# Converging the Data Network with VoIP Fundamentals
# Nortel Communication Server 1000

7.0
NN43001-260, 04.08
April 2012

© 2012 Avaya Inc.

All Rights Reserved.

**Notice**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third-party components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

**Preventing Toll Fraud**

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

**Avaya Toll Fraud Intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Trademarks**

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

**Contact Avaya Support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

## Contents


**Chapter 1: New in this Release** ..... 11
- Navigation ..... 11
  - Features ..... 11
  - Other changes ..... 11

**Chapter 2: How to get help** ..... 15
- Getting help from the Nortel Web site ..... 15
- Getting help over the telephone from a Nortel Solutions Center ..... 15
- Getting help from a specialist by using an Express Routing Code ..... 16
- Getting help through a Nortel distributor or reseller ..... 16

**Chapter 3: Introduction** ..... 17
- Navigation ..... 17
- Subject ..... 17
- Note on legacy products and releases ..... 17
- Applicable systems ..... 18
- System migration ..... 18
- Intended audience ..... 18
- Conventions ..... 19
- Related information ..... 20
- Technical documents ..... 20
- Online ..... 21
- CD-ROM ..... 21

**Chapter 4: Overview** ..... 23
- Navigation ..... 23
- Network convergence ..... 23
- Voice applications ..... 24
- Quality of Service ..... 25
- Network Bandwidth Management ..... 25
- Adaptive Network Bandwidth Management ..... 27
- Tandem Bandwidth Management ..... 27
- Network Wide Virtual Office ..... 27
- Abbreviated Dialing ..... 28
- Zones ..... 28
- SIP Line Service ..... 28
- Redundancy operation ..... 29
- Survivable SIP Media Gateway Data Replication ..... 29
- Supported codecs ..... 29
- Codec selection ..... 30
- Codec payload sizes considerations ..... 30
- Zone Based Dialing plan ..... 30
- New prompts and changed overlays ..... 30
- Meridian Customer Defined Network Alternate Routing and Vacant Number Routing ..... 31
- Alternate Call Routing for Network Bandwidth Management ..... 33
- Quality of Service versus Bandwidth Management ..... 33
- Security ..... 33

Security domain considerations and guidelines ... 34
Secure Transport Enhancements ... 34
SSH File Transport Protocol ... 35
UNIStim Security with DTLS ... 35
Network design and implementation ... 35
Network performance measurement and monitoring ... 36
Available tools ... 37
**Chapter 5: Planning and engineering ... 39**
Navigation ... 39
Quality of Service ... 40
QoS mechanism ... 40
Traffic mix ... 41
TCP traffic behavior ... 41
QoS problem locations ... 42
Campus networks ... 42
Wide area networks ... 43
The QoS process ... 43
Classification ... 43
Marking ... 44
Queueing ... 44
WAN QoS mechanisms ... 46
Bandwidth demand ... 46
Fragmentation and interleaving ... 47
Traffic shaping ... 49
RTP header compression ... 50
PPP QoS ... 50
Frame Relay QoS ... 51
ATM QoS ... 51
Layer 2 (Ethernet) QoS ... 51
MAC address ... 51
IEEE 802.1Q ... 52
Port prioritization ... 54
Layer 3 QoS ... 54
IP address classification ... 54
DiffServ for VoIP ... 55
Trust configuration ... 56
Voice signaling and media DSCPs ... 56
Setting DSCP values ... 57
Element Manager QoS configuration ... 59
Layer 4 (TCP/IP) classification ... 60
Port number classification ... 61
Protocol ID classification ... 61
Communication Server 1000 and Meridian 1 ports ... 61
Policy management ... 61
ENMS Policy Services ... 61
Codec selection ... 62
Protocols in use ... 62

Routing protocols ... 63
LAN protocols ... 63
WAN protocols ... 63
Convergence ... 63
Mixing protocols ... 63
Security and QoS ... 64
IP network best practices ... 64
Fallback to PSTN ... 64
Best IP network engineering practices for IP Telephony ... 65
Considerations for using IP Trunk to achieve QoS fallback to PSTN ... 66
Alternate circuit-switched routing ... 66
Bandwidth Management ... 73
VoIP Bandwidth Management zones ... 73
Nodal Bandwidth Management ... 76
VPNI and Zone numbers ... 76
Relationship between zones and subnets ... 77
Adaptive Network Bandwidth Management ... 78
VoIP network voice engineering considerations ... 84
Tandem Bandwidth Management ... 88
Codec negotiation ... 89
SIP Offer/Answer model ... 93
Best Bandwidth codec selection algorithm ... 94
Bandwidth Management parameters ... 95
Zones ... 95
Zone Assignments ... 96
Zone based digit manipulation ... 98
CLID composition ... 99
CLID verification ... 99
Vacant Number Routing ... 99
Time of Day ... 100
MG 1000B IP Phone calls to a local PSTN ... 100
Special Number (SPN) for emergency services ... 101
Emergency Services ... 101
LAN/WAN bandwidth requirements ... 101
Calculation tables ... 102
Branch office conference engineering ... 104
Dialing plan ... 106
Prerequisites to configure the dialing plan ... 106
Configuration ... 106
Branch office dialing plan ... 107
Zone parameters ... 108
Abbreviated Dialing ... 108
Abbreviated dialing ... 109
Bandwidth and data network switch efficiency ... 110
Network design assessment ... 110
Network modeling ... 111
Link speeds ... 116

Link types ... 117
Link utilization assessment ... 118
Traffic flows in the network ... 120
Service level agreements ... 121
Network planning ... 122
Network Performance Measurement ... 122
Performance criteria ... 123
Network availability ... 126
Media Security ... 126
Determine QoS expectations ... 127
G.729AB codec ... 129
G.711 codec ... 130
G.723 codec ... 131
Bandwidth ... 132
Delay ... 143
Jitter ... 152
Packet loss ... 155
Network delay and packet loss evaluation example ... 158
Estimate voice quality ... 159
LAN design ... 164
CS 1000 configurations ... 165
Server LAN design ... 173
Redundant LAN design ... 188
Zone Based Dialing plan ... 193
Feature dependencies and restrictions ... 194
LD 10, 11 ... 194
LD 12 ... 194
LD 15 ... 194
LD 20 ... 194
LD 21 ... 195
LD 22 ... 195
LD 43 ... 195
LD 81 ... 195
LD 83 ... 195
LD 117 ... 195
Feature impact on planning and engineering tasks ... 196
Vacant Number Routing feature ... 196
Dialing plan ... 196
On-net dialing plan options ... 197
Off-net dialing plan ... 197
Routing ... 198
SIP/H.323 zones ... 198
Distributed Media Gateway 1000E ... 199
Survivable SIP Media Gateway Data Replication ... 200
DHCP configuration ... 200
IP Phones ... 200
Configuring the DHCP server to support full DHCP mode ... 202

The VoIP network operation ... 209
Element Manager ... 209
Network monitoring ... 210
Determine VoIP QoS objectives ... 210
Intranet QoS monitoring ... 211
ITG Operational Measurements ... 212
OM report description ... 212
User feedback ... 213
QoS monitoring and reporting tools ... 213
Network Diagnostic Utilities ... 214
Ping and traceroute ... 214
IP Networking statistics ... 215
Ethernet statistics ... 215
RUDP statistics ... 215
Real-Time Transport Protocol statistics ... 215
DHCP ... 215
Voice quality monitoring ... 220
IP Phones voice quality monitoring ... 221
Voice quality alarms ... 222
Configure voice quality metric thresholds ... 223
Configure voice quality sampling (polling) ... 223
Configure and print zone alarm notification levels ... 223
Network Management ... 225
**Chapter 6: Configuration ... 227**
Navigation ... 227
Communications Server 1000 configuration for network requirements ... 228
Small configuration ... 228
Configuring Quality of Service in Element Manager ... 228
Bandwidth Management ... 229
Configuration rules ... 230
Configuring Bandwidth Management ... 230
Maintenance commands ... 231
Configuring a Bandwidth Management zone ... 232
Configuring Dialing Plan ... 236
Configuring the branch office dialing plan using 1000 Element Manager ... 247
Testing PSTN access using an SRG or MG 1000B IP Phone ... 249
Troubleshooting ... 249
Zone Based Dialing ... 249
LD 15 ... 250
Configuring numbering zone and numbering zone based parameters ... 250
Meridian Customer Defined Network Alternate Routing and Vacant Number Routing ... 252
Meridian Customer Defined Network Alternate Routing configuration ... 252
Vacant Number Routing configuration ... 252
Codec configuration ... 252
G.729 VAD negotiation via SIP ... 252
Configuring codecs ... 253
Adaptive Network Bandwidth Management configuration ... 253

Configuration rules ... 253
Advanced configuration notes ... 254
Provisioning for Tandem Bandwidth Management ... 254
Bandwidth Management support for Network Wide Virtual Office ... 259
Prerequisites ... 259
Operating parameters ... 260
Feature Packaging ... 260
Feature Implementation ... 260
Feature Interactions ... 262
Operating parameters ... 263
Alternate Call Routing ... 264
Insufficient bandwidth ... 265
Unregistered resources ... 266
LD 117 ... 267
Dialing plan ... 267
Feature interactions ... 268
Feature packaging ... 269
ALTPrefix ... 269
Alternate Call Routing for Network Bandwidth Management scenarios ... 270
Feature implementation using Command Line Interface ... 280
Zone configuration ... 281
Zone Basic Property and Bandwidth Management ... 281
Adaptive Network Bandwidth Management and CAC ... 282
Alternate Routing for Calls between IP stations ... 288
Branch Office Dialing Plan and Access Codes ... 290
Branch Office Time Difference and Daylight Saving Time Property ... 291
The MG 1000B zone configuration ... 292
Abbreviated dialing ... 298
Print branch office zone information ... 303
Enable/disable branch office zone features ... 303
View status of branch office zone at main office Call Server ... 304
Change/print Proactive Voice Quality notification levels ... 304
Print PVQ statistics ... 305
Diagnostics ... 305
Maintenance ... 309
SIP Line service ... 317
**Appendix A: Subnet mask conversion ... 319**
Subnet mask conversion from CIDR to dotted decimal format ... 319
**Appendix B: Port number tables ... 321**
Navigation ... 321
Ephemeral ports ... 322
Linux considerations ... 322
VXWorks Call Server port numbers ... 322
Voice Gateway Media Card port numbers ... 328
Media Gateway Controller port numbers ... 337
Co-resident (Linux) Call Server port numbers ... 344
Signaling Server port numbers ... 351

SIP Lines Gateway Port Numbers ... 358
Element Manager Port Numbers ... 364
Network Routing Service Port Numbers ... 369
Unified Communications Manager Port Numbers ... 374
Telephony Manager port numbers ... 379
IP Phone port numbers ... 381
Remote Office port numbers ... 381
CallPilot port numbers ... 382
Application Gateway (AG) 1000 port numbers ... 385
Contact Center port numbers ... 386
TLAN subnet stateless packet filtering ... 387
TLAN subnet stateful packet filtering ... 388
ELAN subnet packet filtering ... 390
**Appendix C: DHCP supplemental information ... 391**
Navigation ... 391
Introduction to DHCP ... 392
DHCP messages ... 392
DHCP message format ... 392
DHCP message exchange ... 393
DHCP options ... 394
Vendor Specific/Encapsulated option ... 394
Site Specific option ... 394
IP acquisition sequence ... 395
Case 1 ... 395
Case 2 ... 396
Case 3 ... 396
Multiple DHCPOFFER messages ... 397
IP Phone support for DHCP ... 398
Full DHCP ... 398
Partial DHCP ... 402
DHCP Auto Discovery ... 402
**Appendix D: Setup and configuration of DHCP servers ... 405**
Navigation ... 405
Install a Windows NT 4 or Windows 2000 server ... 405
Configure a Windows NT 4 server with DHCP ... 405
Configure a Windows 2000 server with DHCP ... 408
Install ISC DHCP Server ... 413
Configure ISC DHCP Server ... 413
Configure ISC DHCP to work with the IP Phones ... 413
Install and configure a Solaris 2 server ... 416
**Appendix E: Change CS 1000 IP addresses ... 419**
**Index ... 423**

# Chapter 1: New in this Release

The following sections detail what's new in *Converging the Data Network with VoIP Fundamentals, NN43001-260* for Nortel Communication Server 1000 Release 7.0.

## Navigation


- Features on page 11
- Other changes on page 11


## Features

### Network Bandwidth Zone

Communication Server 1000 Release 7.0 provides an increase in the number of bandwidth management zones. The range of allowable bandwidth management zone values is increased to 0–8000.

### RLI and DMI enhancement

For Communication Server Release 7.0, the range of allowable Route List Index (RLI) and Digit Manipulation Index (DMI) values is increased from 0–999 to 0–1999. For more information about RLI and DMI values, see Table 54: LD 86 – Configure the Digit Manipulation Index at the main office on page 239.

## Other changes

There are no other changes in this release.

### Revision history

April 2012 Standard 04.08. This document is up-issued to include information about Controlled Directory Numbers and Alternate Route Calling.

March 2012 Standard 04.07. This document is up-issued to include updates to expand instructions on changing the Call Server IP address.

June 2011 Standard 04.06. This document is up-issued to include updates to security domain content.

April 2011 Standard 04.05. This document is up-issued to include an Avaya support link in Appendix B.

March 2011 Standard 04.04. This document is up-issued to correct the MGC DSP daughterboard port ranges.

August 2010 Standard 04.03. This document is up-issued to update the supported MGC DSP daughterboard port ranges.

June 2010 Standard 04.02. This document is up-issued to support Nortel Communication Server 1000 Release 7.0.

June 2010 Standard 04.01. This document is up-issued to support Nortel Communication Server 1000 Release 7.0.

March 2010 Standard 03.13. This document is up-issued for changes in technical content.

February 2010 Standard 03.12. This document is up-issued for changes in technical content. Change CS 1000 IP addresses on page 419 is revised to include formatting changes.

January 2010 Standard 03.11. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

January 2010 Standard 03.10. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

June 2009 Standard 03.09. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

June 2009 Standard 03.08. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

May 2009 Standard 03.07. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

May 2009 Standard 03.06. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.

July 2008 Standard 02.04. This document is up-issued to address a CR.

July 2008 Standard 02.03. This document is up-issued to consolidate Network Bandwidth Management content for Communication Server 1000 Release 5.5. A screen capture for the Edit window in Element Manager was also updated to address a CR.

February 2008 Standard 02.02. This document is up-issued for changes in technical content. References to non-supported systems are removed and updated screen captures are added for release 5.5.

December 2007 Standard 02.01. This document is up-issued to support Nortel Communication Server 1000 Release 5.5. References to non-supported systems are removed and updated screen captures are added for release 5.5.

January 2008 Standard 01.05. This document is up-issued for changes in technical content, including new images and revised port number tables.

November 2007 Standard 1.04. This document is up-issued to reflect changes in the QoS alarms that are listed in Table 48: Voice quality threshold alarm notification levels on page 224.

September 2007 Standard 01.03. This document is up-issued to add Media Gateway Controller (MGC) technical content and to remove references to systems not supported in release 5.0.

June 2007 Standard 01.02. This document is up-issued to reflect changes in technical content for CR Q01669176. A note regarding Secure Real-Time Transport Protocol (SRTP) bandwidth considerations is added to the section.

May 2007 Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0. This document is renamed Converging the Data Network with VoIP Fundamentals (NN43001-260) and contains information previously contained in the following legacy document, now retired: Converging the Data Network with VoIP (553-3001-160).

November 2006 Standard 6.00. This document is up-issued for CR Q01456113, adding explanations and examples of graphical and text XAS configuration strings.

July 2006 Standard 5.00. This document is up-issued for changes in technical content.

March 2006 Standard 4.00. This document is up-issued for CR Q0128628, clarifying Network Diagnostic Utilities CLI commands.

August 2005 Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.

September 2004 Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

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 contained in the following legacy document, now retired: Data Networking Guidelines (553-3023-103).

# Chapter 2: How to get help

This chapter explains how to get help for Nortel products and services.

## Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site: http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

## Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

http://www.nortel.com/callus

## Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

## Getting help through a Nortel distributor or reseller

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

# Chapter 3: Introduction

This document contains the following topics:

## Navigation


- Overview on page 23
- Planning and engineering on page 39
- Configuration on page 227
- Subnet mask conversion on page 319
- Port number tables on page 321
- DHCP supplemental information on page 391
- Setup and configuration of DHCP servers on page 405


## Subject

This document describes the elements and processes necessary to build a converged multimedia network with Nortel Communications Server 1000.

## Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 software. For more information about legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page:

http://www.avaya.com

# Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

# System migration

When particular Meridian 1 systems are upgraded to run Communication Server 1000 software and configured to include a Signaling Server, they become Communication Server 1000 systems.Table 1: Meridian 1 systems to CS 1000 systems on page 18 lists each Meridian 1 system that supports an upgrade path to a Communication Server 1000 system.

**Table 1: Meridian 1 systems to CS 1000 systems**

| This Meridian 1 system | Maps to Communication Server 1000 system |
|---|---|
| Meridian 1 PBX 11C Chassis | Communication Server 1000E |
| Meridian 1 PBX 11C Cabinet | Communication Server 1000E |
| Meridian 1 PBX 61C | Communication Server 1000M Single Group |
| Meridian 1 PBX 81C | Communication Server 1000M Multi Group |

For more information, see *Communication Server 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*, *Communication Server 1000E Upgrades , NN43041-458*, and *Communication Server 1000E Upgrade — Hardware Upgrade Procedures , NN43041-464*.

# Intended audience

This document is intended for individuals responsible for administering Communication Server 1000 and Meridian 1 systems.

# Conventions

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

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)
- Meridian 1

Unless specifically stated otherwise, the term Element Manager refers to the Communication Server 1000 Element Manager.

In this document, the following Chassis or Cabinets are referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Chassis Expander (NTDK92)
- Option 11C Cabinet (NTAK11)
- MG 1000E Chassis (NTDU14) and Expansion Chassis (NTDU15)
- Media Gateway 1010 (MG 1010) (NTC310)
- IPE module (NT8D37) with MG XPEC card (NTDW20)

In this document, the following hardware is referred to as Gateway Controller:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)

**Note:**

Gateway Controllers are based on MGC architecture and use a common MGC loadware. MGC information applies to all Gateway Controllers unless otherwise indicated.

