure** ———————

Bandwidth requirements

Bandwidth requirements in this section refer to the information in Table 29, Table 30, and Table 31.

Table 29
TLAN bandwidth for one channel (one Erlang)

CODEC	Payload	TLAN
G.711	10 ms	126 kbit/s
G.711	20 ms	95 kbit/s
G.711	30 ms	85 kbit/s
G.729A	10 ms	70 kbit/s
G.729A	20 ms	39 kbit/s
G.729A	30 ms	29 kbit/s

Table 30
Traffic capacity at P.01, P.005, and P.001 GOS

Device	P.01	P.005	P.001
SMC (32-port)	794 CCS	744 CCS	655 CCS
T1 (24 ports)	550 CCS	511 CCS	441 CCS
E1 (30 ports)	732 CCS	685 CCS	600 CCS

Table 31
WAN bandwidth for one channel (one Erlang) (Part 1 of 2)

CODEC	Payload	WAN
G.711	10 ms	48 kbit/s
G.711	20 ms	40 kbit/s
G.711	30 ms	37 kbit/s
G.729A	10 ms	20 kbit/s

Table 31
WAN bandwidth for one channel (one Erlang) (Part 2 of 2)

CODEC	Payload	WAN
G.729A	20 ms	12 kbit/s
G.729A	30 ms	9 kbit/s

Procedure 44
Calculating TLAN bandwidth for Internet Telephone traffic

Incremental bandwidth required at TLAN to carry given voice traffic:

1   Calculate the data rate:

Total traffic in Erlangs (from) x 95 kbps

22 x 95 kbps = 2090 kbps = 2.09 Mbps

Note: One Erlang of TDM 64 kbps channel becomes 95 kbps packets after G.711 codec transcoding, which adds overhead. See Table 31 on if another type of codec is used.

Requirement: TLAN bandwidth 2.02 Mbps

───────────   **End of Procedure**   ───────────

Procedure 45
Calculating Branch Office with Virtual Trunk WAN

Assuming G.711/30 ms for the WAN, the traffic distribution is as follows:

1   Calculate the SMC traffic:

SMC traffic = 180 CCS

One SMC is needed (794 CCS capacity).

2   Calculate the Virtual Trunk traffic:

IPPT traffic = 72 CCS

An equivalent of a 24-port channel (capacity 550 CCS from Table 30 on) is sufficient to handle the Virtual Trunk traffic.

3   Calculate the incremental WAN bandwidth:

a.   WAN traffic = IT traffic to MOR + Analog traffic to IPPT
= 252 + 72
= 324 CCS

b.   WAN bandwidth = 324/36 x 37 kbps (from Table 31 on for G.711 codec with 30 ms payload)
= 333 kbps

Refer to Table 31 on for other codecs or payload sizes.

───────── **End of Procedure** ─────────

Branch Office conference engineering

With no local conference

Two parties at a Branch Office using Internet telephones call each other. They conference-in a third party from the same Branch Office. The conference calls use a WAN to reach the Conference Bridge at the Main Office. Refer to Table 31 on for bandwidth requirements if the codec or payload or both differ from what is assumed in the following Branch Office conference scenarios.

The calculated conference WAN bandwidth is added to the normal WAN requirement between the Branch Office and the Main Office for ITG trunks or Virtual Trunks.

Procedure 46
Calculating unspecified conference traffic

When you lack specific information about conference traffic, use the following standard ratio of conference traffic to general traffic. In Nortel Networks PBX engineering, a network group of 32 loops is comprised of 28 traffic loops, 2 Conference loops, and 2 TDS loops. Using the ratio of 2:28, the conference traffic is about 7% (rounded up from 6.7%) of total traffic. Use the default value of 7% in place of specific information about conference traffic.

1   Calculate conference traffic:

Branch Office total traffic (TCCS) = # of Internet telephones x CCS for each telephone

Conference traffic (TCON) = TCCS x 0.07 CCS = TCCS x 0.07/36 Erlangs

2   Calculate WAN bandwidth:

For a G.729A/30 ms codec:

WAN kbps = TCON (erlangs) x 9 kbps

For a G.711/30 ms codec:

WAN kbps = TCON (erlangs) x 37 kbps

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

Procedure 47
Calculating known conference traffic

When a Branch Office is known or expected to make a significant number of conference calls, traffic statistics should be collected or estimated. Use the statistics to calculate WAN bandwidth requirements.

1   Calculate conference traffic:

Cc = conference calls/busy hour (a 6- or 3-way conference call is counted as 6 or 3 calls, respectively)

Ht = Average talk time (holding time) of conference in seconds (if you have no data, use 900 seconds as a default)

TCON = (3 x # 3-way conference calls + 6 x # 6-way conference calls + ...) x Ht/100 CCS = Total Cc x Ht/3600 erlangs

2   Calculate WAN bandwidth:

For a G.729A/30 ms codec:

WAN kbps = TCON (erlangs) x 9 kbps

For a G.711/30 ms codec:

WAN kbps = TCON (erlangs) x 37 kbps

Use other bandwidth data from Table 31 on if the codec and payload differ from those listed above.

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

With local conference MICB card

When a Branch Office conference is provided locally, there is no need to route conference traffic to the Main Office for service. A local conference

generates no WAN traffic, and does not require a WAN bandwidth calculation.

Procedure 48 covers only simple CallPilot voice messaging traffic for a WAN bandwidth calculation.

The engineering requirement for Multimedia Processing Units (MPU), such as CallPilot, depends on traffic type (for example, voice, fax, and speech-recognition) and service type (for example, enterprise networking, network message service). The MPU requirement calculations, which require several traffic tables to cover various Grade of Service practices, do not impact WAN calculation directly and are not presented here. Refer to *CallPilot Planning and Engineering Guide* (555-7101-101) for more information.

To leave a voice message for a user in a Branch Office, route the incoming call to the Main Office. Similarly, when a user retrieves the voice mail message, the connection takes place over the WAN to the Main Office. To leave or retrieve a message, the connection requires WAN bandwidth.

Procedure 48
Calculating Branch Office traffic, and WAN bandwidth without local messaging (CallPilot) capability

The following are default values of parameters to estimate CallPilot traffic. Specific traffic information about a site should be used if known.

1   Calculate Messaging traffic:

Average holding time of a voice message: 40 seconds (default recommended by the CallPilot NTP)

Voice Messaging Traffic (VMT) = Voice Messaging Calls x 40/100 CCS = Voice Messaging Calls x 40/3600 erlangs

If you have no information about messaging calls (leaving or retrieving a message), use the following approximation:

VMT = 10% x Total Branch Office traffic in CCS = 10% x Total Branch Office CCS traffic/36 (Erlangs)

2   Calculate WAN bandwidth:

For a G.729A/30 ms codec:

WAN kbps = VMT (erlangs) x 9 kbps

For a G.711/30 ms codec:

WAN kbps = VMT (erlangs) x 37 kbps

─────────────────   **End of Procedure**   ─────────────────

Appendix C: On-net dialing plan configuration examples

Contents

This section contains information on the following topics:

Introduction

This section contains configuration examples for the following on-net (or private) dialing plans:

- Coordinated Dialing Plan (CDP)

- Uniform Dialing Plan (UDP)

- Group Dialing Plan (GDP)

- Transferable DN (TNDN)

Coordinated Dialing Plan (CDP)

A sample CDP configuration is shown in Figure 81.

Figure 81
Coordinated Dialing Plan (CDP)
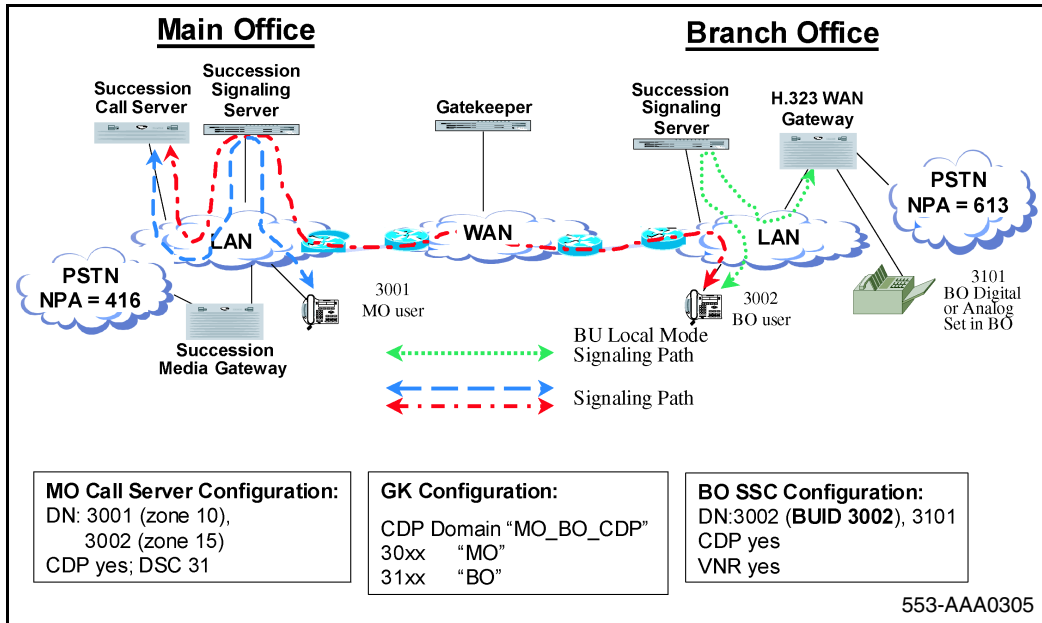
Call Scenarios

This section describes the following call scenarios, all based on Figure 81:

- From Main Office to Branch Office

- From Branch Office to Main Office

- When the Branch User telephone is in Local Mode

From Main Office to Branch Office

In this scenario, the following occurs:

- DN 3001 (in the Main Office) or 3002 (in the Branch Office) dials DN 3101 (a TDM telephone in the Branch Office).

- The Main Office Succession Call Server recognizes the first two digits "31" as a CDP DSC. It accesses the RLI appropriate for that steering code and uses the Virtual Trunk specified for that route.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. Since "31" is registered with the Branch Office, the Branch Office node IP address is returned.

- The Branch Office H.323 WAN Gateway terminates the incoming Virtual Trunk call to DN 3101.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to Main Office

In this scenario, the following occurs:

- DN 3101 (in the Branch Office) dials DN 3001 (or 3002 - both are registered with the Main Office).

- The Branch Office recognizes 3001 as a vacant number. Since VNR is enabled, the call is routed using the RLI defined for VNR, using the Virtual Trunk specified for that route.

- The Gatekeeper is queried for the destination node IP address with which to route the call over the Virtual Trunk. Since "30" is registered to the Main Office, the Main Office node IP address is returned.

- The Main Office Succession Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002).

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

When the Branch User telephone is in Local Mode

In this scenario, the following occurs:

- The Branch Office H.323 WAN Gateway handles the call processing of DN 3002.

- If there is no network outage or Succession Signaling Server/Gatekeeper failure, DN 3002 can call any telephone in the Branch Office and Main Office.

- However, DN 3002 cannot be reached from the Main Office by using CDP, because the DN is not registered at the Main Office as it would be in Normal Mode.