In this document, the following hardware is referred to generically as Server:

- Call Processor Pentium IV (CP PIV)
- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
    - IBM x306m server (COTS1)
    - HP DL320 G4 server (COTS1)
    - IBM x3350 server (COTS2)

- Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

Co-res CS and SS is not supported on COTS1 servers. You can deploy a COTS1 server as a stand-alone Signaling Server.

The following table shows CS 1000 Release 7.0 supported roles for hardware platforms.

**Table 2: Hardware platform supported roles**

| Hardware platform | VxWorks Server | Linux Server | Co-res CS and SS | Gateway Controller |
|---|---|---|---|---|
| CP PIV | yes | no | no | no |
| CP PM | yes | yes | yes | no |
| CP DC | no | yes | yes | no |
| CP MG | no | no | yes (see note) | yes (see note) |
| MGC | no | no | no | yes |
| MG XPEC | no | no | no | yes |
| COTS1 | no | yes | no | no |
| COTS2 | no | yes | yes | no |

**Note:**

The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying slot 0 in a Media Gateway.

# Related information

This section lists information sources that are relevant to this document.

# Technical documents

This document references the following technical documents:

- *Features and Services Fundamentals, NN43001-106*
- *Unified Communications Management Common Services Fundamentals, NN43001-116*
- *IP Peer Networking Installation and Commissioning, NN43001-313*

- *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Hospitality Features Fundamentals, NN43001-553*

## Online

To access Nortel documentation online, click the Technical Documentation link under Support & Training on the Nortel Web site:

http://www.avaya.com

## CD-ROM

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

# Chapter 4: Overview

This chapter provides a brief technical description of all the components associated with converging the data and voice network.

## Navigation


- Network convergence on page 23
- Quality of Service on page 25
- Network Bandwidth Management on page 25
- Abbreviated Dialing on page 28
- Zones on page 28
- SIP Line Service on page 28
- Zone Based Dialing plan on page 30
- Meridian Customer Defined Network Alternate Routing and Vacant Number Routing on page 31
- Alternate Call Routing for Network Bandwidth Management on page 33
- Quality of Service versus Bandwidth Management on page 33
- Security on page 33
- Network design and implementation on page 35
- Network performance measurement and monitoring on page 36
- Available tools on page 37


## Network convergence

Network convergence transports all services over the same network structure. Previously, different types of applications used separate dedicated networks, such as voice, video, and data. Today, you can merge many of these applications into a single network to reduce operating costs and to increase ease of operation.

A traditional enterprise can have the following network types:

- private Time Division Multiplexing (TDM)-based voice network
- IP network to the Internet
- Integrated Services Digital Network (ISDN) for video conferencing
- Systems Network Architecture (SNA) an IBM computer network architecture
- multiprotocol network, including varied protocol types, such as Internetwork Packet Exchange (IPX)

Many enterprises use converged networks to achieve cost and operational efficiency. A converged network mixes different types of traffic, each with various requirements, that creates difficulties that you must address. When applications have dedicated networks, Quality of Service (QoS) technology plays a small role. Dedicated network traffic is similar in behavior, and the networks are fine-tuned to achieve the required application behavior.

For example, the expectation for interactive voice is low packet loss and a minimal, fixed amount of delay. Data is sent in a steady stream, with samples transmitted at fixed time intervals. This performance is obtained on a circuit-switched network. A best-effort data network includes varying amounts of packet loss and variable delay usually caused by network congestion. A packet-based data network usually has the opposite requirements of a voice application.

Implementing QoS mechanisms can address the issue described above.

# Voice applications

Voice applications originate on Public Switched Telephone Networks (PSTNs) and use circuit switching in the form of Time Division Multiplexing (TDM).

TDM is engineered with very specific, predetermined behaviors to support real-time voice conversations. On a TDM network, bandwidth is guaranteed available for any voice call; therefore voice traffic experiences a low, fixed amount of delay with essentially no loss.

IP networks do not guarantee available bandwidth for voice calls unless QoS mechanisms are used to restrict delay and data loss to maintain acceptable user quality.

If a voice application is sent over a best-effort IP network, the following can occur:

- Voice packets experience variable, unpredictable amounts of delay.
- Voice packets drop when the network becomes congested.
- The network can reorder voice packets if the packets arrive out of sequence.

You can apply QoS techniques to properly-engineered networks to support VoIP with acceptable, consistent, and predictable voice quality.

# Quality of Service

IP networks are inherently best-effort networks. They treat all packets in the same manner. A best-effort network has no specified parameters. It does not guarantee how fast data transmits over a network, and has no assurances that the data is delivered.

Quality of Service (QoS) mechanisms guarantee that the network treats certain packets in a specified manner.

QoS mechanisms refer to packet tagging mechanisms and network architecture decisions on the TCP/IP network to expedite packet forwarding and delivery.

QoS is especially important for low-speed links, where the usual amount of available bandwidth is only several hundred kbit/s. For example, data traffic could easily use all of the bandwidth available on a link, thereby causing voice quality problems. QoS mechanisms can guarantee that network bandwidth remains available for voice traffic.

End-to-end QoS is required for IP Telephony applications to achieve good voice quality and is achieved by ensuring that the different parts of the network apply consistent treatment to the telephony packets.

Many of the available QoS mechanisms are described in QoS mechanism on page 40.

# Network Bandwidth Management

Communication Server 1000 supports Network Bandwidth Management on a network-wide basis, so that voice quality can be managed between multiple Call Servers.

With the Network Bandwidth Management feature, you can configure bandwidth zones on a network basis, so that codec selection and bandwidth allocation software can identify whether Internet Telephones or gateways are physically collocated (in the same bandwidth zone) even though controlled by different Call Servers.

Adaptive Network Bandwidth Management is an enhancement of Bandwidth Management in which Quality of Service (QoS) metrics automatically lower available bandwidth.

Bandwidth management provides a means of controlling the amount of Voice over IP (VoIP) traffic in an IP network. Call Servers in the network keep track of the various amounts of VoIP traffic and provide treatment to VoIP calls. Treatment may consist of blocking new calls (Call Admission Control) or rerouting them if the required bandwidth is not available. For example, when a caller attempts to make a VoIP call and the network reaches bandwidth limit, the system blocks or reroutes the call.

Bandwidth Management also allows for a particular codec to be selected depending on the type of call — a local call within the Local Area Network (LAN) or a remote call across a Wide Area Network (WAN).

Bandwidth Management is considered a QoS mechanism because it provides a means of guaranteeing that VoIP traffic does not use more network bandwidth than available.

Bandwidth Management Zones simplify VoIP network voice engineering. Bandwidth Management Zones allow an administrator to simply enter the amount of bandwidth available for voice on the IP network, instead of detailed voice CCS calculations across a particular link.

For example, if you use a CCS-type approach to VoIP network voice engineering, an administrator must calculate the maximum CCS expected between sites A to B, A to C, and B to C, and subsequently engineer the network to support the required call volume.

Alternatively, through the use of Bandwidth Management Zones, an administrator can enter the amount of bandwidth available for voice on the IP network into the Call Server. The amount of bandwidth is ensured using other QoS mechanisms, such as priority and the type of voice codec used. The Call Server ensures that the VoIP call volume entering or leaving a zone does not exceed the IP network available bandwidth. This enables users to avoid quality degradation because of insufficient bandwidth for active connections.

Call admission control applies to a single distributed system with centralized call control, or multiple systems, such as a main site with numerous branch offices connected with VoIP.

The following figure shows an example of Bandwidth Management.

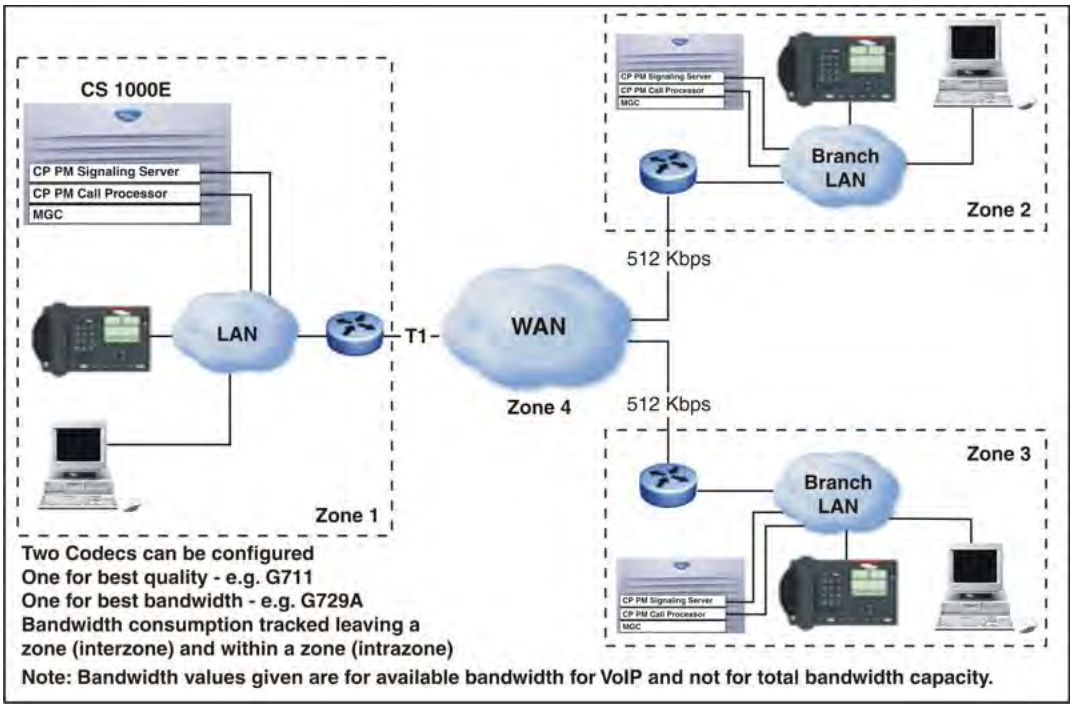


**Figure 1: Bandwidth management example**

**Important:**

After all bandwidth is used, the system blocks and reroutes additional calls. Keep this in mind when you design and implement Network Bandwidth Management.

# Adaptive Network Bandwidth Management

Adaptive Network Bandwidth Management applies only to Interzone traffic. Adaptive Bandwidth Management builds on Bandwidth Management but adds the following functionality:

- Adaptive Bandwidth Management automatically changes the bandwidth limit depending on the Quality of Service (QoS) in the network.
- Bandwidth limit automatically adjusts on a zone-to-zone basis. If there are QoS problems reported between a Call Server in Zone 3 and another in Zone 5, then the bandwidth limit reduces for calls between Zone 3 and Zone 5.

For more information about configuring Adaptive Network Bandwidth Management, see Adaptive Network Bandwidth Management configuration on page 253.

# Tandem Bandwidth Management

For the main office to correctly monitor all the bandwidth used to and from a branch office the call must tandem through the main office. When calls tandem through the main office, only the signaling is tandemed, the actual voice bandwidth travels directly between the source and destination. For more information about provisioning for Tandem Bandwidth Management, see Provisioning for Tandem Bandwidth Management on page 254.

# Network Wide Virtual Office

Bandwidth Management support for Network Wide Virtual Office allows for the correct bandwidth calculation for IP users who are using the Virtual Office feature to login to their home IP Phones from different Call Servers within the network. Two fields are used to achieve this —Configured Zone and Current Zone.

The same Virtual Private Network Identifier (VPNI) to all Call Servers in a network is assigned, so you can identify the entire network by one VPNI number. You can assign the same Bandwidth zone number to different Call Servers and an INTRAZONE policy between them.

The Network Wide Virtual Office feature does not interfere with the existing functionality of the Bandwidth Management feature, because it supports previous bandwidth configuration rules. This feature extends the meaning of the Virtual Private Network Identifier (VPNI). In previous releases, VPNI was used to identify one customer system that consisted of a Main Office (MO) switch and a branch office (BO) switch. Now a VPNI number identifies the whole customer network that includes all MO and BO switches. For more information about Bandwidth

Management support for Network Wide Virtual Office, see Bandwidth Management support for Network Wide Virtual Office on page 259.

## Abbreviated Dialing

With Abbreviated Dialing, IP Phone 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. For more information about configuring Abbreviated Dialing, see Abbreviated dialing on page 298.

## Zones

A zone is a collection of IP Phones that:

- share similar IP bandwidth restrictions
- exist geographically close to one another
- exist in the same time zone
- exist in the same PSTN dialing plan

Dialing plans treat all telephones in the same zone identically. You assign each IP Phone to a zone during configuration. For more information about configuring Zones, see Zone configuration on page 281.

**Important:**

This document uses the term "zone" to refer to a Bandwidth Management Zone (not a Gatekeeper Zone).

## SIP Line Service

The SIP Line feature comprises three major software components: Call Server (CS), SIP Line Gateway (SLG), and SMS. Software changes on Communication Server 1000 are bundled within the SIP Line Package (417) and reside on the same hardware platform as supported in Release 5.5 in addition to Linux COTS and CP PM Call Server.

**Important:**

You must upgrade Communication Server 1000 software to enable and configure SIP Line Service.

No upgrade is required for the SLG Service.

For more information on upgrading your Communication Server 1000, see *Communication Server 1000E – Software Upgrades, NN43041-458*.

# Redundancy operation

For redundancy, you can configure a leader and follower for a SIP Line Gateway (SLG) node with both servers sharing the same node IP. However, clients on the same node can be registered on only the current node master. No load sharing occurs between the two SLG nodes.

# Survivable SIP Media Gateway Data Replication

Survivable SIP Media Gateways offer full survivability to the gateway and its associated endpoints because a copy of the primary system database exists on the survivability blade of the gateway. The system keeps the gateway copy up-to-date by automatically replicating data from the primary system to the gateway.

To ensure proper operation of the survivability feature the data network must meet the performance requirements for the successful replication of data from the primary system to the gateway across the data network. These performance requirements are:

- 300ms round trip delay, maximum
- Less than 1% packet loss

# Supported codecs

Codec negotiation and selection follow the same operation as SIP Gateway. No new codecs are added.

In summary, support exists for the following codecs:

- G.711 u-law/a-law
- G.729A/AB
- G.723.1
- T.38 for FAX

By default, G.711 requires support at both ends of a call. The default payload sizes for G.711 and G.729 are both 20 milliseconds (ms). Any other unrecognized codec (including video) are forwarded to the far end through the SDP transparency feature. The SDP transparency feature

enables multiple media descriptions and sends the associated codec attribute information to the destination.

## Codec selection

The SLG always sends the originating node codec list in order of preference, and the terminating node selects one common codec based on preference. This means that the receiver of an offer always performs the codec selection, and it selects one common codec based on the best bandwidth selection mechanism.

## Codec payload sizes considerations

If the SDP has no packet time (ptime), the default payload size is used: 20 ms for G.711 and G.729, 30 ms for G.723, and 20 ms for G722.

If you configure a specific payload size different from the default payload size, the offer includes a ptime. Only one ptime can exist for each codec in this version of SDP.

## Zone Based Dialing plan

Switching to a ZBD requires development on dial plans, numbering plans and routing features to make sure that the migration is transparent to the enterprise network users and that the same dial plan and business grade telephony features are used.

## New prompts and changed overlays

Numbering zone and zone based flexible dial plan concepts are introduced to provide ZBD functionality.

Numbering zones are assigned to all sets and attendant, and they contain zone specific information such as site prefix, country code, access prefixes (for international, national, and subscriber calls).

Zone based Flexible Dialing Plan (ZFDP) is introduced to reduce complexity of configuration.

The following prompts are introduced:

- LD 10, 11 — New prompt NUMZONE is introduced to assign a numbering zone to a phone (analog, TDM, and IP).
- LD 12 — New prompt NUMZONE is introduced to assign a numbering zone to an attendant.
- LD 15 — New prompt ZBD is introduced to enable or disable the ZBD feature.

  — New prompt DIALPLAN is introduced to show DN/CLID for private and public on-net dial plans.
- LD 20 — New prompt NUMZONE is introduced to display a numbering zone configured for a telephone (analog, TDM, and IP) or attendant.
- LD 21 — New prompt ZBD is introduced to display the value of ZBD option.

  New prompt DIALPLAN is introduced to show configured value in customer data block.
- LD 22 — ZBD package is printed.
- LD 43 — ZBD databases are dumped into /u/db/ during EDD.

  — ZBD databases are restored from /u/db/ during database restore.
- LD 81 — New prompt NZON is introduced to print a list or count of telephones with selected numbering zone.
- LD 83 — New prompt NUMZONE is introduced to print a list of units with configured numbering zone.
- LD 117 — New commands are introduced to configure numbering zones, parameters for numbering zones (prefix, DAPC, CC, NPA, and ACx) , and a zone dialing plan.

# Meridian Customer Defined Network Alternate Routing and Vacant Number Routing

Vacant Number Routing (VNR) is a default route used for routing untranslatable, invalid, and unassigned dialed numbers (DNs). When the call is routed by VNR to the IP network, the user has the flexibility to perform Meridian Customer Defined Network Alternate Routing (MALT) on the Call Server for an additional 10 causes other than the existing six. Configure these additional MALT causes within Element Manager (EM). If the call is determined to be a VNR call, which is tried at least once to route over an IP route, then vacant number treatment is provided to the call. Thus, this feature development combines both the VNR and MALT functionality for calls routed over IP, to give more benefit to the customer, by routing a call to the proper destination and providing appropriate vacant number treatment. For more information about configuring VNR and MALT, see *IP Peer Networking Installation and Commissioning, NN43001-313*. For more information about Element Manager, see *Element Manager – System Administration, NN43001-632*.

Calls to the IP network need the ability to reroute to another alternate, while maintaining the ability to receive vacant number treatment when the called destination is an unassigned number. There are two parts of this feature:

1. MALT on calls routed to the IP domain

   This feature deals with VNR calls at the CS1K, routed over H.323/SIP. If the call fails to route to the destination the call gets disconnected with a cause which matches one of the original MALT cause codes, or disconnects with an indication to use MCDN Alternate Routing. If MALT exhausts all routes in the VNR route list block hen the treatment corresponding to the disconnect cause is provided.

   With the default MALT handling, there are six causes, which perform MALT at the Communication Server 1000:

   - 3 - No route to destination
   - 27 - Destination is out of service
   - 34 - No circuit or channel available
   - 38 - Network out of service
   - 41 - Temporary failure
   - 42 - Switching equipment congestion

2. Configurable MALT causes for different vendors

   A configurable option is provided in EM for the different vendors in order to configure causes to accomplish MALT at the Communication Server 1000. Element Manager provides the following causes to be configured to perform MALT:

   - 01 – unassigned number
   - 20 – subscriber absent
   - 47 – Resources unavailable
   - 51 – Call rejected; blocked by MBG
   - 52 – Outgoing call barred
   - 53 – Outgoing call barred in closed user group
   - 54 – Incoming call barred
   - 55 – Incoming call barred in closed user group
   - 63 – service or option not available
   - 127 – Interworking unspecified

   If a call disconnects prior to establishing a clear message, using one of the causes listed previously, and the causes are configured on the Signaling Server to perform MALT, then a new IP IE is built with an indication `use MALT` with the cause. This IE is sent to CS with the `in the received clearing` message. The CS would trigger MALT for the cause.

For more information about system messages for VNR and MALT, see *Software Input Output Reference - System Messages, NN43001-712*

## Alternate Call Routing for Network Bandwidth Management

Alternate Call Routing (ACR) for Network Bandwidth Management allows a station-to-station call (a call that does not use a trunk) between a branch office and main office to overflow to traditional routes. Overflow can occur if there is insufficient interzone bandwidth available to carry the call or if the Quality of Service (QoS) has degraded to unacceptable levels. This feature also applies to station-to-station calls from one branch office to another branch office, provided both stations are registered to the same main office. For more information about Alternate Call Routing, see Alternate Call Routing on page 264.

## Quality of Service versus Bandwidth Management

One approach to network engineering states that Quality of Service (QoS) is not needed; simply increasing bandwidth provides enough QoS for all applications. This theory also states that implementing QoS is complicated and adding bandwidth is easy. However, due to the bursty nature of IP network traffic, even very large amounts of bandwidth may not be enough to prevent congestion during a burst of traffic at a particular instance in time.

If all networks had infinite bandwidth available, so that network congestion never occurred, QoS technology would not be needed. While having adequate bandwidth provisioned on the network is very important, over provisioning may not be very realistic; therefore, QoS mechanisms are needed. For more information about QoS mechanisms, see QoS mechanism on page 40.

## Security

For more information about CS1000E and CS1000M system security, see *Security Management Fundamentals, NN43001-604*.

## Security domain considerations and guidelines

The security domain is established after the primary security server is installed and configured. The following is a high-level list of considerations and guidelines for installing and configuring a security domain:

| Considerations and guidelines |
| --- |
| Ensure the latest patches are installed on all systems.<br>For information about patching, see *Patching Fundamentals, NN43001–407*. |
| If you are using DNS, configure DNS first. |
| Install and configure the primary UCM security servers (and if desired, the backup security servers) before any other elements. Ensure they are fully patched.<br>For information about installing and configuring the primary and backup security servers, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*. |
| The FQDN of a UCM security server is associated with its TLAN IP address. You must always configure a security server using the TLAN. |
| The PC used for web browser access to UCM must be connected to the TLAN (except for networks in the Managed Services configuration). If no DNS server is in use, the PC hosts file should include an entry containing the TLAN IP address and FQDN of the primary security server. |
| Ensure that all elements can communicate with the UCM security servers. When required, configure static routes. |
| Register VxWorks-based servers and devices using the ELAN IP address of the UCM primary security server. You require a CLI (telnet, rlogin or ssh) connection for this.<br>For information about registering VxWorks devices, see *Avaya Security Management Fundamentals, NN43001-604*. |
| Register Linux-based servers and devices using the TLAN FQDN of the UCM primary security server.<br>For information about registering Linux devices, see *Avaya Security Management Fundamentals, NN43001-604*. |
| Use the Secure FTP Token Management page to validate successful registration by generating and distributing the token to all elements.<br>For information about generating the Secure FTP Token, as well as information about overall security management, see *Avaya Security Management Fundamentals, NN43001-604*. |

## Secure Transport Enhancements

This feature enhances the security of the File Transfer Protocol (FTP) infrastructure in Communication Server 1000.

## SSH File Transport Protocol

SSH File Transport Protocol (SFTP) is a network protocol that provides confidentiality and integrity to the data (such as files or commands) transmitted between an SFTP client and a server. In addition, SFTP allows a client and a server to authenticate each other. In this feature, password is used by an SFTP server to authenticate an SFTP client.

## UNIStim Security with DTLS

UNIStim Security with DTLS provides signaling encryption for UNIStim IP Phones based on the industry standard DTLS protocol (RFC 4347).

# Network design and implementation

**Important:**

Before a Communication Server 1000 system can be installed, a network assessment must be performed and the network must be VoIP-ready. For more information, see Configuration on page 227.

If the minimum VoIP network requirements are not met, the system does not operate properly.

Many considerations are important when you create and maintain a converged network. It is important to gain a detailed understanding of the design of the existing data network before you implement a Voice over Internet Protocol (VoIP) network.

To create a VoIP-grade network, certain QoS standards for various basic network elements must be met. Several QoS parameters can be configured, measured, and monitored to determine if the desired service levels are provided and obtained. The mechanisms needed to design a robust, redundant QoS-managed VoIP network are described in this document.

The following figure contains a logical view of the steps necessary to assess a network for Voice over Internet Protocol (VoIP) readiness. Use this network assessment flow chart as a guideline for the network engineering process.

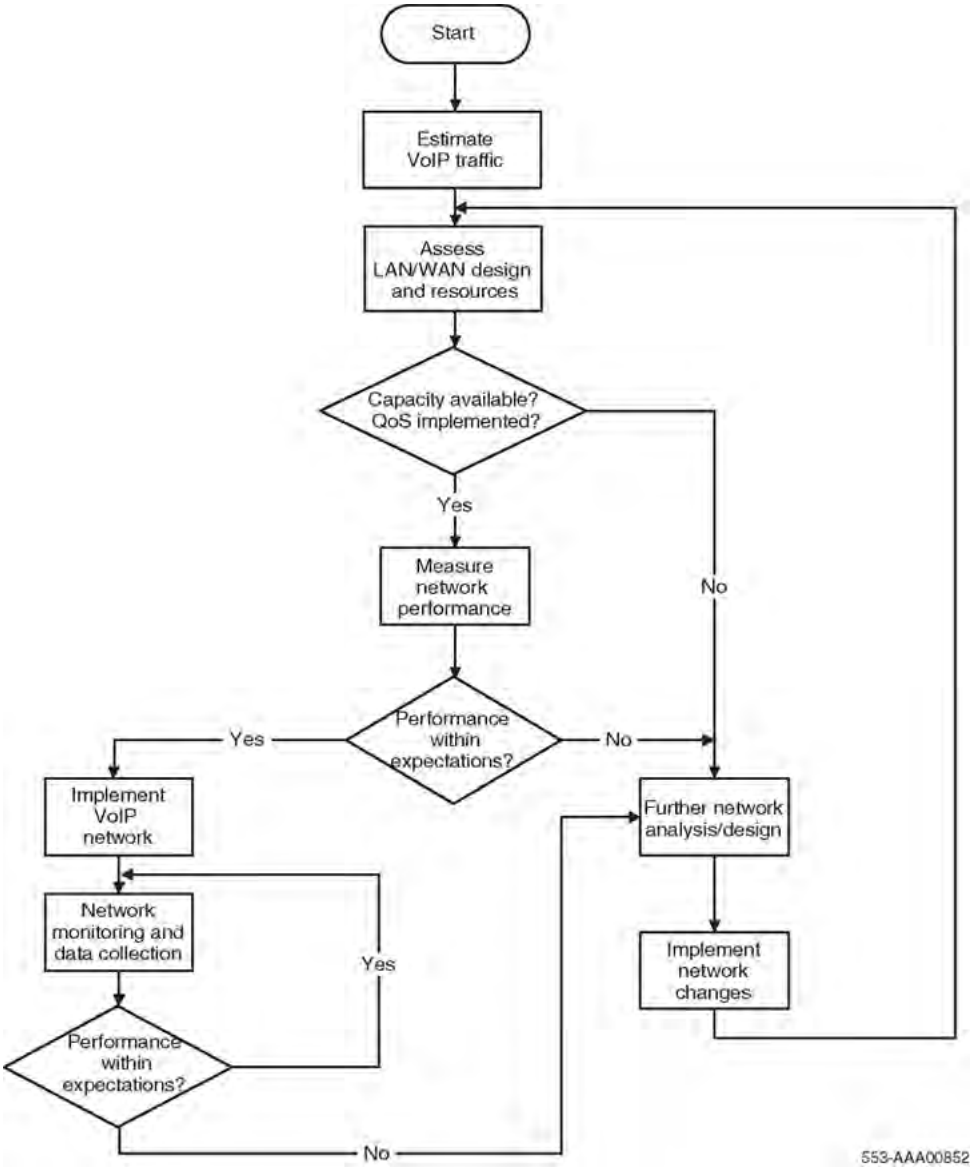


**Figure 2: Network assessment flow chart**

# Network performance measurement and monitoring

TCP/IP was originally designed to reliably send a packet to its destination. Little consideration was given to the length of time it took to get there. Today, IP networks transport data from many different application types. Many of these applications require minimal delay. Delay is the length of time needed for information to travel through a network. Significant delay can adversely affect end-user quality; and in some cases, the application does not function at all.

Networks now carry many different types of traffic. Each traffic type has unique requirements for the following QoS parameters:

- network availability
- bandwidth
- delay
- jitter
- packet loss

These QoS parameters apply to any IP (Internet Protocol) network that carries VoIP traffic, including LANs, campus-wide networks, and WANs. These QoS parameters can be measured and monitored to determine if they meet desired service levels. Each of these elements are discussed in detail in Network Performance Measurement on page 122. For more information about the ongoing monitoring, management, and measurement of the network, see The VoIP network operation on page 209.

# Available tools

**Important:**

Tools are available for almost every aspect of converged network engineering. Nortel strongly recommends the use of appropriate tools when performing network engineering.

Some of the available tools include:

- Multiprotocol network design assessment software. These tools can analyze a network, highlight potential problems, and propose possible solutions.
- SNMP-based network management systems for network design assessment and monitoring.
- Graphical device configuration managers for almost all network switches can integrate into SNMP network management systems.
- Policy managers for implementing end-to-end QoS policies.
- Network performance measurement tools for monitoring network jitter, delay, and packet loss.

All of these tools can be operated from a central location on the network. Use the tools to simplify network engineering and operations, ultimately resulting in lower costs and higher quality services.

Nortel offers professional Network Architecture and Design services. For more information, contact a Nortel sales representative.

# Chapter 5: Planning and engineering

This chapter contains information about topics to consider before you implement a converged voice and data network.

## Navigation


- Quality of Service on page 40
- IP network best practices on page 64
- Bandwidth Management on page 73
- Bandwidth Management parameters on page 95
- Abbreviated dialing on page 109
- Bandwidth and data network switch efficiency on page 110
- Network design assessment on page 110
- Network planning on page 122
- Network Performance Measurement on page 122
- LAN design on page 164
- Zone Based Dialing plan on page 193
- Vacant Number Routing feature on page 196
- Dialing plan on page 196
- Distributed Media Gateway 1000E on page 199
- DHCP configuration on page 200
- The VoIP network operation on page 209
- UNIStim Security with DTLS on page 35

# Quality of Service

To ensure consistent voice quality, Quality of Service (QoS) must be supported on the platforms that transport Voice over Internet Protocol (VoIP). Consider the following list to provide QoS:

- Bandwidth Management
- packet classification
- DiffServ
- fragmentation
- traffic shaping
- queueing mechanisms provided by the platform

If appropriate QoS mechanisms are not supported by the platform, an upgrade can be required.

## QoS mechanism

An IP network must be properly engineered and provisioned to achieve high voice quality performance. The network administrator should implement QoS policies network-wide, so voice packets receive consistent and proper treatment as they travel the network.

IP networks that treat all packets the same are called best-effort networks. In such a network, traffic can experience different amounts of delay, jitter, and loss at any given time. This can produce the following problems:

- speech breakup
- speech clipping
- pops and clicks
- echo

A best-effort network does not guarantee bandwidth at any given time.

The best way to guarantee bandwidth for voice applications is to use QoS mechanisms in the intranet when the intranet is carrying mixed traffic types.

QoS mechanisms ensure bandwidth is 100% available at most times, and maintain consistent, acceptable levels of loss, delay, and jitter, even under heavy traffic loads.

QoS mechanisms are extremely important to ensure satisfactory voice quality. If QoS mechanisms are not used, there is no guarantee that the bandwidth required for voice traffic is available. For example, a data file downloaded from the intranet could use most of the WAN bandwidth unless voice traffic has been configured to have higher priority. If the data file download uses most of the available bandwidth, it causes voice packet loss and; therefore, poor voice quality.

Apply QoS mechanisms to the following VoIP media and signaling paths:

- TLAN connections
- VoIP traffic between IP Phones
- VoIP traffic between IP Phones and Voice Gateway Media Cards on the TLAN subnet

**Important:**

Nortel strongly recommends that you implement suitable QoS mechanisms on any IP network that carries VoIP traffic.

## Traffic mix

Before you implement QoS mechanisms, assess the traffic mix of the network. QoS mechanisms depend on the process and ability to distinguish traffic by class to provide differentiated services.

If an intranet delivers only VoIP traffic, and all traffic flows are of equal priority, you do not need to consider QoS mechanisms. This network would only have one class of traffic.

In most corporate environments, the intranet primarily supports data services. When you plan to offer voice services over the intranet, assess the following:

- Are there existing QoS mechanisms? What are they? VoIP traffic should take advantage of established mechanisms, if possible.
- What is the traffic mix? If the volume of VoIP traffic is small compared to data traffic on the intranet, then IP QoS mechanisms are sufficient. If VoIP traffic is significant, data services might be impacted when those mechanisms are biased toward VoIP traffic.

## TCP traffic behavior

The majority of corporate intranet traffic is TCP-based. Unlike UDP, which has no flow control, TCP uses a sliding window flow control mechanism. Under this scheme, TCP increases its window size, increasing throughput, until congestion occurs. Congestion is detected by packet losses, and when that happens throughput quickly throttles down, and the whole cycle repeats. When multiple TCP sessions flow over few bottleneck links in the intranet, the flow control algorithm can cause TCP sessions in the network to throttle at the same time, resulting in a periodic and synchronized surge and ebb in traffic flows. WAN links appear to be congested at one period of time and then are followed by a period of under-utilization. Two consequences are:

- WAN link inefficiency.
- VoIP traffic streams are unfairly affected.

The solution to this problem is Weighted Random Early Detection queueing (WRED) as described on Weighted Random Early Detection on page 44.

## QoS problem locations

Figure 3: Potential uplink problem areas on page 42 identifies typical network congestion areas. Voice traffic competes for limited bandwidth on the uplinks. These uplinks are shown in Figure 3: Potential uplink problem areas on page 42. Congestion at these points causes the majority of all packet loss, delay, and jitter. QoS mechanisms can alleviate this congestion by using multiple queues with different priorities.

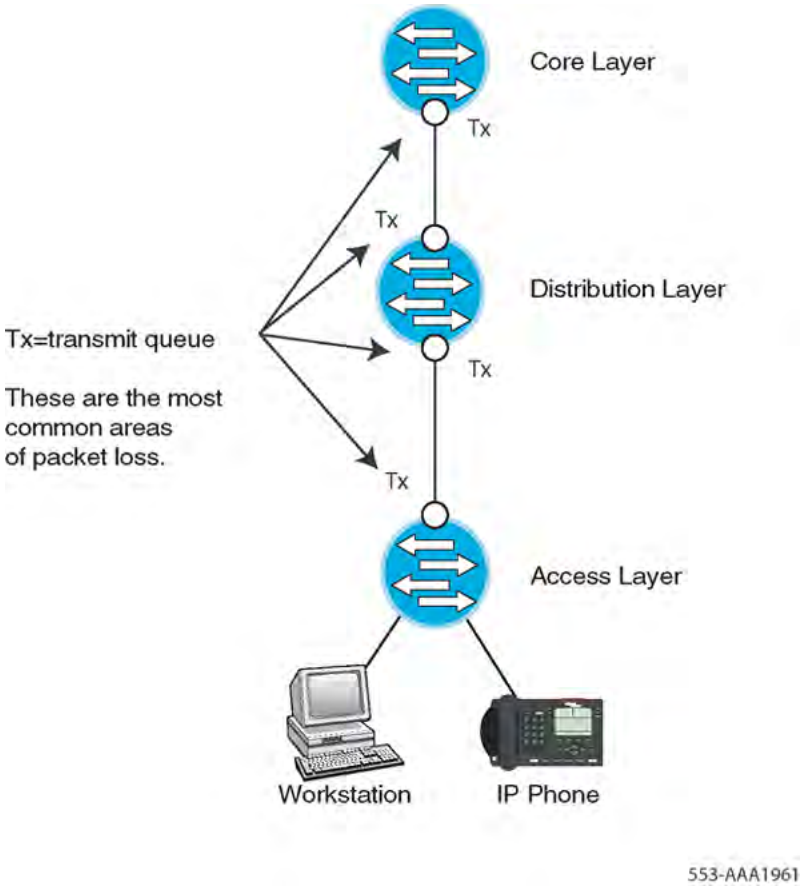


**Figure 3: Potential uplink problem areas**

## Campus networks

In most cases, campus Ethernet networks require less sophisticated QoS mechanisms than low-bandwidth WAN connections, because the available bandwidth is much greater. This results in significantly lower queueing and network delay. However, network congestion on an Ethernet network (even for short periods of time) and bursty TCP-based Internet traffic can cause significant voice quality problems if QoS is not applied.

QoS mechanisms, such as 802.1Q, VLANs, and Layer 2 Port prioritization (802.1p), can be used for VoIP traffic over Ethernet networks. If the Layer 2 (Ethernet) switches also support Layer 3 (IP) capabilities, then QoS mechanisms such as DiffServ and IP Address prioritization can also be used. For example, the Business Policy Switch (BPS) is a Layer 2 switch that can recognize, filter, monitor, and remark 802.1p and DiffServ markings, based on implemented policy.

## Wide area networks

A wide area network (WAN) is a geographically-dispersed telecommunications network. For example, a WAN can extend across many cities or countries.

WANs require more sophisticated QoS mechanisms, such as fragmentation and interleaving.

For more information, see WAN QoS mechanisms on page 46.