Configuration example

Main Office

To configure CDP at the Main Office, do the following:

1   Configure ESN Control Block for CDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
DLTN YES
```

2   Configure CDP Distant Steering Code

```
>LD 87
REQ NEW
CUST 0
FEAT CDP
TYPE DSC
DSC 31
FLEN 4
RLI 12
```

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

Gatekeeper configuration

To configure the Gatekeeper, do the following:

1   Create CDP Domain: "MO_BO_CDP".

2   Create H.323 endpoints: "MO", "BO".

3   Create Numbering Plan entries in CDP Domain:

    a   Add "31" for endpoint "BO".

    b   Add "30" for endpoint "MO".

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

Branch Office

To configure CDP at the Branch Office, do the following:

1   Configure ESN Control Block for CDP

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
DLTN YES
```

2   Configure Branch User

```
> LD 11
REQ: NEW
TYPE: i2004
TN 61 0
CUST 0
BUID 3002
```

Refer to Procedure 23 on and *IP Peer Networking* (553-3001-213) for more information.

Uniform Dialing Plan (UDP)

A sample Uniform Dialing Plan (UDP) (Access Code + LOC + DN) configuration is shown in Figure 82.

Figure 82
Uniform Dialing Plan (UDP)
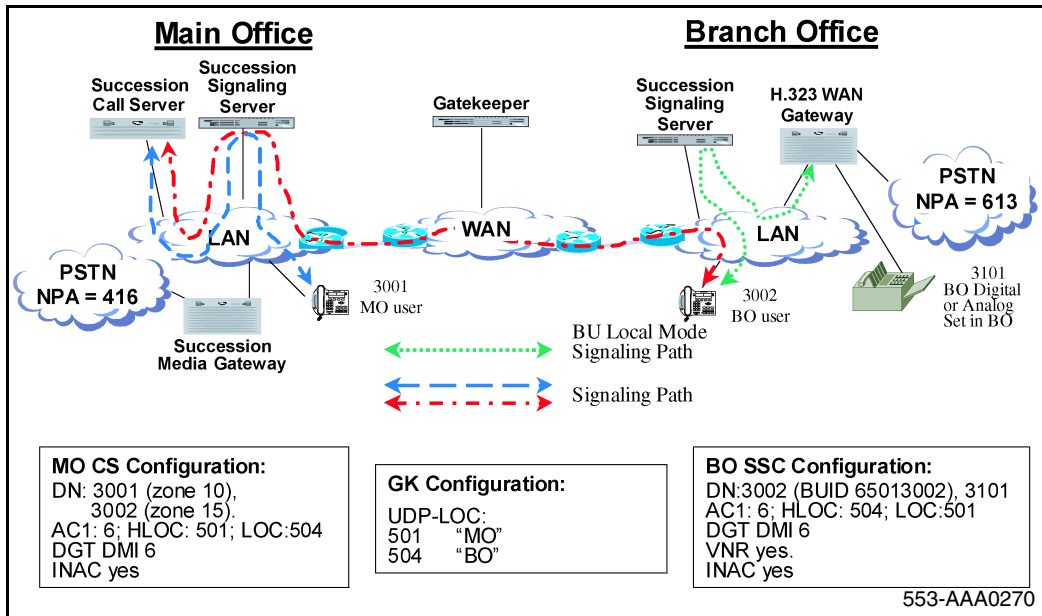
Call Scenarios

This section describes the following call scenarios, all based on Figure 82:

- From Main Office to Branch Office

- From Branch Office to Main Office

- When the Branch User telephone is in Local Mode

From Main Office to Branch Office

In this scenario, the following occurs:

* DN 3001 or 3002 dials DN "65043101" (a digital telephone in the Branch Office).

* The Main Office Succession Call Server recognizes the digit "6" as AC1 and the digits "504" as LOC. It accesses the associated RLI and uses the defined Virtual Route and Virtual Trunk.

* The Gatekeeper is queried for the destination node IP address with which to route the call over the Virtual Trunk. Since "504" is registered to the Branch Office, the Branch Office node IP address is returned for "ESN 504 3101".

* The Branch Office H.323 WAN Gateway terminates the incoming Virtual Trunk call to DN 3101, since "504" matches the HLOC of the Branch Office.

* The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to Main Office

In this scenario, the following occurs:

* DN 3101 dials DN "65013001" (or "65013002").

* The Branch Office H.323 WAN Gateway recognizes the first digit "6" as AC1. It accesses the RLI appropriate for the LOC of "501" and uses the Virtual Trunk specified for that route.

* The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. Since "501" is registered to the Main Office, the Main Office node IP address is returned.

* The Main Office Succession Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002) because "501" matches the HLOC of the Main Office.

* The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

When the Branch User telephone is in Local Mode

In this scenario, the following occurs:

- The Branch Office H.323 WAN Gateway handles the call processing of DN 3002.

- If there is no network outage or Succession Signaling Server/Gatekeeper failure, DN 3002 can still make and receive a call to or from any telephone in the Branch Office or Main Office using UDP.

- However, dialed in/out digits are different from those used in Normal Mode because the LOC is changed. For example:

  — DN 3001 can call DN 3002 by dialing "65043002", instead of the "3002" dialed in Normal Mode.

  — DN 3101 can call DN 3002 by dialing "3002", instead of the "65013002" dialed in Normal Mode.

  — DN 3002 can call DN 3001 by dialing "65013001", instead of the "3001" dialed in Normal Mode.

  — DN 3002 can call DN 3101 by dialing "3101", instead of the "65043101" dialed in Normal Mode.

Configuration example

Main Office

To configure UDP at the Main Office, do the following:

1   Configure ESN Control Block for UDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
AC1 6
```

2 Configure Digit Manipulation (DGT).

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3 Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 504
FLEN 7
RLI 12
LDN 0
```

4 Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 501
DMI 6
```

5 Configure HLOC in Customer Data Block.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 501
```

6   Configure Virtual Trunk route.

```
>LD16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE51
TKTP TIE
VTRK YES
ZONE 101
NODE 51
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

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

Gatekeeper configuration

To configure the Gatekeeper, do the following:

1   Create H.323 endpoints: "MO", "BO".

2   Create Numbering Plan entries.

   a   Choose type "UDP-LOC".

   b   Add "504" for endpoint "BO".

   c   Add "501" for endpoint "MO".

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

Branch Office

To configure UDP at the Branch Office, do the following:

1   Configure ESN Control Block for UDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
AC1 6
```

2   Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3   Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 501
FLEN 7
RLI 1
LDN 0
```

4   Configure UDP HLOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 504
DMI 6
```

5   Configure HLOC in Customer Data Block.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 504
```

6   Configure Branch User.