## The QoS process

Packet handling on a QoS-enabled network consists of three stages:

1. Classification
2. Marking
3. Queueing, also known as Forwarding

To implement QoS on an IP network, all packets entering the IP network must be classified and marked. The packets are then placed into transmission queues of a certain priority.

Packets in high-priority queues are transmitted before packets in best-effort lower priority queues. VoIP packets no longer have to compete with best-effort data packets for IP network resources. Typical QoS implementations protect call quality by minimizing loss, delay, and jitter. Bandwidth cannot be assured without the use of some type of reservation protocol, such as Resource Reservation Setup Protocol (RSVP).

## Classification

Software on the following hardware elements can classify and mark VoIP packets:

- Signaling Server – classifies packets as signaling packets.
- Voice Gateway Media Card – classifies packets as voice or signaling packets.
- IP Phones – classifies packets as voice or signaling packets.

**Important:**

To classify Signaling Server and Voice Gateway Media Card packets at Layer 2 (802.1p), Layer 3 (DiffServ) or both, implement QoS mechanisms on the Signaling Server and Voice

Gateway Media Card and the Layer 2 switch ports to which they are attached. IP Phones with firmware 1.31 (or later) can classify voice and signaling packets at Layer 2 (802.1p), Layer 3 (DiffServ), or both.

Classification can be implemented on Layer 2 or Layer 3 switches. See the switch documentation for information about configuring classification.

Policy management also provides other methods to classify and mark packets, based on identifiers, such as the originating IP address of the packet. For more information about Policy Management, see Policy management on page 61.

Packets can also be premarked with default 802.1p and DiffServ CodePoint (DSCP) values. Configure the Layer 2, Layer 3, or Policy switches to trust that these packets are marked correctly.

## Marking

When powered-up, Nortel IP Phones contact the Terminal Proxy Server (TPS) that controls them. The TPS then instructs the IP Phones to mark all packets with a default configurable (through Communication Server 1000 Manager) DSCP and/or 802.1Q/802.1p tag. The tag is also configurable using Communication Server 1000 Element Manager. The control packets are marked for each of the following.

- Signaling Server
- Voice Gateway Media Cards
- Media Gateway 1000T (MG 1000T)
- Network Routing Service

## Queueing

Queueing delay is a major contributor to delay, especially on highly used and low-bandwidth WAN links (see Queueing delay on page 148). Routers that are QoS-aware and that support priority queueing can help reduce the queueing delay of voice packets when these packets are treated with preference over other packets.

### Weighted Random Early Detection

The global synchronization situation described in TCP traffic behavior on page 41 can be countered using a buffer management scheme that discards packets randomly as the queue starts to exceed a threshold. Weighted Random Early Detection (WRED), an implementation of this strategy, also inspects the DiffServ bits in the IP header when considering which packets to drop during buffer build up. In an intranet environment where TCP traffic dominates real-time traffic, WRED can be used to maximize the packet dropping from long-lived TCP sessions and minimize the voice packet dropping. Check the configuration guidelines with the router vendor for performance ramifications when you enable WRED. If global synchronization is to be countered effectively, implement WRED at core and edge routers.

## Packet prioritization and schedulers for VoIP

All VoIP packets must be given a priority higher than the priority of non voice packets to minimize delay, jitter (delay variation), and packet loss that adversely affect voice quality.

All voice packets must be placed in the highest-priority queue using a strict-priority scheduler, or a scheduler that can be configured to behave as a strict-priority scheduler. Some switches only permit network-controlled traffic in the highest-priority queue, which leaves the second highest-priority queue for the remaining user traffic.

**Important:**

Nortel strongly recommends that you place voice traffic in a queue separate from other traffic types. However, if there are few queues available in the Layer 2 or Layer 3 switch, then voice traffic can be combined with other high-priority network-controlled traffic. Because the queueing delay is small for Ethernet network interfaces, this should have very little impact on voice quality.

Most Layer 2 switches use a strict-priority scheduler that schedules all packets in a higher-priority queue before it services any packets in a lower priority queue.

All VoIP packets must be queued in a router or switch using a strict priority scheduler. This ensures that VoIP packets receive priority treatment over all other packets. Because a strict priority scheduler can starve the servicing of all other traffic queues, a threshold must be determined to limit the maximum amount of bandwidth that the VoIP traffic can consume. This threshold is also called rate limiting.

**Important:**

Nortel strongly recommends that you use a strict priority scheduler for VoIP.

The Business Policy Switch (BPS) places the voice packets in the highest-priority queue using a strict-priority scheduler in its 4-queue system, when QoS is enabled on an interface.

Other vendors often refer to priority queueing when they describe techniques for strict-priority scheduling.

Some Layer 3 switches and routers support priority and weighted schedulers. Voice packets must be placed in a queue that uses a strict-priority scheduler, or in a queue that uses a weighted scheduler configured to behave like a strict-priority scheduler.

The Passport 8600 uses a weighted scheduler, with its highest-priority user queue configured by default to behave like a strict-priority scheduler. The queue is configured with all Packet Transmit Opportunities (PTOs) enabled. This is equivalent to a weight of 100% (high priority). Voice packets with DSCPs marked with EF (Expedited forwarding) and CS5 (Class Selector 5) are placed in this queue by default when QoS is enabled on an interface.

Nortel does not recommend other weighted schedulers, such as Weighted Round Robin (WRR) or Weighted Fair queueing (WFQ). If the router or switch does not support a priority scheduler and only supports a weighted scheduler, the queue weight for VoIP traffic should be configured to 100%. If a 100% weight cannot be configured due to a product limitation, consider replacing the product because it can cause unpredictable voice quality.

## WAN QoS mechanisms

There are many things to consider when using routers with low-bandwidth WANs and low bandwidth access network connections such as T1, xDSL, or Packet Cable.

This section specifically discusses WAN connections, but the techniques and recommendations described also apply to low-bandwidth access network connections.

## Bandwidth demand

VoIP can use an existing WAN data network to save on interoffice toll calls. However, offices often connect over low-bandwidth WAN connections, so special considerations must be made when you add VoIP over a bandwidth-limited connection.

When VoIP calls are active, routers configured with QoS (which prioritizes voice traffic over data traffic) reduce the data traffic throughput by the amount of bandwidth used for the VoIP call. This reduces the data traffic throughput to a possibly unacceptable level. Adding VoIP to the existing WAN data network might require an increase in the WAN bandwidth.

VoIP bandwidth depends on the following:

- type of codec used
- Voice Activity Detection (VAD), if used; also known as Silence Suppression
- packetization rate (voice sample size)
- IP/UDP/RTP encapsulations
- RTP Header Compression, if used
- Layer 2 (link layer) protocol overhead for the specific link the voice traffic is traversing. Depending on the link protocol used and the options invoked, the link protocol adds the following to each VoIP packet:
  - 5 to 6 octets (FR)
  - 7 to 8 octets (PPP)
  - 18/22:26/30:38/42 octets (802.3 LAN – with or without 802.1Q/802.1p 8-octet preamble and 12-octet interframe gap)

  The extra octets create an additional overhead of 2 kbit/s (5-octet FR) to 16.8 kbit/s (42-octet 802.3 LAN) for each VoIP call.

  ATM has its own overhead requirements. Due to the fixed cell size of 53 octets, the additional overhead varies widely, depending on the codec and packetization rate used.

### Bandwidth example

A company has two sites connected by a leased-line WAN connection (PPP) operating at 128 kbit/s. Due to the potential use of 20% of link capacity for zero-bit stuffing, a safe assumption for link capacity is 102 kbit/s. For design purposes, assume a maximum use of 70% (in this example, 90 kbit/s).

The 70% bandwidth is sufficient for the current data requirements. The company believes that it only needs 70-80 kbit/s most of the time, with occasional traffic peaks up to the full capacity. The company wants to support up to 4 simultaneous voice calls over the IP WAN network between the sites.

With 4 simultaneously active calls, the company requires 108.8 kbit/s (using a G.729 codec, 20 ms voice sample, and PPP overhead/frame) of the available 90 kbit/s of the 128 kbit/s link.

This requirement exceeds the carrying capacity of the link and completely starves that data traffic. The solution is to upgrade the WAN connection bandwidth. A 256 kbit/s link is the minimum speed to provide 109 kbit/s for four G.729 VoIP calls, 80 kbit/s for data, and 20% availability for zero-bit stuffing.

## Fragmentation and interleaving

To minimize voice delay and jitter in mixed voice/data IP networks, fragment large packets before they traverse limited-bandwidth (<1 Mbit/s) connections. There are several different protocols that can be used to fragment packets.

For Frame Relay connections, the FRF.12 standard can be used to fragment packets. ATM provides fragmentation because all packets are fragmented into 53-byte ATM cells. Both of these fragmentation techniques are acceptable.

Two types of fragmentation are more universal and not limited to a specific link-layer technology, such as ATM or Frame Relay. These methods are PPP fragmentation and IP fragmentation.

See the router documentation for information about configuring PPP and IP fragmentation.

Layer 2 fragmentation (ATM, FRF.12, PPP) is preferred over Layer 3 fragmentation, as Layer 2 fragmentation universally affects all higher-layer protocols. Layer 3 fragmentation is less desirable for the following two reasons:

1. Layer 3 fragmentation applies only to the specific protocol used. For example, the Internet Protocol Maximum Transmission Unit, in bytes, affects only IP traffic. It has no effect on IPX or other protocols.
2. Some applications do not function because the Do not Fragment bit is turned on. This Do not Fragment bit prevents application packets from transmitting.

### PPP fragmentation and interleaving

Many routers support PPP fragmentation, which splits large packets into multiple smaller packets and encapsulates them into PPP frames before they are queued and transmitted. PPP fragmentation lets higher-priority VoIP packets to be transmitted ahead of the lower-priority data packet fragments that have already been queued. The voice packets and data fragments are interleaved, so the maximum delay a voice packet experiences is one fragment time (ideally <=10 ms), rather than one large packet time.

For example, a small voice packet enters a router, followed by a large data packet, which is followed by a second voice packet. The first voice packet is transmitted as the first frame on the link. Next, the first data fragment is transmitted, followed by the second voice packet, then

the second data fragment. If no more packets, enter the router then the remaining data fragments will continue to be transmitted until the entire data packet has been sent.

Interleaving is a result of voice packets having a higher priority than data packets. A data fragment can be transmitted first; however, when a high-priority voice packet arrives, the voice packet is sent before the rest of the data packet.

### IP fragmentation

All routers support IP fragmentation, which configures all IP packets to a size determined by the MTU (Maximum Transmission Unit). Most routers use a default maximum packet size of 1500 bytes (the largest packet allowed on Ethernet LANs), which can take a long time to transmit over a low-bandwidth connection.

**Important:**

When you determine the fragment size for a packet, ensure that the fragment size is not smaller than the voice packet. Fragment only large data packets, not the voice packets.

For example, when you send using a 64 kbit/s link, a 1500-byte data packet takes 188 ms to transmit. If the WAN connection is Frame Relay (FR), this same queueing delay is added again when the packet is queued at the far-end FR switch on the other side of the connection. To achieve high voice quality, the desirable end-to-end delay for a voice packet is less than 150 ms. In this example, the data packet uses up almost the entire delay budget for the voice traffic before the first voice packet transmits. Jitter of 188 ms is created, which exceeds the normal jitter buffer settings of 2 to 3 voice sample sizes (40 to 90 ms). In this case, at least one packet (usually many packets) arrive too late for use.

If you use bandwidth-limited connections (<1 Mbit/s) without Layer 2 (ATM, FRF.12, or PPP) fragmentation, the router must be configured to transmit smaller packets by adjusting the MTU size for the IP packets. Ideally, the MTU size is adjusted to achieve an optimum delay of 10 ms or less over the different connection speeds. Therefore, a higher bandwidth connection has a larger MTU size than a lower bandwidth connection.

**Important:**

When IP fragmentation is used, the packets remain fragmented from source to destination. This can result in reduced data performance as the larger data packets fragment into multiple, smaller fragments that use more bandwidth

The following table provides the recommended maximum MTU sizes for different connection speeds when you use IP fragmentation. These choices result in a maximum delay of 8 ms.

Table values also apply to Layer 2 fragmentation techniques.

**Table 3: Recommended MTU sizes for various connection speeds**

| | Connection Rate (in kbit/s) | | | | |
|---|---|---|---|---|---|
| | **56** | **64** | **128** | **256** | **512** |
| Maximum MTU size (in bytes) | 56 | 64 | 128 | 256 | 512 |

**Important:**

Nortel strongly recommends that you use PPP for packet fragmentation. Use IP fragmentation only if the router does not support a Layer 2 fragmentation protocol, such as PPP or FRF.12.

### Packet reordering

In some cases, there can be multiple paths for a VoIP packet when it travels from source to destination. If all VoIP packets do not take the same path, packets can arrive out-of-order. This can cause voice quality issues, even though packet reordering often has little or no adverse affect on data traffic quality due to the design of the data protocols.

For example, if two locations connect using two Frame Relay Permanent Virtual Circuits (PVCs), ensure that all voice traffic for a specific call travels on the same PVC. The routers can be configured to direct voice packets from the same source/destination IP address to traverse the same PVC. You can also configure the router to send all voice traffic over only one PVC.

## Traffic shaping

In a Frame Relay environment, a typical design could have many low-speed links that terminate at Media Gateway 1000B (MG 1000B) locations with a single high-speed link into a hub location as illustrated in the following diagram.

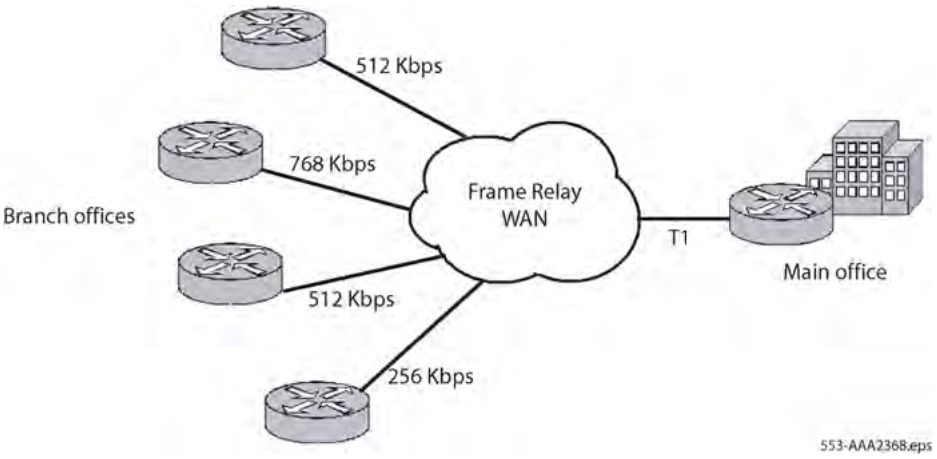


**Figure 4: Traffic shaping**

In this example, the MG 1000B sites with a low speed link can be overrun by traffic from the central site that has a larger bandwidth connection, or the main office site could be overrun with traffic from all of the MG 1000B sites. Without traffic shaping, the network can randomly drop packets. The resulting packet loss degrades voice quality.

Traffic shaping prevents voice quality degradation by determining which packets to drop due to congestion and which packets receive priority.

Traffic shaping works by queueing excess traffic to lower the amount of bandwidth across a Frame Relay WAN to limit traffic to a predetermined level. This is known as the Committed Information Rate (CIR). CIR is negotiated with the service provider.

If data is offered too fast and the Committed Burst (Bc) rate plus the Excess Burst (Be) rate exceeds the CIR over a certain Time Interval (Tc), the Frame Relay network can mark packets as Discard Eligible. This cannot be tolerated when running real-time applications, such as voice.

When you run traditional data applications over Frame Relay, the network allows bursting over a certain Time Interval (Tc). If the data burst exceeds the contract during the Tcl, the Frame Relay network starts sending Layer 2 (L2) feedback in the form of Forward Explicit Congestion Notifications (FECN) and Backward Explicit Congestion Notifications (BECN). This L2 feedback informs the Data Terminal Equipment (DTE) devices (routers) that congestion exists in the upstream or downstream direction. Upon receiving this feedback, the DTE should throttle back to the Bc or a fraction of the Bc. It is also possible for the DTE to completely shutdown until the feedback indication abates for a period of time.

While this is considered a benefit for data applications, the resulting packet loss is detrimental to quality.

## RTP header compression

IP Real-Time Transport Protocol (RTP) header compression can be used to compress 40-byte (IP, UDP, RTP) VoIP packet headers to a size of 2 to 4 bytes.

This results in significant bandwidth savings across low-bandwidth WAN links. Note current WAN platform CPU levels before you implement RTP header compression, because it is CPU intensive.

## PPP QoS

It is important that QoS mechanisms are used over low-bandwidth links that carry both voice and data traffic.

If you implement QoS mechanisms over a PPP WAN link, it may involve the use of the following:

- priority queueing (possibly mapped from the Diffserv CodePoint (DSCP))
- RTP header compression
- fragmentation and interleaving

## Frame Relay QoS

Nortel recommends that you use separate Permanent Virtual Circuits (PVCs) for voice and data whenever possible. Ensure voice PVCs strictly conform to the CIR. Do not allow bursting or shaping. You can use partially meshed PVCs, depending on traffic patterns.

If voice and data traffic share the same PVC, it can be necessary to use priority queueing with traffic shaping to ensure that voice packets are not discarded or queued for a long period time. On low bandwidth links (<1 Mbit/s), fragmentation and interleaving (FRF.12) may have to be used.

## ATM QoS

Two methods exists to ensure VoIP QoS on ATM links:

- separate voice and data PVCs
- priority queueing on a shared voice and data PVC

Nortel recommends that you use separate voice and data PVCs. The available bandwidth for a particular ATM PVC is usually guaranteed by a service provider. If traffic through the PVC is restricted to VoIP traffic only, then no other QoS mechanisms in the ATM network must be used. Voice traffic can be mapped into the voice-only PVC according to the source IP address or Diffserv CodePoint. VoIP Bandwidth Management on the Call Server can then be used to ensure that the VoIP traffic volume does not exceed the amount of bandwidth available in the voice-only PVC.

If a shared voice and data PVC is used, then priority queueing must be configured across the ATM network to guarantee that voice traffic has priority over data traffic.

## Layer 2 (Ethernet) QoS

At Layer 2, VoIP packets can be classified by the following fields in the Ethernet header:

- source/destination MAC address
- 802.1Q
    - VLAN ID
    - 802.1p user priority bits

## MAC address

All MAC addresses are unique and should not be changed.

Packets can be classified by the MAC address. Packets from a Nortel IP Phone can be recognized because each Nortel IP Phone has a unique MAC address. When the Layer 2 switch recognizes the IP Phone packet MAC address, it marks the packets with the appropriate 802.1p value. The Layer 2 switch then places the packets in the correct switch queue. The correct queue is determined by the QoS policy implemented by the network administrator.

# IEEE 802.1Q

The IEEE 802.1Q standard extends the Ethernet frame format by adding four bytes to the Ethernet packet header. See the following figure.

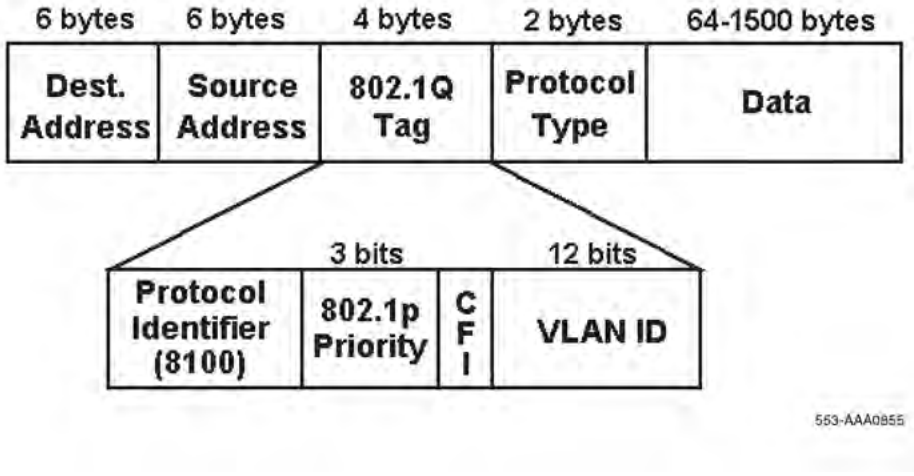


**Figure 5: Ethernet 802.1Q extensions**

The 802.1Q extensions contain two important fields – the 802.1p field and the VLAN ID field. Table 4: IEEE 802.1Q field definitions on page 52 lists the 802.1Q field names and definitions.

**Table 4: IEEE 802.1Q field definitions**

| 802.1Q field | Description |
|---|---|
| Tag protocol identifier | Always set to 8100h for Ethernet frames (802.3 tag format) |
| 3-bit priority field (802.1p) | Value from 0 to 7 that represents user priority levels (7 is the highest) |
| Canonical field | Always set to 0 (zero) |
| 12-bit 802.1Q VLAN ID | VLAN identification number |

## VLAN ID

A VLAN logically groups network devices into a single broadcast domain. Each VLAN has its own IP subnet. This ensures that devices on separate VLANs cannot communicate with each

other unless their traffic is routed. The routing enables traffic separation and isolation by creating separate broadcast domains.

VLANs provide a popular method of supporting QoS, using a Layer 2 (Ethernet) switching structure.

**Important:**

The routers must be compatible. Routers must support VLANs on their physical ports.

VLANs include advantages when applied to voice traffic on an IP network. VLANs enable packets with similar QoS requirements to be grouped together to receive the same QoS treatment.

After routing into a specific VLAN, configure the router interface to tag the incoming Layer 2 Ethernet frames with the correct VLAN ID and priority.

VLANs provide a useful way to separate and prioritize the IP telephony packets for Layer 2 switches. A telephony VLAN can be created so that all IP telephony devices are members. This enables the Layer 2 switch to prioritize all telephony traffic, so that it receives consistent QoS treatment.

**Important:**

A VLAN can only provide QoS on Layer 2 switches that support the 802.1Q (VLAN) standard. After the packets leave the Layer 2 switch, and encounter routers or WAN switches, DiffServ should be used to provide end-to-end QoS. Nortel IP Phones also mark the DSCP, so after voice packets encounter routers, the routers can be configured to prioritize the packets based on their DSCP value.

IP Phones 200x support IEEE 802.1Q using firmware version 1.39 or later. The default Ethernet Class of Service (CoS) is 0; this is the same as the 802.1Q priority bits.

The IP Phones 200x firmware tags the Ethernet frames with both the telephone VLAN ID and the 802.1p priority specified in Element Manager. Nortel recommends that you assign the 802.1p priority to 6.

The Nortel IP Softphone 2050 client support of IEEE 802.1Q priority depends on the underlying operating system and hardware.

### 802.1p user priority bits

The 802.1p field has three bits that provide eight Classes of Service (CoS). 802.1p-capable Layer 2 and Layer 3 switches use these CoS to prioritize packets, and then place them in different queues to provide service differentiation. For more information about configuring, see Configuring Quality of Service in Element Manager on page 228.

### 802.1p configuration

Use Configuring Quality of Service in Element Manager on page 228 to configure the 802.1p priority bits in Element Manager.

For more information about Element Manager, see *Element Manager System Reference — Administration , NN43001-632*.

## Port prioritization

You can configure a Layer 2 switch port to prioritize all packets that enter it, for example, in cases where IP Phones connect to a Layer 2 switch port not shared with other devices.

### 3-port switch port prioritization

IP Phones have an optional external 3-port Layer 2 switch module that is inserted into the bottom of the phone.

The IP phones have a built-in 3-port switch. The internal port is used by the IP phone. The two external ports provide connection to the network and another device (such as a PC).

The 3-port Layer 2 switch enables a PC and an IP Phone to share a single Ethernet connection. All packets entering the port connected to the IP Phone are given a higher priority than packets entering the port connected to the PC to ensure that all voice packets are sent ahead of any data packets. This has little effect on the data packets because the IP Phone packets are small and use little bandwidth.

This approach has limitations. For example, if a network user connects a PC to the IP Phone Ethernet port, the user can unfavorably take advantage of network resources. This situation can be prevented by ensuring that all packets that enter the port are also prioritized through MAC or VLAN ID classification to determine that they are from an IP Phone.

**Important:**

Nortel strongly recommends that, for stationary IP telephony devices, such as VoIP gateways, use port prioritization on the Ethernet switch port that connects to the device.

## Layer 3 QoS

DiffServ is the recommended Layer 3 QoS mechanism. Layer 3 IP devices (routers and Layer 3 switches) can classify IP Phone packets by using the following fields in the IP packet header:

- source/destination IP address
- DiffServ CodePoint (DSCP) (the 6 Most Significant Bits (MSB) in the 8-bit DiffServ field)

**Important:**

The values entered in the fields must be coordinated across the entire IP data network. Do not change the fields arbitrarily.

## IP address classification

A Nortel IP Phone obtains an IP address in one of two ways:

- DHCP is used to automatically obtain the IP address.
- the IP address is permanently assigned through the keypad.

To make it easier to prioritize packets by IP addresses, a pool of IP addresses can be assigned exclusively for IP Phones. The Layer 3 switch/router can then prioritize the packets based on this range of IP addresses by marking the voice packets from those designated IP addresses with the recommended DSCP.

This method does not differentiate between voice media and signaling packets. Only a single DSCP is used for both. However, if additional filters are applied to sort the different packet types, the voice media and signaling packets can be marked with different DSCPs.

## DiffServ for VoIP

DiffServ-based QoS at Layer 3 provides end-to-end QoS. By using DSCP, DiffServ enables service assignment to network traffic on a per-hop basis.

Figure 6: DiffServ-based QoS architecture on page 55 shows the architecture of DiffServ-based QoS.

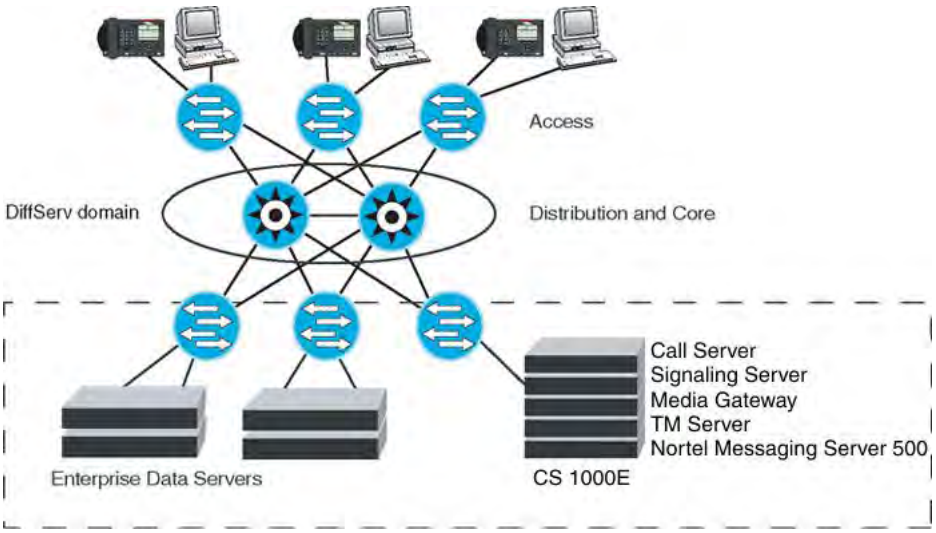


**Figure 6: DiffServ-based QoS architecture**

The DiffServ CodePoint (DSCP) is a 6-bit value contained in the second byte of the IPv4 header. See Figure 7: IPv4 header showing DSCP location on page 56. The DSCP determines the DiffServ Per Hop Behavior (PHB) treatment that the router/Layer 3 switch provides to the IP packets.

The DSCP is contained in the 8-bit DiffServ Field (DS Field), formerly known as the Type of Service (ToS) Field. Some routers use the ToS terminology instead of the DiffServ terminology. However, in either case, the six most significant bits in this field are the DSCP value. See Figure 7: IPv4 header showing DSCP location on page 56.

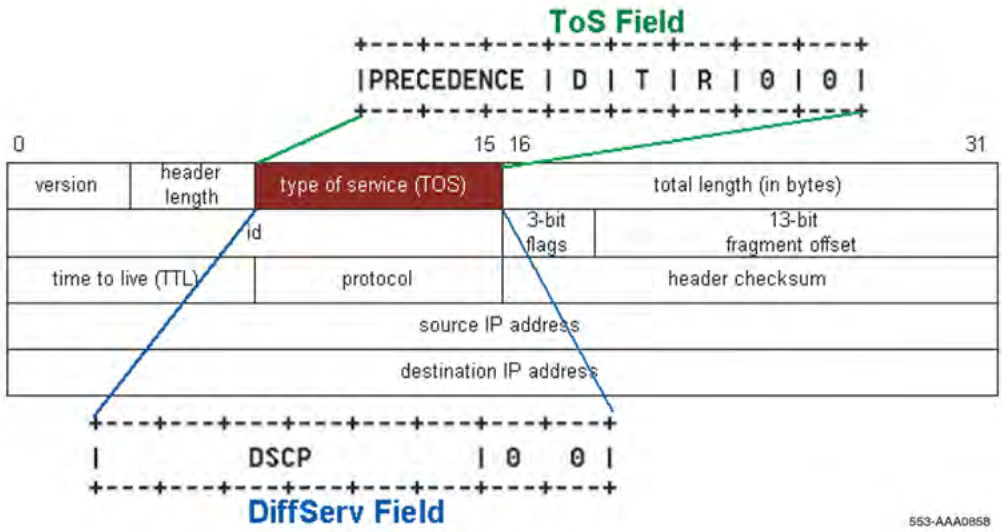


**Figure 7: IPv4 header showing DSCP location**

You can see the 8-bit value, rather than the 6-bit value, if you use a network analyzer to look at the DiffServ byte.

## Trust configuration

DiffServ edge routers and switch interfaces can be configured to trust or distrust a previously marked DSCP or 802.1p tagged packet. Voice packets that enter untrusted interfaces are remarked to a DSCP/802.1p value of 0 (best effort), unless filters are configured to classify the packets and mark them with the DSCP or 802.1p value specified by the network administrator. If the router and switch interfaces are configured as trusted interfaces, then the packets are not remarked and the premarked voice packets are prioritized based on their DSCP and 802.1p values.

A router can use the DSCP to queue premarked IP Phone packets if they arrive from a trusted source.

For example, a Layer 3 switch can have Ethernet ports assigned only to IP Phones. These ports can be configured to trust that the IP Phones marked the packets correctly.

## Voice signaling and media DSCPs

Over a high-bandwidth, low-latency Ethernet LAN connection, voice media packets and signaling packets can be placed in the same queue in the Layer 2 or Layer 3 switch. In this

case, it is not necessary to differentiate between voice media packets and voice signaling packets.

However, when the voice packets use a low-bandwidth (less than 1 Mbit/s) connection, considerable queueing delay can occur. This queueing delay, when coupled with the arrival of different sized voice packets (signaling and media), creates an unacceptable amount of voice jitter, which in turn results in poor voice quality.

To minimize voice jitter over low bandwidth connections, the voice media and voice signaling packets must be separated into different queues. By marking the voice media and voice signaling packets with a different DSCP, the packets can be classified and separated into different queues by the router connected to the low bandwidth connection.

**Important:**

It is important to categorize signaling packets so they are not discarded by the network. The IP Phone contains a watchdog timer that resets the IP Phone if signaling packets are not seen within a certain amount of time. Lost signaling packets can also cause the IP Phones to reset.

## Setting DSCP values

If a best effort network is currently in place, and VoIP is being added, the simplest approach is to create the network QoS with only three priority levels:

1. VoIP voice media traffic
2. VoIP signaling traffic
3. best effort IP data traffic

Routers connected to low bandwidth interfaces must separate voice media and voice signaling packets to minimize jitter introduced by the signaling packets to the voice media packets. Jitter occurs if the packets are placed in the same queue instead of separate queues.

IP packets are prioritized based on the DSCP in the distribution layer, core layer, and WAN.

DiffServ is supported on the Signaling Server, Voice Gateway Media Cards, and the IP Phones.

Table 5: Recommended DiffServ classes on page 57 shows the recommended DiffServ traffic classes for various applications.

**Table 5: Recommended DiffServ classes**

| Traffic type | DiffServ class | DSCP (binary) | DSCP (decimal) |
|---|---|---|---|
| Voice media | Expedited Forwarding | 101110 | 46 |
| Voice signaling | Class Selector 5 | 101000 | 40 |
| Data traffic | Default | 000000 | 0 |

**Important:**

If you use Sniffer, the values in a sniffer capture are 8-bit values. The EF DSCP can appear as 184 decimal. The CS5 DSCP can appear as 160 decimal.

The Nortel standard DSCP for signaling is decimal 40. The Nortel standard DSCP for voice is decimal 46, based on six bits of an 8-bit field. Two bits are unused. The DSCP is configured in Element Manager.

## Mapping DSCP to 802.1Q

Some switches, such as the Passport 8600 and Business Policy Switch, can map the DSCP to and from an 802.1p tag. See the following figure.

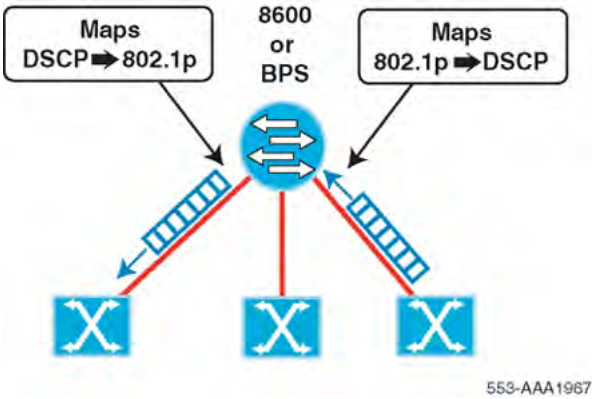


**Figure 8: Mapping DSCP to 802.1p**

This extends the IP QoS to Layer 2 QoS for the downstream Layer 2 switches that are not IP-aware. The Passport 8600 has a mapping table for DSCP to 802.1p. The Passport 8600 can map packets marked with EF and CS5 DSCPs to 802.1p user priority 110'. The downstream Layer 2 switch should be configured to place this 802.1p tag of 110 into its highest priority queue.

If a network administrator configured a different 802.1p tag for IP Phone packets, then packets tagged with this value should be placed in the highest priority queue of the Layer 2 switch. The network administrator must also ensure consistency in mapping the EF and CS5 marked packets to this 802.1p tag.

## Example

A network administrator can configure the IP Phone 2004 controlled by a Voice Gateway Media Card to mark the voice media packets with the EF DSCP, and the voice signaling packets with the CS5 DSCP.

The Passport 8600 routing switch trusts the premarked packets that enter ports configured as core ports. The Passport 8600 places these packets into the highest priority queue by default. The scheduler for this queue is preconfigured with a Packet Transmit Opportunity (PTO) or queue weight of 100%.

This configuration provides the necessary behavior required for IP Phone packets to achieve the required QoS.

## Element Manager QoS configuration

Use Element Manager to configure QoS for Communication Server 1000 systems.

Adhering to Nortel standards, the DSCP bits for VoIP control packets are configured to CS5, a decimal value of 40. The voice packets are configured to the EF decimal value of 46. By default, the Passport 8600 and BPS place the voice and control packets into the same queue.

For slower links (<1 Mbit/s), the control and voice packets marked with different DSCP values should be separated into different queues; otherwise, the voice packets experience significant queueing delays.

Figure 9: Voice Gateway Media Card DSCP configuration using Element Manager on page 60 shows DSCP configuration using Element Manager.