```
>LD 11
REQ: NEW
TYPE: i2004
TN 61 0
CUST 0
BUID 65013002
```

7   Configure Virtual Trunk Route

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE53
TKTP TIE
VTRK YES
ZONE 104
NODE 53
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

Refer to Procedure 23 on page 182 and *IP Peer Networking* (553-3001-213) for more information.

Group Dialing Plan (GDP)

A sample GDP configuration is shown in Figure 83.

Figure 83
Group Dialing Plan (GDP)
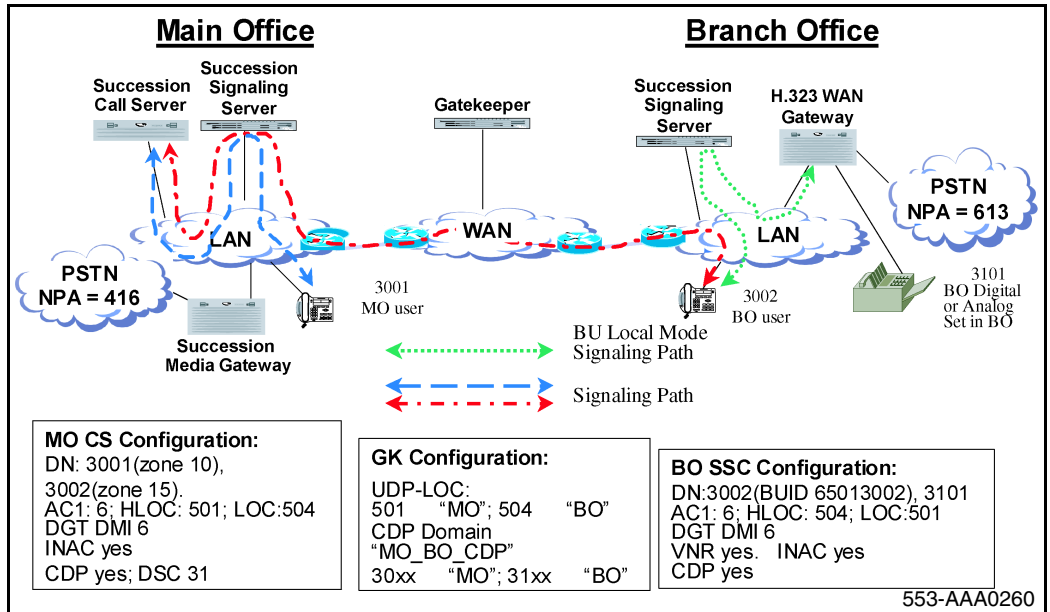
Call Scenarios

This section describes the following call scenarios, all based on Figure 83:

- From Main Office to Branch Office using CDP

- From Main Office to Branch Office using UDP-LOC

- From Branch Office to Main Office using CDP

- From Branch Office to Main Office using UDP-LOC

- Branch User telephone (DN 3002) is in Local Mode

From Main Office to Branch Office using CDP

In this scenario, the following occurs:

- DN 3001 or 3002 dials a number "3101".

- The Main Office Succession Call Server recognizes the digits "31" as a CDP DSC. The Succession Call Server accesses the RLI appropriate for that DSC and uses the Virtual Trunk specified for that route.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. Since "31" is registered to the Branch Office, the Branch Office node IP address is returned.

- The Branch Office H.323 WAN Gateway terminates the incoming Virtual Trunk call to DN 3101.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Main Office to Branch Office using UDP-LOC

In this scenario, the following occurs:

- DN 3001 or 3002 dials a number "65043101".

- The Main Office Succession Call Server recognizes the digit "6" as AC1. The Call Server accesses the RLI appropriate for the LOC "504" and uses the Virtual Trunk specified for that route.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. For "ESN 504 3101", the Branch Office node IP address is returned since "504" is registered to the Branch Office.

- The Branch Office H.323 WAN Gateway terminates the incoming Virtual Trunk call to DN 3101 since "504" matches the HLOC of the Branch Office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to Main Office using CDP

In this scenario, the following occurs:

- DN 3101 dials a number "3001"(or "3002").

- The Branch Office Succession System Controller recognizes the number as a vacant number. Since VNR is enabled, it uses the Virtual Trunk specified for that route according to the RLI defined for VNR.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. The Main Office IP address is returned since "30" is registered to the Main Office.

- The Main Office Succession Call Server routes the incoming Virtual Trunk call to DN 3001 (or 3002).

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to Main Office using UDP-LOC

In this scenario, the following occurs:

- DN 3101 dials a number "65013001"(or "65013002").

- The Branch Office H.323 WAN Gateway recognizes the first digit "6" as AC1. The Branch Office H.323 WAN Gateway accesses the RLI appropriate for LOC "501" and uses the Virtual Trunk specified for that route.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. The Main Office node IP address is returned since "501" is registered to the Main Office.

- The Main Office Succession Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002) since "501" matches the HLOC of the Main Office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

Branch User telephone (DN 3002) is in Local Mode

In this scenario, the following occurs:

- The Branch Office H.323 WAN Gateway handles the call processing of DN 3002.

- If there is no network outage or Succession Signaling Server/Gatekeeper failure, DN 3002 can still make or receive a call to or from any telephones in the Branch Office and Main Office using UDP. However, DN 3002 cannot be reached from the Main Office by using CDP. Refer to Local Mode scenarios for CDP () and UDP ().

- By having UDP and CDP working together, GDP provides the convenience of CDP and the flexibility of UDP.

Configuration example

Main Office

To configure GDP at the Main Office, do the following:

1   Configure ESN Control Block for CDP and AC1.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
AC1 6
DLTN YES
```