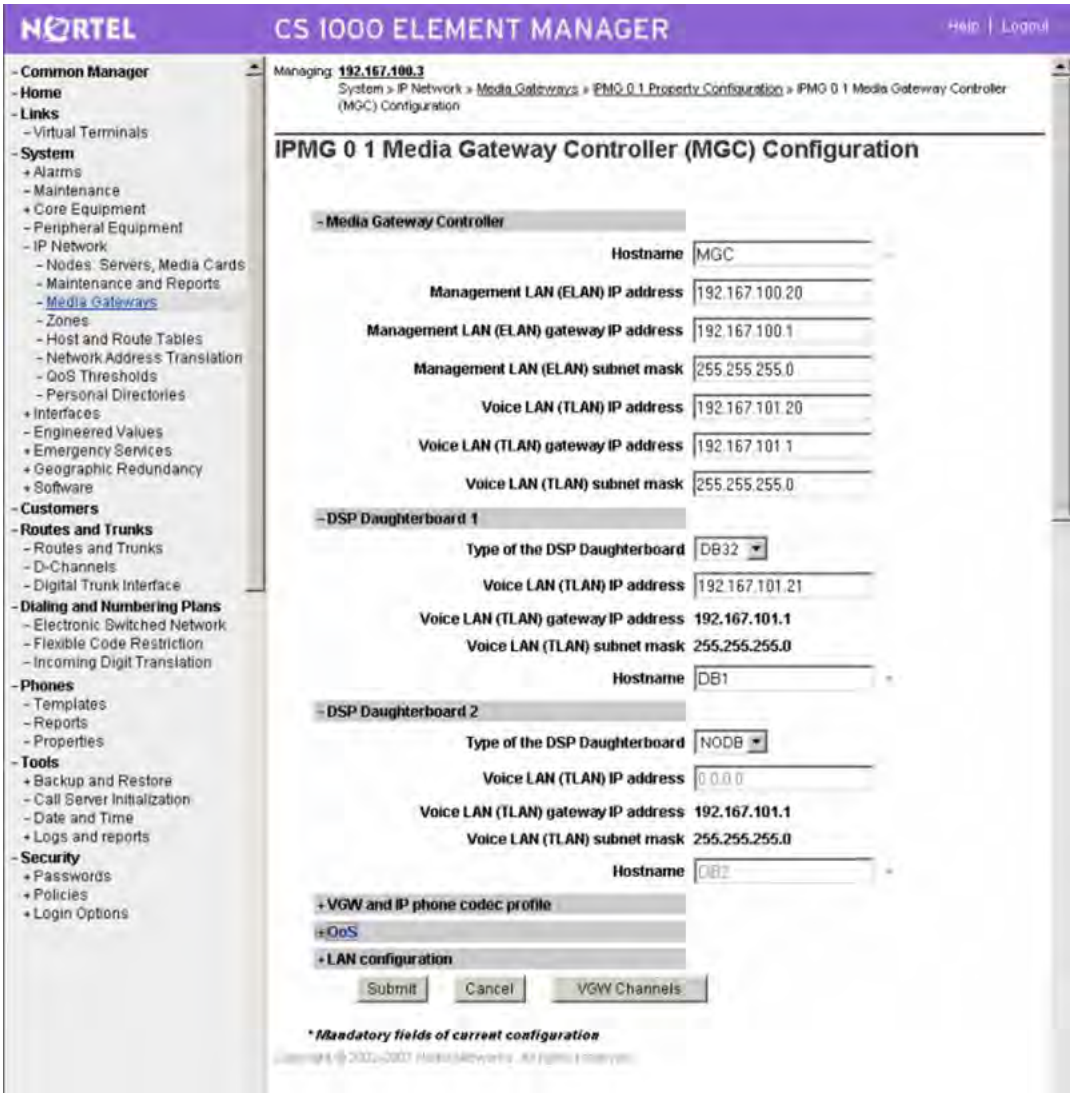


**Figure 9: Voice Gateway Media Card DSCP configuration using Element Manager**

For more information about configuring DiffServ values in Element Manager, see *IP Peer Networking Installation and Commissioning, NN43001-313*.

## Layer 4 (TCP/IP) classification

All Layer 4 IP devices can classify IP Phone packets by using the following fields in the packet header:

- source/destination TCP/UDP port number
- protocol ID

## Port number classification

UDP port numbers that use IP Phone RTP packets are dynamically assigned, which makes it difficult to classify packets by port number. However, if a specific range of port numbers is assigned to IP Phones, then the router recognizes that the packet came from a port number assigned to IP Phones and prioritizes the packet as a voice packet.

There is a disadvantage to using the previous method of prioritization. Another application can use the same port number range, causing its packets to be mistaken for voice packets and allowing packets to be assigned an incorrect QoS behavior and prioritization.

## Protocol ID classification

Many multimedia applications (for example, real-time fax and video, and voice) use the Real-Time Transport Protocol (RTP); therefore, prioritizing packets according to the protocol used does not provide accurate results.

## Communication Server 1000 and Meridian 1 ports

For more information, see Port number tables on page 321.

## Policy management

You can prioritize traffic through policy management, which Nortel supports through ENMS Policy Services software.

## ENMS Policy Services

ENMS Policy Services (OPS) is network management software that the network administrator can use to prioritize and manage different types of network traffic. OPS 2.0 is designed to manage policies on the BPS and Business Communication Server (BCM). To manage BayRS, Accelar, and Passport devices, OPS 1.1.1 must be installed.

For more information about configuration examples, see DHCP supplemental information on page 391.

## Codec selection

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

The Call Server considers BQ codec as G.711 and BB as either G.729 or G.723 (assuming that both parties support it).

Each codec has specific parameters that must be configured, such as packetization delay and voice activity detect. These parameters are configured on the Signaling Server using Element Manager. For more information, see Element Manager on page 209.

Ensure the voice codec images on all sites match by using the same software version at each site. Use the same codecs, packetization, and jitter buffer settings on each system.

There is a potential to degrade the voice quality if codecs are cascaded. This can occur when there are multiple compression and decompression stages on a voice call. The more IP links used in a call, the more delay is added, and the greater the impact on voice quality.

The following applications and devices can impact voice quality if you use a compression codec, such as G.729A:

- Voice mail, such as Nortel CallPilot, introduces another stage of compression and decompression.
- Conferences can double the number of IP links.
- IP Trunks can add additional stages of compression and decompression.

**Important:**

Nortel recommends that all cards in a system have the same image. If multiple codec images are used in an VoIP network, the calls default to the G.711 group when the originating and destination codecs differ.

If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

For more information about codecs, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

## Protocols in use

When you assess the network for VoIP readiness, observe the distribution of protocols in the network, specifically on the WAN. Tools available for this task include Network Management Systems (NMS), which can poll devices through SNMP probes, remote monitoring (RMON) probes, or both, and analyze the results.

## Routing protocols

It is important to note the routing protocols used within the network, as they can affect network availability.

## LAN protocols

Routing protocols in the LAN must be considered when implementing VoIP.

## WAN protocols

Routing protocols in the WAN can be very important when you consider how VoIP calls are routed and how quickly fail-over occurs. When you plan a VoIP network, be aware of the situations that trigger a routing table update with respect to the routing protocol. This helps when you predict what path a VoIP flow might take during a failure in the network.

## Convergence

Convergence is the point where all internetworking devices have a common understanding of the routing topology. The time it takes a network to reconverge after a link failure must be considered, as the process might take several minutes depending on the network size and routing protocol in use.

## Mixing protocols

VoIP performance can be impacted if a network is using multiple protocols on any particular segment.

For example, even with fragmentation implemented, if there are protocols in use other than IP, those protocols can maintain larger frame sizes. This can introduce additional delay to the VoIP traffic.

It is important to be aware that certain applications that run over IP can configure the frames with the fragment bit to 1 to prevent fragmentation. As part of the overall assessment process, the network analysis on the LAN can determine if applications include this bit setting.

## Security and QoS

The following security features must be considered.

- firewalls
- Network Address Translation (NAT).
- Secure Virtual Private Network (VPN) access through Secure Internet Protocol (IPSec) encryption.

Routers might use NAT and IPSec for remote network users who connect to the network through the public Internet. A firewall connection could also exist. The network designer must consider the security policy in force and determine if the ports required for VoIP can go through the firewall.

For more information about security management, see *Security Management , NN43001-604*.

# IP network best practices

This section describes IP network engineering best practices.

## Fallback to PSTN

It is possible to automatically fall back to PSTN, if calls cannot be completed due to loss of connectivity between sites over the IP network. This is achieved using the standard Meridian Customer Defined Network (MCDN) Alternate Routing feature when:

- the IP network is down
- the destination IP Peer endpoint is not responding
- the destination IP Peer endpoint responds that there are no available IP Peer trunk resources
- the destination IP Peer endpoint is not registered with the Networking Routing Service (NRS)
- there are address translation errors
- all Virtual Trunks are busy at the originating sites
- all bandwidth configured for a bandwidth zone has been allocated
- Quality of Service (QoS) metrics cause a reduction in available bandwidth

Fallback to PSTN can be configured by programming an alternate route entry after the virtual IP trunk route entry in RLB in LD 86 and entering RRA at the SBOC prompt for the virtual IP

trunk entry. For the configuration of RLB in LD 86, see *Software Input Output Reference — Administration (NN43001-611)*.

Fallback to PSTN for IP Peer Networking refers to the use of the MCDN Alternate Routing feature to step back to an alternate switched-circuit trunk route to the destination that the call first attempted to reach by the IP Peer virtual IP trunk route.

The alternate switched-circuit trunk route can include any of the following:

- a direct ISDN PRI tie trunk route
- a Virtual Private Voice Network tie trunk route using a common carrier voice network
- a PSTN trunk route

**Important:**

If fallback to PSTN uses PSTN trunks as the alternate route, then the appropriate ESN digit manipulation features must be implemented to convert the dialed number from on-net to off-net, or from private to public E.164 format.

If fallback to PSTN uses PSTN trunks as the alternate route, Nortel recommends that you configure both the original and alternate trunk routes as en bloc capable or overlap capable.

A similar feature, Alternate Call Routing for Network Bandwidth Management is available to provide alternate routing between a branch office (or Survivable Remote Gateway [SRG]) and a main office. For more information, see Alternate Call Routing for Network Bandwidth Management on page 33.

## Best IP network engineering practices for IP Telephony

In general, the best IP network engineering practices for IP telephony remove the requirement for QoS fallback to PSTN. Best practices include

- the implementation of network QoS features such as DiffServ and 802.1Q to give priority to real-time voice traffic
- the fragmentation of large data frames to limit the maximum frame size on low speed WAN links and limiting the quantity of voice traffic that is transmitted over low speed links

When QoS fallback to PSTN is required for specific network locations (in an IP Peer network) because WAN links have not been engineered according to best practices, IP Trunk 3.0 (or later) can be used to achieve QoS fallback to PSTN between those locations and an IP Peer node located on the IP network backbone. An IP Trunk 3.0 (or later) node must be configured in the same Communication Server 1000 system with the IP Peer node.

## Considerations for using IP Trunk to achieve QoS fallback to PSTN

If you use IP Trunk 3.0 (or later) nodes to provide QoS fallback to PSTN in an IP Peer network, you must consider specific engineering and network management trade-offs:

- QoS fallback to PSTN only works between symmetrically configured pairs of IP Trunk nodes. QoS fallback to PSTN does not work between an IP Trunk node and an IP Peer node. Each IP Trunk node in a symmetrically configured pair must have QoS fallback to PSTN enabled for the opposite destination node.
- A pair of symmetrically configured IP Trunk nodes must each have a local Dialing Plan entry in the IP Trunk node that points to these opposite IP Trunk nodes. The Gatekeeper cannot be used for IP Trunk destinations symmetrically configured to enable QoS fallback to PSTN.
- An IP Trunk node configured in a Communication Server 1000 system with an IP Peer node does not support the Direct Media Path feature of IP Peer Networking. All IP Trunk calls that originate or terminate at a network location that requires QoS fallback to PSTN must have a tandem media path connection through the Communication Server 1000 IP Peer node. The tandem media path can occasionally cause voice quality degradation due to multiple transcoding and higher end-to-end latency of the voice conversation.

For more information, see *IP Trunk Fundamentals, NN43001-563* and *Basic Network Feature Fundamentals, NN43001-579*.

## Alternate circuit-switched routing

The following scenario describes alternate circuit-switched routing when there is an IP network outage.

An IP network outage occurs at Site B.

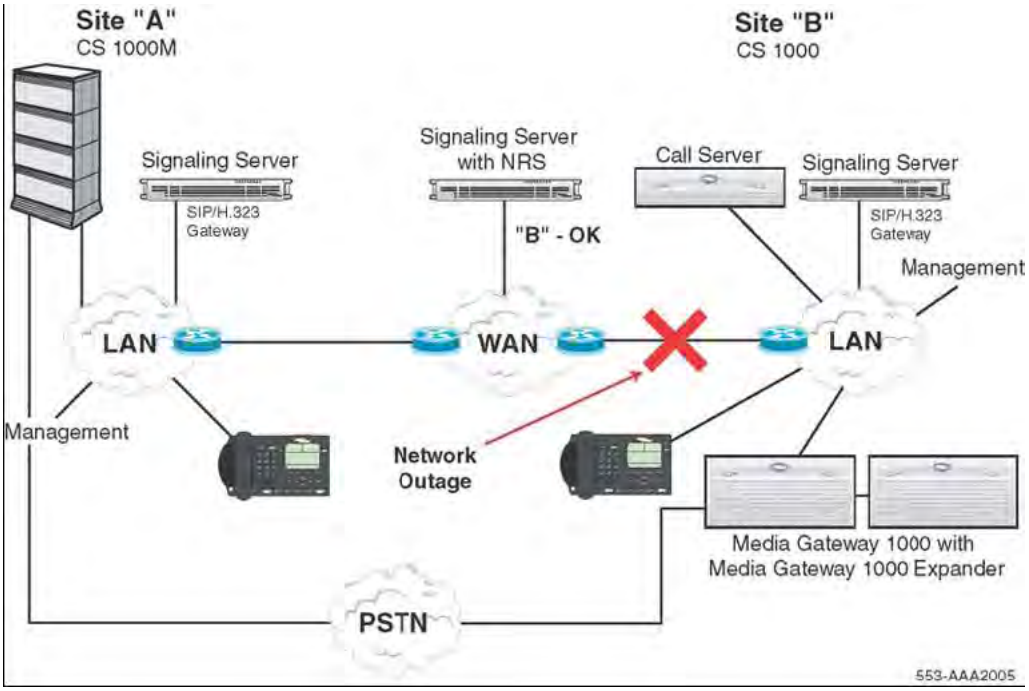


**Figure 10: IP network outage at Site B**

The registration of Site B times out at the NRS; the status updates.

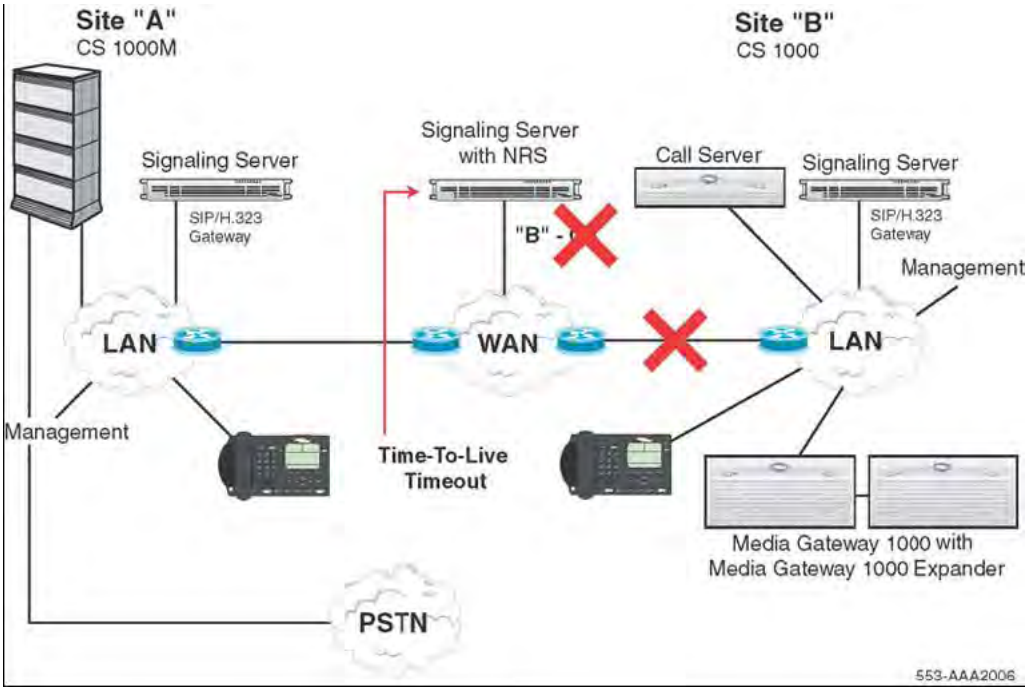


**Figure 11: Registration at Site B times out**

User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the dialed digits through the Terminal Proxy Server (TPS) on the Signaling Server.

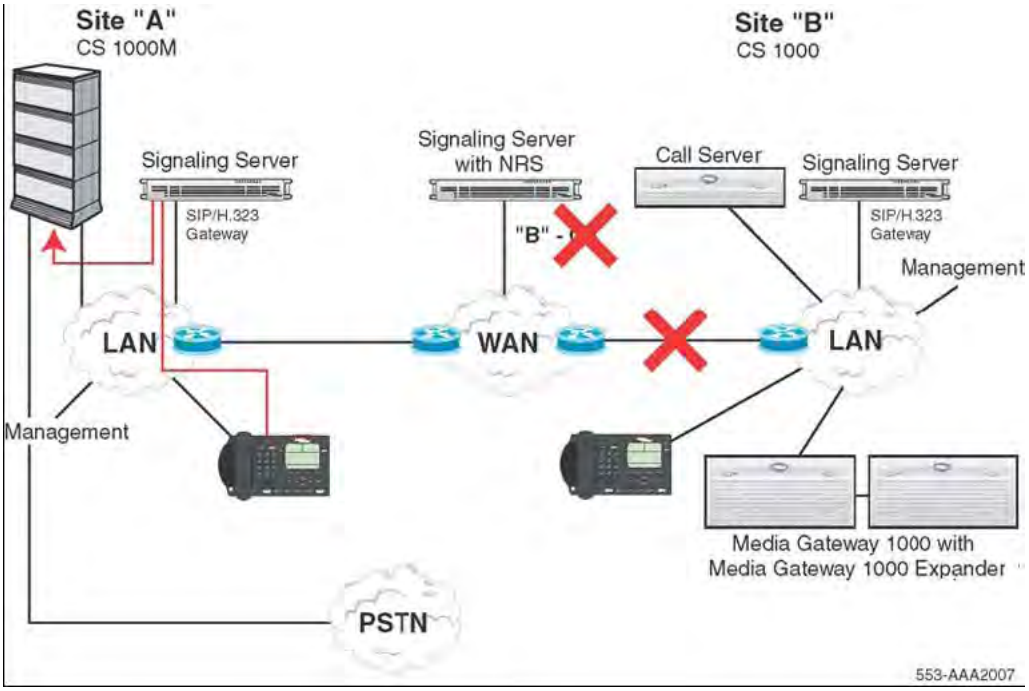


**Figure 12: User A dials User B**

Call Server A determines that the DN is at another site. Call Server A selects the codec list, allocates bandwidth, and routes the call to the IP network, using a virtual trunk and the SIP/H.323 Gateway.

To select the virtual trunk to use for routing, Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

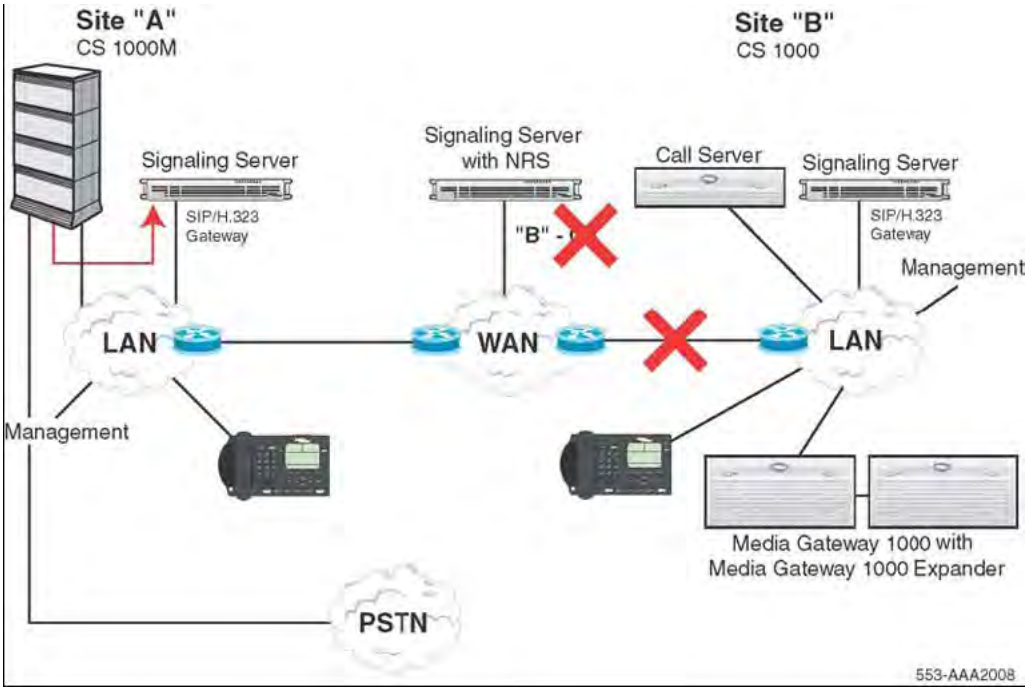


**Figure 13: Call Server A routes the call to the IP network**

SIP/H.323 Gateway A asks the NRS to search for a dialed DN in the database (for example, within the appropriate CDP domain). The NRS replies that no SIP/H.323 Gateways are available for the dialed number.

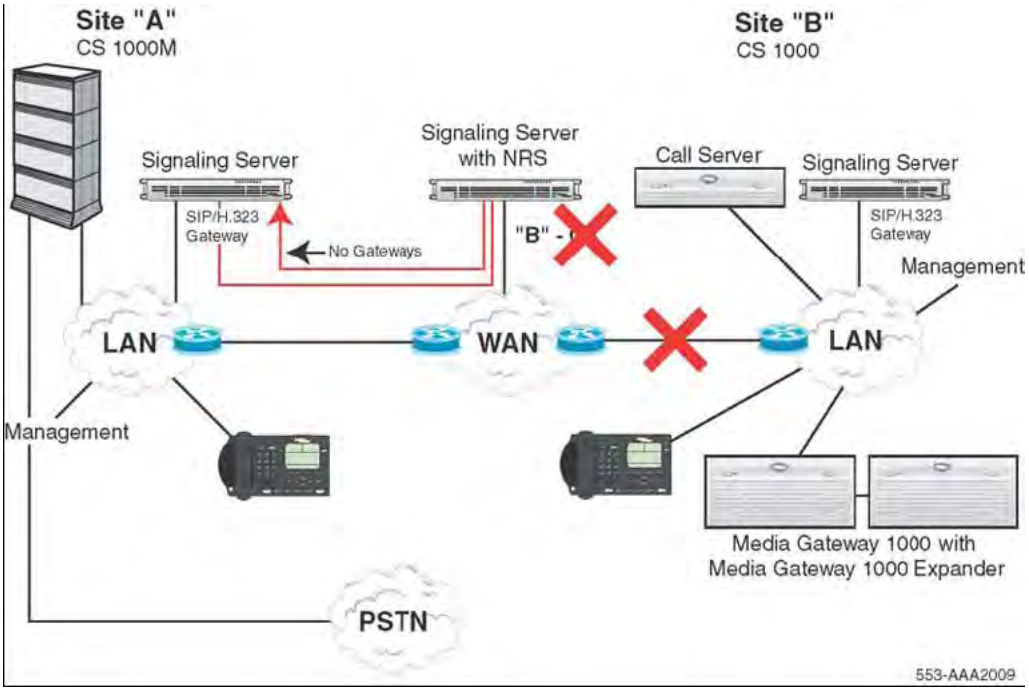


**Figure 14: No SIP/H.323 Gateways are available for the dialed DN**

SIP/H.323 Gateway A replies to Call Server A with a message that all IP trunks are busy for the dialed DN.

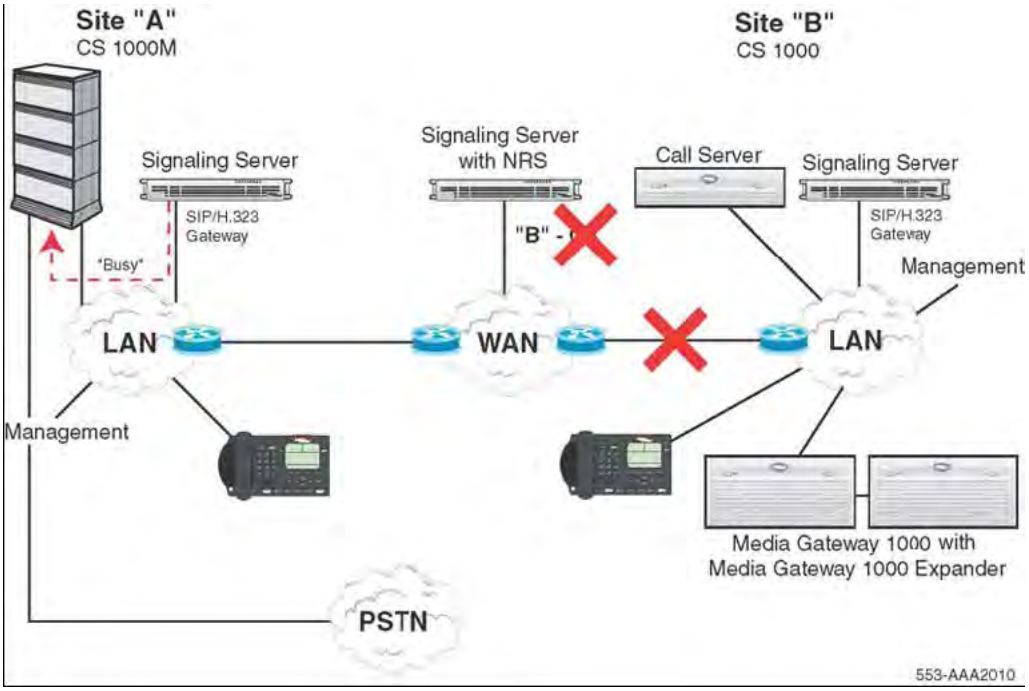


**Figure 15: SIP/H.323 Gateway A replies to Call Server A**

Call Server A chooses the next route in the Route List Data Block. The next route is a local PSTN trunk route. Call Server A allocates a Voice Gateway Media Card and PRI channel. Digit manipulation is applied to the route using the local PSTN. A successful call is made.

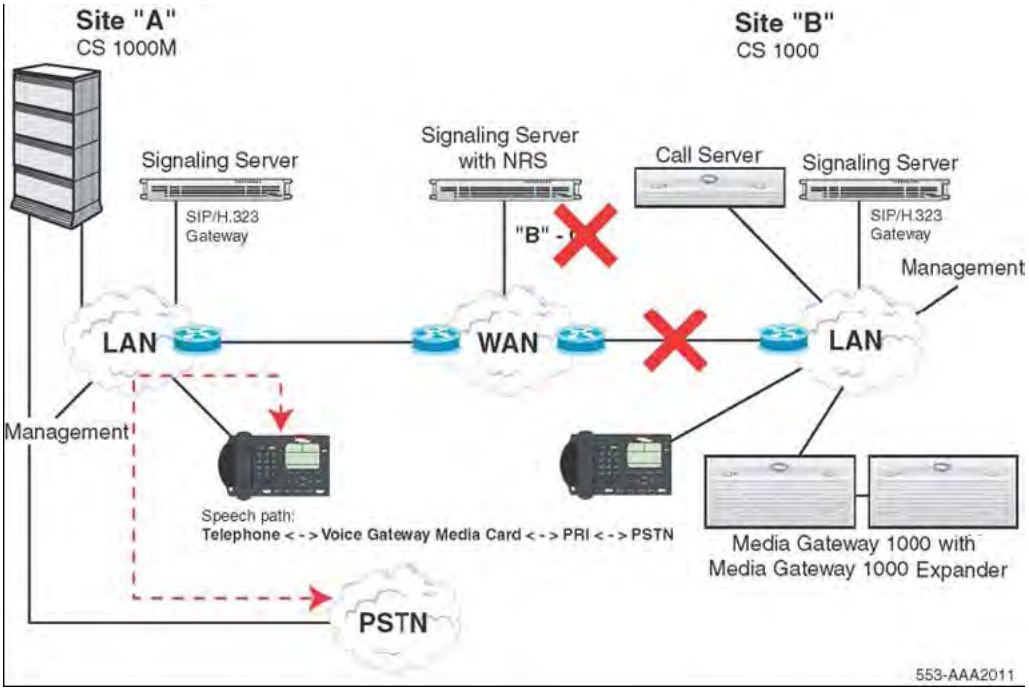


**Figure 16: Call Server A chooses the next route in the Route List Data Block**

The call is routed across PSTN and enables the users to talk to each other. The call is terminated over PSTN to Site B.

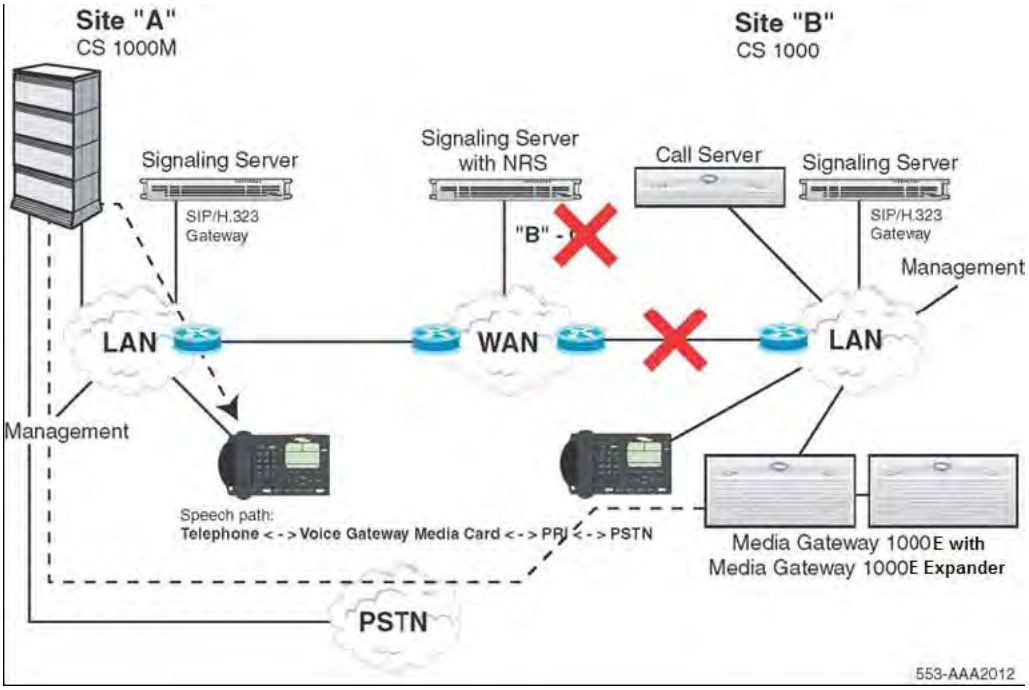


**Figure 17: Call is terminated over PSTN**

# Bandwidth Management

This section describes how the Bandwidth Management feature works, and is useful when considering how to engineer a network of Call Servers.

## VoIP Bandwidth Management zones

Bandwidth Management zones divide IP Phones and Voice Gateway Media Cards into logical groups (zones) to determine codec selection and Bandwidth Management. Zones are configured after the QoS managed IP network has been designed.

As calls are made, the Call Server software chooses a codec to be used for the call based on the zone configuration (interzone or intrazone). The software also tracks bandwidth usage within each zone and between zones. When making an interzone call, the codec is selected according to interzone policy. This policy is a configurable value and can be configured to BQ or BB.

Each IP Phone and Voice Gateway Media Card port is assigned a zone number in which it resides. Place all IP Phones and Voice Gateway Media Cards at a site in the same zone (for example, configure IP Phones and Voice Gateway Media Cards at the same branch office in the same Media Gateway 1000B [MG 1000B] zone).

Virtual Trunk routes also allow configuration of a zone. A single Call Server considers calls sent from a Virtual Trunk as terminated on that Virtual Trunk. Therefore, Virtual Trunks should not be in the same zones as any IP Phones or Voice Gateway Media Cards.

Place all virtual trunk routes in the same zone for all main office and MG 1000B systems. Virtual trunk zones are not for Bandwidth Management except when they connect to a third-party gateway. Configure virtual trunk intrazone and interzone policy to Best Quality (BQ) and intrazone and interzone bandwidth to the maximum value of 1 Gbit/s (1 000 000 kbit/s). Bandwidth is already managed within the IP Phone zone.

Bandwidth management zones can be network-wide but this is dependent on your VPNI setting and zone number. If the VPNI setting and zone number match on the originating system and terminating system the call servers will treat the call as INTRAZONE, even though its traversing between those two systems. The following table captures the different cases of VPNI settings and zone numbering.

| Originating VPNI | Originating Zone | Terminating VPNI | Terminating Zone | Choose policy |
|---|---|---|---|---|
| 1 | 100 | 1 | 100 | INTRAZONE |
| 1 | 100 | 1 | 150 | INTERZONE |
| 1 | 100 | 5 | 100 | INTERZONE |
| 1 | 100 | 5 | 200 | INTERZONE |

MG 1000B zones should be configured on the MG 1000B and main office systems. The MG 1000B zones only contain equipment located at that branch office. The information configured for the zone should be identical in both the main and MG 1000B configuration. Main office Zone information does not have to be entered into all MG 1000Bs.

Zone properties are defined in LD 117. A maximum of 8001 zones can be configured. The systems use the zones for Bandwidth Management. New calls are blocked when the bandwidth limit is reached.

Each Zone includes the following parameters:

- IntraZoneBandwidth which is defined as the total bandwidth available for intrazone calls
- IntraZoneStrategy which is defined as the preferred policy for the choice of codec for intrazone calls (preserve best quality or best bandwidth)
- InterZoneBandwidth which is defined as the total bandwidth available for interzone calls
- InterZoneStrategy which is defined as the preferred strategy for the choice of codec for interzone calls
- ZoneIntent which determines whether the Zone is part of the main office, a branch office (Media Gateway 1000B [MG 1000B]), or a Virtual Trunk.
- ZoneResourceType which is either shared or private. Resources in private zones are accessible to users in the same Zone. This allows resources, such as DSPs, to be reserved for users in the private Zone.

For more information about Bandwidth Management Zone commands, see Table 50: LD 117 – Configure Bandwidth Management zone on page 233.

The intrazone and interzone bandwidth is entered in kbit/s (for example, 2.7 Mbit/s equals 2700 kbit/s). Each bandwidth zone must have the intrazone and interzone bandwidth values entered.

Zone 0 operates as a default zone when there are no IP voice zones configured in LD 117. Zone 0 can then be configured as a default zone for ITG Physical TNs (IPTN) in LD 14 and for virtual line in LD 11. However, if additional zones are required by an IP Phone or IPTN, zone 0 must be configured first

**Important:**

When you move an IP Phone, the system administrator checks and changes, if necessary, the zone assignment of the telephone in LD 11. See *Software Input Output Reference — Administration (NN43001-611)*.

**⚠ Caution:**

Zone 0 must be configured in LD 117 before other zones are configured or all calls associated with Zone 0 are blocked.

Do not configure endpoints in bandwidth Zone 0 if you plan to use Network Bandwidth Management. Configure Zone 0, but do not use it. Ensure that no endpoints (for example, IP Phones, VGWs, or virtual trunks) exist in Zone 0.

**⚠ Caution:**

It is possible that the Bandwidth Management zone is already provisioned for IP Phones, Virtual Trunks, and/or VGW for your network even though they do not exist in LD 117. This

can occur when upgrading from a release prior to version 4.5 to a new release greater than version 4.5. New installations of Communication Server 1000 release 4.5 can catch and prevent the above scenario as the Bandwidth Management feature is enhanced. It is still mandatory to configure all zones (once only) that are used for upgrades to release 4.5 and higher. Release 4.5 and higher upgrades convert the old database to a new release database but do not create non-existent zones. If the zones are not configured, using non-existent zones in call processing can result in blocked calls.

## Relationship between zones and WLAN sets

The existing Communication Server 1000 software bandwidth management mechanism, using bandwidth zones, applies to the handsets in the same manner as it does for IP Phones.

For more information see, *WLAN IP Telephony Installation and Commissioning, NN43001-504*

## Interzone versus Intrazone

For Bandwidth Management, a network of Call Servers is divided into zones, typically one Zone for each Call Server. Calls between zones are interzone calls and calls within a Zone are intrazone calls. Typically, intrazone calls travel over LANs on which bandwidth is widely available. Conversely, interzone calls travel over WANs on which bandwidth can be limited and expensive. Distinguish between intrazone and interzone VoIP calls for increased control over VoIP traffic.