2   Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3   Configure Route List Block (RLB). For more information, refer to
Procedure 1 on .

```
>LD 86
REQ NEW
FEAT RLB
RLI 12
ENTR 0
ROUT 120
DMI 0
```

4   Configure CDP Distant Steering Code (DSC).

```
>LD 87
REQ NEW
CUST 0
FEAT CDP
TYPE DSC
DSC 31
FLEN 4
RLI 12
```

5   Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 504
FLEN 7
RLI 12
LDN 0
```

6   Configure UDP HLOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 501
DMI 6
```

7   Configure HLOC in CDP.

```
>LD 15
REQ: NEW
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 501
```

8   Configure Virtual Trunk Route.

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE51
TKTP TIE
VTRK YES
ZONE 101
NODE 51
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

Refer to Procedure 1 on page 82 in this document and *IP Peer Networking* (553-3001-213) for more information.

Gatekeeper configuration

Configure the following in the Gatekeeper:

- CDP domain: "MO_BO_CDP"

- H.323 endpoints: "MO", "BO"

- Numbering Plan entries

  — in CDP domain "MO_BO_CDP"

    – add "31" for endpoint "BO"

    – add "30" for endpoint "MO"

  — for type "UDP-LOC"

    – add "504" for endpoint "BO"

    – add "501" for endpoint "MO"

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

Branch Office

To configure GDP at the Branch Office, do the following:

1 Configure ESN Control Block for CDP and AC1.

```
>LD86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
AC1 6
DLTN YES
```

2 Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3   Configure UDP LOC.

```
>LD90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 501
FLEN 7
RLI 1
LDN 0
```

4   Configure UDP LOC.

```
>LD90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 504
DMI 6
```

5   Configure HLOC in CDP.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 504
```

6   Configure Branch User.

```
>LD 11
REQ: NEW
TYPE: i2004
TN 61 0
CUST 0
BUID 65013002
```

7   Configure Virtual Trunk Route.

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE53
TKTP TIE
VTRK YES
ZONE 104
NODE 53
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

Refer to Procedure 23 on in this document and *IP Peer Networking* (553-3001-213) for more information.

Transferable DN (TNDN)

Overview

Transferable DN allows a user to retain their DN when they move to a different office, whether the new "office" is a Branch Office or a full peer.

Original configuration (pre-transfer)

A sample of a TNDN configuration before the transfer is shown in Figure 84.

Figure 84
Transferable DN (TNDN) (pre-transfer)
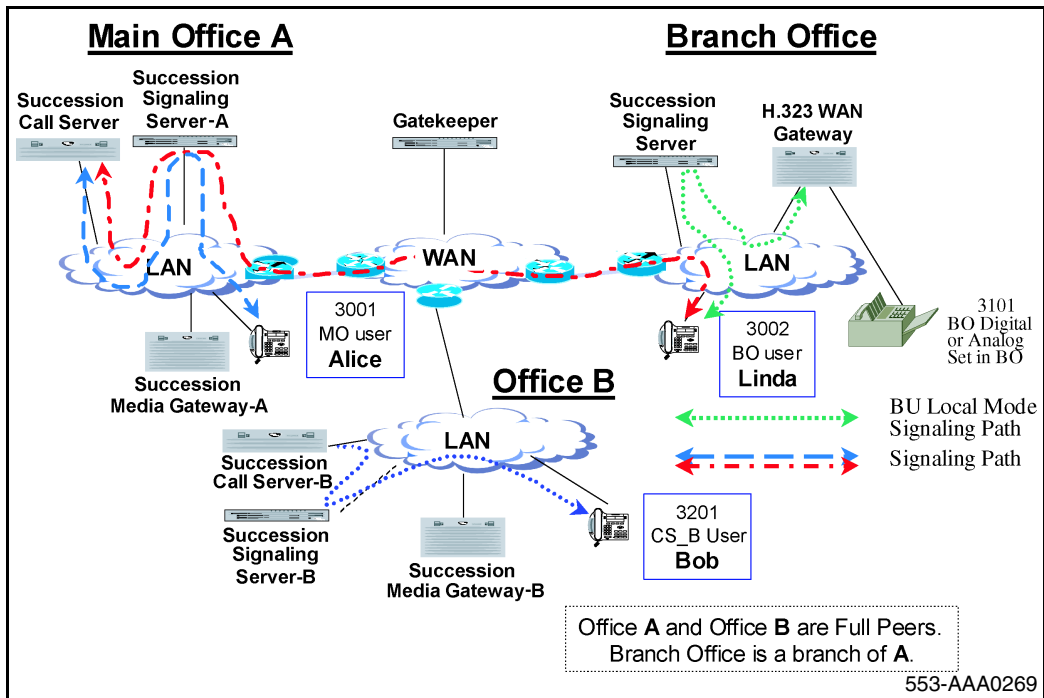
The components are configured as follows:

- Main Office Succession Call Server A

  — DN: 3001 (zone 10), 3002 (zone 15)

  — VNR: YES

- Call Server B

  — DN: 3201 (zone 20)

  — VNR: YES

- Branch Office SSC

  — DN: 3002 (zone 15, BUID 3002), 3101

  — VNR: YES

- Gatekeeper

  — CDP Domain "TNDN"

  — 3001 "MO"

  — 3002 "MO"

  — 3101 "BO"

  — 3201 "CS_B"

The Transfer

Alice is transferred from Main Office A to Office B. Bob is transferred from Office B to Branch Office A. Linda is transferred from the Branch Office to Main Office A. They all want to keep their existing telephone numbers.

New configuration (post-transfer)

The TNDN configuration after the transfer is shown in Figure 85 on .

Figure 85
Transferable DN (TNDN) (post-transfer)
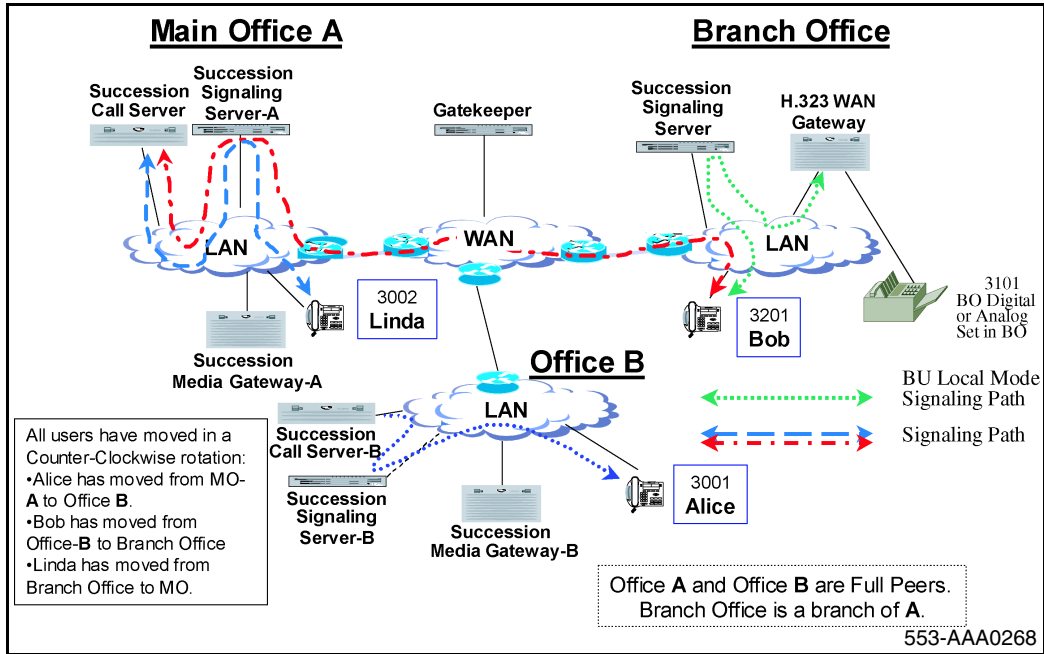
After the transfer, the components are configured as follows:

- Main Office Succession Call Server A

    — DN: 3002 (zone 10), 3201 (zone 15)

    — VNR: YES

- Call Server B

    — DN: 3001 (zone 20)

    — VNR: YES

- Branch Office SSC

    — DN: 3201 (zone 15, BUID 3201), 3101

    — VNR: YES

- Gatekeeper

    — CDP Domain "TNDN"

    — 3001 "CS_B"

    — 3002 "MO"

    — 3101 "BO"

    — 3201 "MO"

Call Scenario

A general example of a call scenario after the transfer has occurred, based on Figure 85 on , follows:

- Alice (at Office B) calls Bob (at the Branch Office) by dialing DN 3201.

- The CS of Alice's current office (Office B) recognizes 3201 as a vacant number. VNR is enabled, so according to the RLI defined for VNR, it uses the Virtual Trunk specified for that route.

- The Gatekeeper is queried for a destination node IP address with which to route the call over the Virtual Trunk. Since the Gatekeeper has been updated to reflect the current location of "3201", the corresponding node IP address of Main Office A is returned.

- The Destination Succession Call Server terminates the incoming Virtual Trunk call to DN 3201.

Configuration for TNDN

To configure TNDN, do the following:

1 Configure VNR. VNR must be enabled at all Succession Call Servers and Branch Office SSCs.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
VNR YES
RLI 12
```

2   Remove the TN at Office A when the user has moved from office A to office B.

```
>LD 11
REQ: OUT
TYPE: I2004
TN 61 0
```

3   Add the new TN at Office B, using a new telephone with the same DN.

```
>LD 11
REQ: NEW
TYPE: I2004
TN 62 8
```

4   Configure the GateKeeper as follows:

  a   CDP Domain: "TNDN".

  b   H323 endpoints: "MO", "BO", "CS_B"

  c   Numbering Plan Entry: In CDP domain "TNDN", keep the configuration updated to reflect the current location of the DNs.

Refer to "Numbering Plans" and "Managing the Gatekeeper" in *IP Peer Networking* (553-3001-213) for more information.

Appendix D: Off-net dialing plan configuration example

Contents

This section contains information on the following topics:

Introduction

This section contains an example of how to configure a dialing plan for a call from a Branch Office user in Normal Mode to the local PSTN. This example will walk you through the steps outlined in "Dialing plan configuration" on .

Call scenario

Figure 86 on shows the call scenario for the example.

Figure 86
Off-net dialing plan example - call scenario.
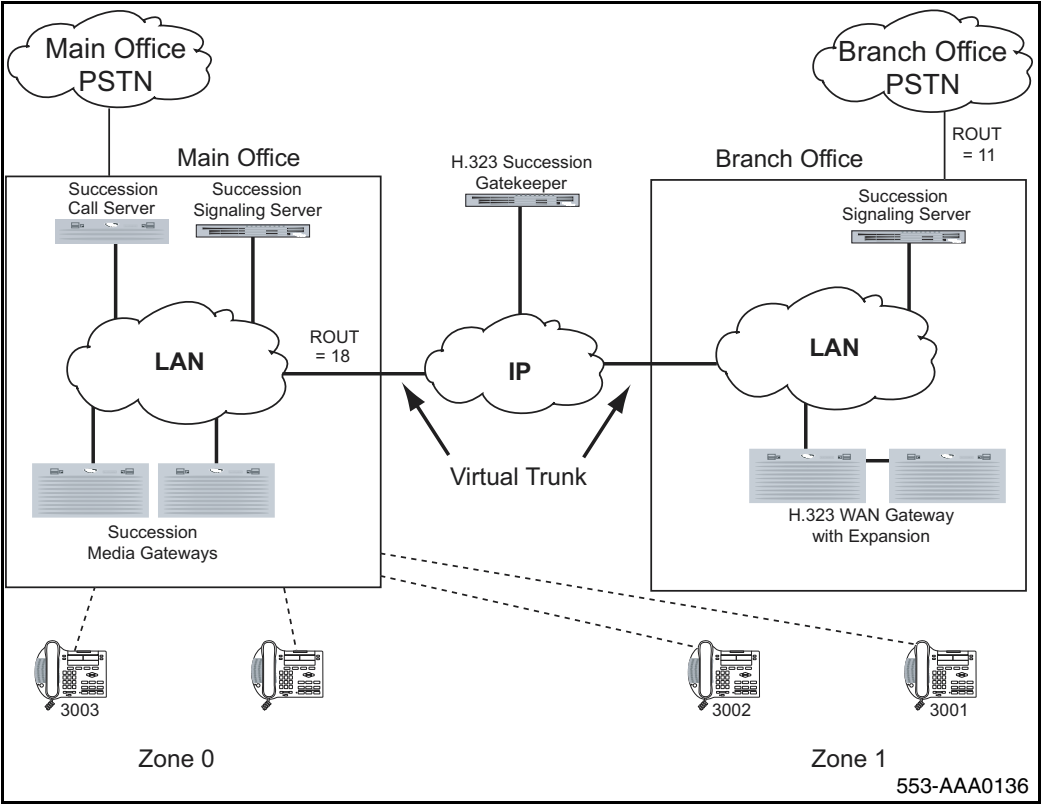
Provisioning

Main Office

At the Main Office Succession Call Server, the following is provisioned:

- AC1 = 1, and AC2 = 2

```
>LD86
REQ  PRT
CUST 0
FEAT ESN

MXLC 50
...
NCDP 4
AC1  1
AC2  2
DLTN YES
...
TGAR NO
```

- For Zone 1, ZACB = ALL, and ZDP = 101

```
>LD 117

=> PRT ZACB 1
```

```
 _____
|              |     |        Access Code Behavior      |
|     Zone     |State|----------------------------------|
|              |     |     |     |     | Dialed | New |
| #  DES       |     | DC1 | DC2 | DC3 |   AC   | AC  |
|--------------------------------------------------|
| 1 BRANCH_ZONE | ENL | 101 |     |     | ALL    | AC1 |
|--------------------------------------------------|
  Number of Zones configured = 2

=>
```

- DMI = 10, with DEL = 0 and CTYP = INTL

```
>LD86
REQ  PRT
CUST 0
FEAT DGT
DMI  10

DMI  10
DEL  0
CTYP INTL
```

- RLI = 1, with DMI = 10 and ROUT = 18, where this is the route number for the Virtual Trunk

```
>LD86
REQ  PRT
CUST 0
FEAT RLB
RLI  1

RLI  1
...
ROUT 18
...
DMI  10
...
```

- SPN = 101, with CTYP = INTL and RLI = 1
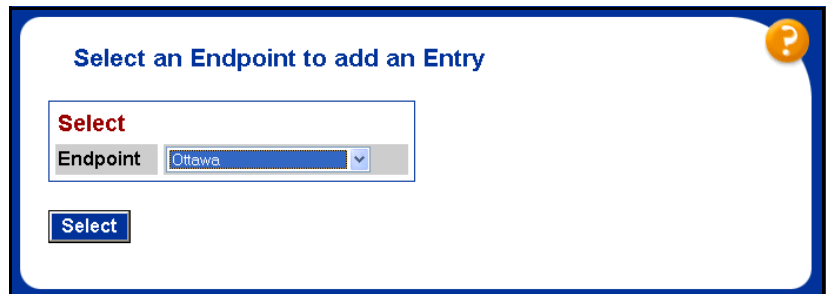
```
>LD90
REQ  PRT
CUST 0
FEAT NET
TRAN AC1
TYPE SPN
SPN  101

SPN  101
FLEN 0
ITOH NO
CLTP INTL
RLI  1
SDRR NONE
ITEI NONE
```

Gatekeeper

At the Gatekeeper, a Numbering Plan entry is provisioned that associates the SPN 101 with the Branch Office endpoint.

The Gatekeeper is provisioned using Element Manager, as shown in Figures 87 and 88.

Figure 87
Element Manager—Select an Endpoint to add an Entry

Figure 88
Element Manager—Add Entry

Branch Office

At the Branch Office Succession System Controller, the following is
provisioned:

- DMI = 12 with DEL = 3 to remove the ZDP digits added in the
  Main Office

```
>LD86
REQ  PRT
CUST 0
FEAT DGT
DMI  12

DMI  12
DEL  3
CTYP NCHG
```

- RLI = 4, with DMI = 12 and ROUT = 11, where this is the route number for the PSTN Trunk

  ```
  >LD86
  REQ  PRT
  CUST 0
  FEAT RLB
  RLI  4

  RLI  4
  ...
  ROUT 11
  ...
  DMI  12
  ...
  ```

- SPN = 101, with CTYP = INTL and RLI = 4

  ```
  >LD90
  REQ  PRT
  CUST 0
  FEAT NET
  TRAN AC1
  TYPE SPN
  SPN  101

  SPN  101
  FLEN 0
  ITOH NO
  CLTP INTL
  RLI  4
  SDRR NONE
  ITEI NONE
  ```

Call example

This section describes what happens when Branch Office User 3001 is in Normal Mode and dials "1 87654321", using the configuration provisioned in the previous section.

Main Office

At the Main Office Succession Call Server:

1 The call is recognized as originating from a Branch Office User in Zone 1.

2 Based on the ZACB property, the Succession Call Server recognizes that the call has been dialed with AC1, and that zone-based digit manipulation must be performed.

3 The ZDP digits are inserted after the Access Code, changing the digit string to "1 101 87654321".

4 The digits are translated by the ESN feature.

    a ESN recognizes that the number has been dialed using AC1, so "101" is a Special Number.

    b RLI "1" is associated with SPN "101", so route "18" and DMI "10" should be used.

    c DMI "10" sets the call type to International.

5 The call is routed to route "18", the Virtual Trunk. The digit string sent by the Succession Call Server is "101 87654321", as the Access Code is not sent out.

Gatekeeper

The Gatekeeper recognizes the digits "101" and call type of International, and identifies the endpoint as the Branch Office. It then routes the call to the Branch Office.

Branch Office

At the Branch Office Succession System Controller:

1 The call comes in on the Virtual Trunk. The INAC field in the Route Block of the Virtual Trunk is configured as "YES", so AC1 is inserted at the beginning of the digit string, changing the digit string to "1 101 87654321".

2 The digits are translated by the ESN feature.

    a ESN recognizes that the number begins with AC1, so "101" is a Special Number.

    b RLI "4" is associated with SPN "101", so route "11" and DMI "12" should be used.

    c DMI "12" deletes the first three digits of the digit string, and sets the call type to International.

3 The call is routed to route "11", the PSTN trunk.

List of terms

CDP

Coordinated Dialing Plan. Under the recommended Coordinated Dialing Plan, the Branch User ID can be an extension (for example, 4567). For more information about CDP, consult *Dialing Plans: Description* (553-3001-183).

data dump

A data dump, or Equipment Data Dump (EDD), is performed on the Succession Call Server to save the active database to backup and to copy the database to static memory on the pertinent Succession Media Gateway Succession System Controller.

DSP

Digital Signal Processing, which refers to manipulating analog information, such as sound or photographs that has been converted into a digital form. DSP also implies the use of a data compression technique.

When used as a noun, DSP stands for Digital Signaling Processor, a special type of coprocessor designed for performing the mathematics involved in DSP. Most DSPs are programmable, which means that they can be used for manipulating different types of information, including sound, images, and video.

ELAN

Embedded Local Area Network. This isolated section of the LAN connects the Succession Call Server, Succession Signaling Server, Succession Media Gateway SSC, Voice Gateway Media Card, and OTM for system communication purposes.

gateway

In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, enable users on different e-mail systems to exchange messages.

H.323

A standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks. In theory, H.323 enables users to participate in the same conference even though they are using different videoconferencing applications. Although most videoconferencing vendors have announced that their products conform to H.323, it is too early to say whether such adherence actually results in interoperability.

IP

Abbreviation of **Internet Protocol**, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It enables you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

ITG-P

The ITG-Pentium card has a Pentium processor and 24 Digital Signaling Processor channels. It occupies two slots in an H.323 WAN Gateway or H.323 WAN Gateway Expansion chassis. It provides the same functionality as the Succession Media Card when equipped with the IP Line 3.1 application. See Voice gateway.

Layer 2 switching

Packets are forwarded according to the destination's MAC address. The switch automatically determines which switch port must be used to send the packet, according to the destination's MAC address. The MAC address location was determined from incoming packets from that MAC address received on that port.

Layer 3 switching

Packet traffic is grouped according to the source and destination addresses. The first packet in a flow is routed by a software-based algorithm. Subsequent packets with the same source and destination addresses are switched according to the destination's MAC address (hardware mechanism). This is similar to multi-layer routing and routers with hardware assist.

NAT

Network Address Translation. It is defined as an internet standard that lets a LAN use both internal and external IP addresses. This protects an internal IP address from being accessed from outside. NAT translates the internal IP addresses to unique IP addresses before sending out packets. NAT is practical when only a few users in a domain need to communicate outside of the domain at the same time.

NCS

Short for Network Connection Server, which is an H.323 Gatekeeper. It provides standard H.323 Gatekeeper functionality, as well as support for Succession 3.0 Branch Office and Virtual Office features.

PSTN

Short for Public Switched Telephone Network, which refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks based on digital technologies, such as ISDN and FDDI.

Telephone service carried by the PSTN is often called plain old telephone service (POTS).

QoS

Short for **Quality of Service**, a networking term that specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies, such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This enables ATM providers to guarantee to their customers that end-to-end latency does not exceed a specified level.

There are several methods to provide QoS, as follows:

• high bandwidth

- packet classification

- DiffServ

- IP fragmentation

- traffic shaping

- use of the platforms queuing mechanisms

routing

The process of selecting the correct path for packets transmitted between IP networks by using software-based algorithms. Each packet is processed by the algorithm to determine its destination.

TDM

Short for Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel.

Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

TLAN

Telephony Local Area Network. This isolated section of the network connects the Voice Gateway Media Cards, the Signaling Server, and the Internet Telephones for telephony communication purposes.

TPS

Internet Telephone Terminal Proxy Server. This server controls the connection of Internet Telephones. It resides on the Signaling Server with an emergency backup on the Voice Gateway Media Card.

UDP

Uniform Dialing Plan. Each location within the network is assigned a Location Code, and each telephone has a Directory Number that is unique within the network. Under the Uniform Dialing Plan (UDP), the Branch User ID is the user's Main Office Directory Number (DN) with the Access Code (for example, 6 343-5555). For details of other Numbering Plan options, see *Succession 1000 System: Overview* (553-3031-010).

Voice gateway

The voice gateway application is used any time an IP and TDM device are connected together. The cards are equipped with DSPs to perform media transcoding between IP voice packets and TDM-based devices. The Succession Media Cards also provide echo cancellation and compression and decompression of voice streams. The voice gateway software can run on a 32-port Succession Media Card or the 24-port TG-P card. Within the Branch Office, both of these cards register the voice channels to the Branch Office Succession System Controller when they are configured.

WAN

Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Succession 1000, Succession 1000M
Branch Office

NORTEL
NETWORKS™