The following call scenarios describe how each call type works.

### Intrazone call

An intrazone call works as follows:

- An intrazone call is made between two endpoints on the same Call Server.
- The intrazone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.
- Based on the intrazone treatment, the correct codec is selected.
- The intrazone bandwidth table is also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked.

### Interzone call

An interzone call works as follows:

- An interzone call is made between two Call Servers.
- An interzone call is made between an endpoint in one Zone to another endpoint in a different Zone. The Zone of the endpoints are compared to the Virtual Trunk Zone as the two zones are different, the call is an interzone call.
- The interzone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.

- Based on the interzone treatment, the correct codec list is selected for the call setup. For more information about codec selection, see Codec selection on page 62.
- The interzone bandwidth table and the virtual trunk bandwidth limit are also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked, or alternate treatment is provided.

# Nodal Bandwidth Management

Bandwidth Management is controlled independently on each Call Server in the network. Each Call Server acts independently of other Call Servers in the network when calculating bandwidth used, and when blocking or rerouting calls. Often referred to as nodal Bandwidth Management, each node, or Call Server, independently controls the Bandwidth Management. Therefore, the parameters used in configuring Bandwidth Management must be configured on each Call Server.

The Bandwidth Management at the branch office is controlled by the associated main office. For the main office to keep track of the bandwidth going to and from the branch office, calls must tandem through the main office Call Server. The signaling for the call goes through the main office, but the media path is not direct between endpoints.

# VPNI and Zone numbers

## Network Bandwidth Zone

For Network Bandwidth Management to work correctly in a Communication Server 1000 network, each Call Server must be configured with a unique Network Bandwidth Zone. You can choose from 8000 (1 to 8000) Zone numbers in a Communication Server 1000 Call Server. To allow the network to expand beyond the 8000 zones, the Virtual Private Network Identifier (VPNI) is combined with the Zone number to form a unique Network Bandwidth Zone. The Communication Server 1000 system allows up to 16 383 VPNIs, which result in a total of 131 064 000 unique Network Bandwidth Zones. A Call Server typically has one VPNI and one Zone number for IP Phones and IP gateways. For example, Call Server A is provisioned with VPNI 53 and Zone 21. Each IP Phone has two zone properties—configured zone and current zone. Configured zone is the zone chosen by the administrator and current zone identifies who the zone IP Phone currently belongs to based on the VO login. For more information, see Bandwidth Management support for Network Wide Virtual Office on page 259.

**⚠ Caution:**

Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.

**Important:**
Zone 0 is not supported by most of the Network Bandwidth Management features.

### VPNI and Zone numbering rules

If bandwidth zone numbers are duplicated on different call servers with the same VPNI then the calls will receive INTRAZONE call treatment. If you need to ensure INTERZONE call treatment then you to need ensure bandwidth zone numbers are not duplicated.

Branch office Call Servers associated with a main office must have the same VPNI number as the main office for correct operation of the Network Bandwidth Management feature.

For a branch office associated with a main office, the branch office Zone number must be different than the main office Zone number. For example, MO VPNI=22, MO Zone=33, BO VPNI=22, BO Zone=34. The branch office Zone number is provisioned at both the branch office and the main office; configured in LD 117 on the main office and MG 1000B.

The VPNI is also used to identify a customer network. For example, the same VPNI is required for Bandwidth Management support for the Network Wide Virtual Office and Alternate Call Routing features, and Geographic Redundancy.

The provisioned Zone number is also used for other features in the Communication Server 1000 network. For more information, see *.Emergency Services Access Fundamentals, NN43001-613*

## Relationship between zones and subnets

IP Phones and Voice Gateway Media Cards gateway ports are assigned to zones based on the Bandwidth Management requirements of the particular installation. Devices in different subnets must traverse a router to communicate and can reside on different ends of a WAN facility. When IP Phones and gateway ports are in different subnets, the network facilities between them must be examined to see if it warrants placing the separated devices in different zones.

It is not necessary to always assign different zones. For instance, there can be different subnets within a LAN interconnected by routers with sufficient bandwidth. The IP Phones, and gateway channels spread across them, could all reside in a single zone. However, if there is a WAN facility with limited bandwidth exists between two subnets, the devices on the opposite ends should be placed in different zones so the bandwidth across the WAN can be managed.

For remote users, such as telecommuters, Bandwidth Management is not normally a consideration because only one IP Phone is present at the remote location. It can be convenient to allocate zones for users with similar connection speeds. In these situations, configuration both the interzone and intrazone codec to Best Bandwidth.

### Disabling Bandwidth Management

Bandwidth Management may be disabled by provisioning the VPNI to 0 in LD 15. The local Bandwidth Management feature will continue the codec calculation process and call blocking, therefore; you must configure the Bandwidth zones with the maximum available bandwidth.

Provision the Intrazone bandwidth limit and Interzone bandwidth to the maximum (1 Gbit/s or 1 000 000 kbit/s) in LD 117. By default, the Virtual Trunk is configured with the maximum bandwidth limit.

Nortel recommends that you do not mix enabled and disabled Bandwidth Management zones in the network.

## Adaptive Network Bandwidth Management

The Adaptive Network Bandwidth Management feature enhances the performance of VoIP networks based on real-time interaction. It provides the means to automatically adjust bandwidth limits and take corrective action in response to QoS feedback. The dynamic bandwidth adjustment maintains a high level of voice quality during network degradation.

The Adaptive Network Bandwidth Management feature dynamically adapts to QoS in the network and reduces the bandwidth available for interzone calls if QoS degrades. Typically, each Call Server in the network has a Zone assigned to it. The Call Server keeps track of the bandwidth being used between its own Zone and zones that belong to other Call Servers. If the QoS degrades between the Call Server Zone and a particular Zone that belongs to another Call Server, the available bandwidth reduces automatically between those two zones. When the QoS between the two zones improves, then the bandwidth limit returns to normal.

When an IP Phone encounters degradation of the network, it informs the Call Server through various QoS alarms (packet loss, jitter, delay; and, for phase 2 IP Phones, R value). Depending upon the rate of the incoming alarms and the value of the alarms, the Call Server reduces the available bandwidth to make new calls. The Call Server lowers, limits, or both the number of new calls allowed, based on the available bandwidth to prevent excessive calls on a network with limited bandwidth (resulting in poor voice quality). After the adjusted (lowered) bandwidth reaches its full capacity, new calls are either routed to an alternate route (if available), using Network Alternate Routing Service (NARS) or the Alternate Call Routing for the Network Bandwidth Management feature, or new calls are blocked. The Call Server continues to monitor the network throughout the network degradation period. When the degradation is removed or the performance of the network improves, the allowable bandwidth returns to provisioned levels and the Call Server gradually starts to allow new calls.

Essentially, Adaptive Network Bandwidth Management provides a fallback to PSTN on QoS degradation for new calls. As a result, bandwidth is managed and quality measured between all zones across the entire network, and corrective action taken when necessary. Due to the real-time interaction with the network, less maintenance is required for the network as the system reacts automatically to network conditions.

With Adaptive Network Bandwidth Management, it is not necessary to provision bandwidth parameters between every Zone in the network. Rather, the Call Server automatically learns

of new zones in the network and applies Adaptive Network Bandwidth Management to these new zones as required. As new Call Servers are added to the network, it is not necessary to reprovision all the other Call Servers on the network. Conversely, when Call Servers are removed from the network, the remaining Call Servers age out the old Call Server information and provide only up to date bandwidth information.

The Adaptive Network Bandwidth Management feature operates between all IP Peer Communication Server 1000 systems, including the Media Gateway 1000B and Survivable Remote Gateway 50.

## Call scenario

A call is requested from a telephone in VPNI 1/Zone 2 on Call Server A to a telephone in VPNI 3/Zone 3 on Call Server B. Both zones have Adaptive Network Bandwidth Management enabled.

1. Call Server A contacts the Network Redirect Server to obtain the address of Call Server B.
2. Call Server A sends a call setup message to Call Server B, identifying the calling telephone's VPNI and Zone.
3. Call Server B determines if there is sufficient bandwidth for the call, and sends back the VPNI and Zone of the called telephone.
4. Call Server A checks its bandwidth table to determine if there is sufficient bandwidth available for the call from Call Server A to Call Server B.
5. If Call Server A determines there is enough bandwidth available, the call is established; otherwise, alternate treatment is provided (block or reroute the call).

Both Call Server A and Call Server B must consult their own bandwidth tables to determine if there is enough bandwidth for the call to proceed.

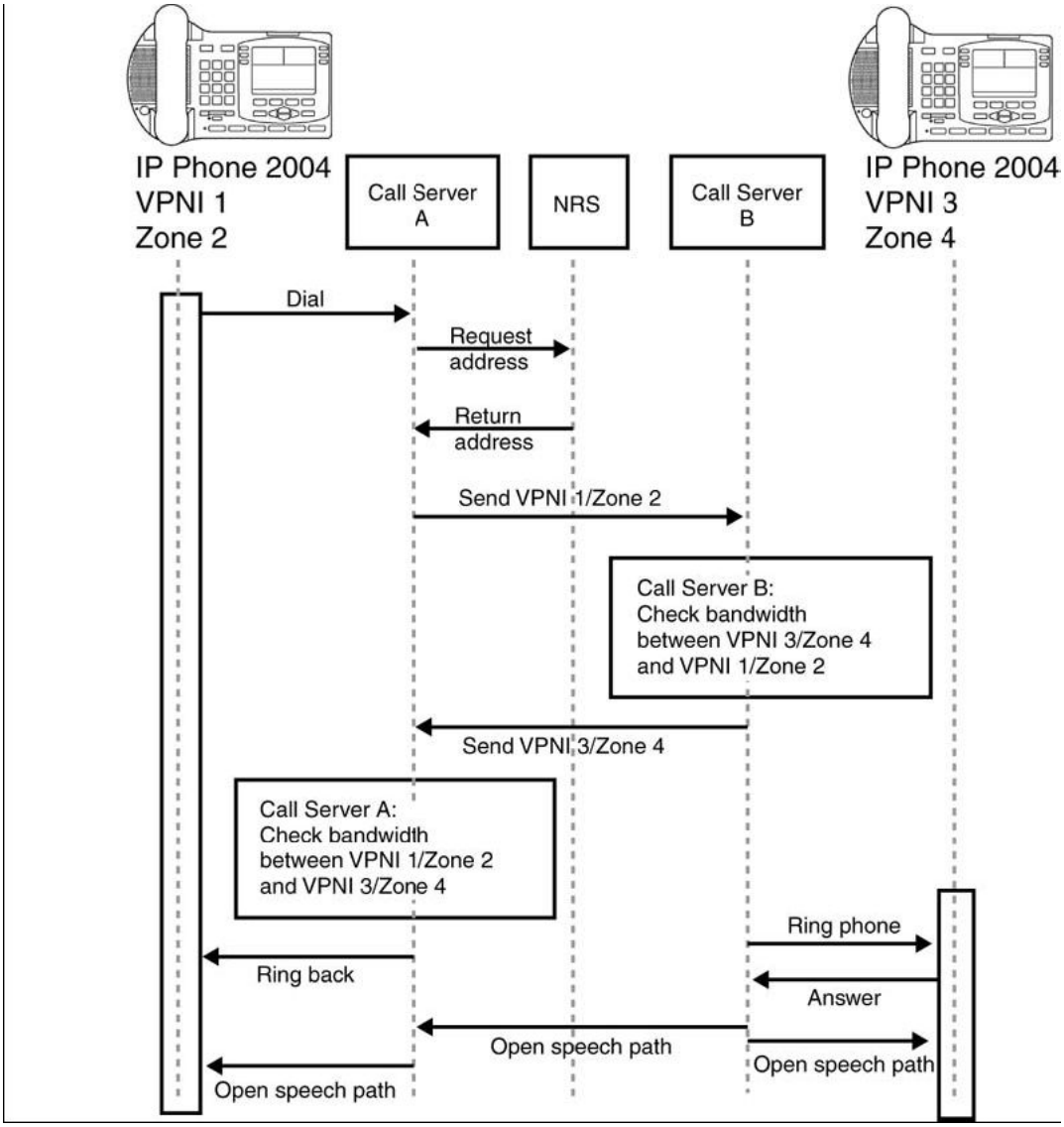


**Figure 18: Call Progress with Adaptive Network Bandwidth Management**

## Zone Bandwidth Management and Adaptive Network Bandwidth Management

Using Element Manager or the command line interface (CLI), previously configured zones (except Zone 0) can have the Adaptive Network Bandwidth Management feature turned on or off. After turned on, alarm threshold levels and the QoS coefficients can be adjusted from the default values. Adaptive Network Bandwidth Management cannot be enabled for Zone 0.

When Adaptive Network Bandwidth Management is enabled for a particular Zone on the Call Server, the Zone appears in the Zone table. The Zone table can be displayed using Element

Manager or LD 117. When a call is made from the configured Zone to another Zone, the bandwidth used appears in the Zone table.

When a call is made from a Zone with Adaptive Network Bandwidth Management enabled to a third-party gateway with no Zone, the Zone of the Virtual Trunk (VTRK) is used and appears in the Zone table.

Figure 19: Adaptive Network Bandwidth Management graph on page 81 depicts an example of bandwidth changes.

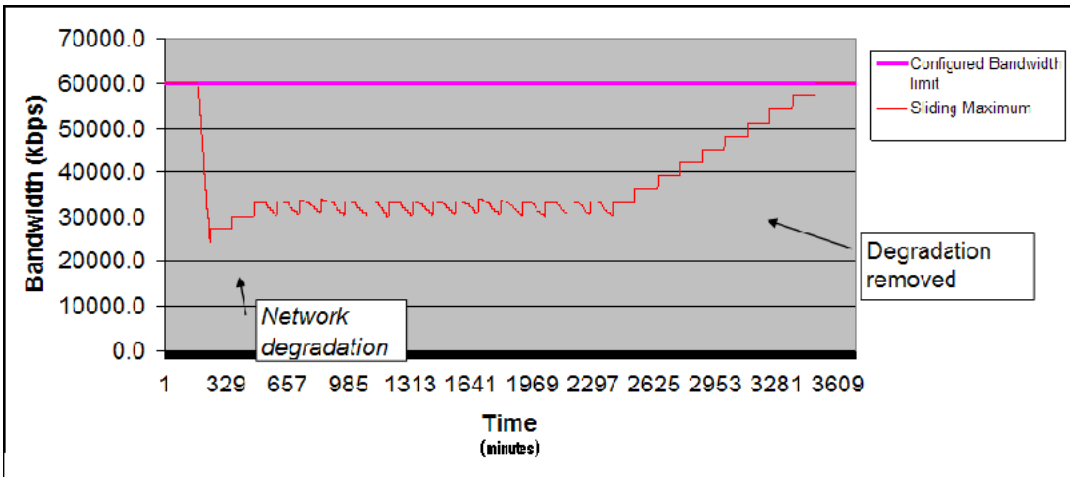


**Figure 19: Adaptive Network Bandwidth Management graph**

When a Call Server receives a QoS alarm, the two zones that originated the alarm are determined. Using this information, the Call Server reduces the bandwidth limit between the two zones. This Zone-to-Zone bandwidth limit (in effect at any particular time) is known as the Sliding Maximum Bandwidth Limit and is a percentage of the Configured Interzone bandwidth limit. The Sliding Maximum value is displayed using the prt interzone command. The QoS Factor % value is also displayed as the percentage of the Sliding Maximum versus the configured allowable bandwidth. The Call Server checks the Network Bandwidth Zone management tables for the originating and terminating zones of the new call to determine the available bandwidth for the call.

For more information about alarms, see *Software Input Output Reference — System Messages, NN43001-712*.

When feedback indicates a significant QoS change in a Zone, the Call Server reduces the available bandwidth (Sliding Maximum Bandwidth Limit) in the Zone until the QoS reaches a satisfactory level. After satisfactory QoS is reached, the bandwidth is slowly raised until either the full bandwidth is available or until QoS degrades again. Bandwidth changes can be configured to be gradual (to reduce rapid swings and variations) or rapid.

Multiple Appearance Directory Numbers (MADN) can exist on different zones. Calls to an MADN are handled the same as other IP Phone calls, and are subject to the same bandwidth limitations.

SNMP alarms monitor the system. When the bandwidth limit between zones is reduced below configured levels, an alarm is raised. A Warning alarm and an Unacceptable alarm, each

corresponding to a drop below a configured threshold, are used. When the bandwidth returns to normal, the alarm is cleared. If the bandwidth limit reaches zero, an additional Unacceptable alarm is raised. These alarms allow the system administrator to monitor the system and take corrective action when required.

**⚠ Caution:**

Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.

## Adaptive Network Bandwidth Management configuration parameters

Packet Loss (pl), Jitter (j) and Delay (d) measurements, along with the R factor (r) in IP Phone 200x Phase II telephones, are used to calculate the QoS level for the zones. The coefficients for these QoS measurements — Packet Loss (Cpl), jitter (Cj), delay (Cd), and the R factor (Cr) — can be configured and are used to calculate the rate of bandwidth change. Increasing the coefficients from their default values causes the Sliding Maximum to decrease faster in response to the specific QoS alarm.

The QoS coefficient (CQoS) can be varied from its default value. Increasing this value causes the Sliding Maximum to change more rapidly in response to QoS alarms. Making this value too large will result in loss of overall bandwidth. The following tables illustrate the effect of the default and a high CQoS coefficient.

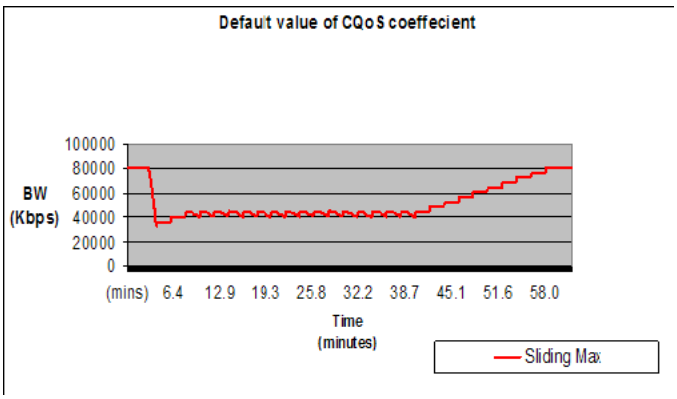


**Figure 20: Effect of the default CQos coefficient**

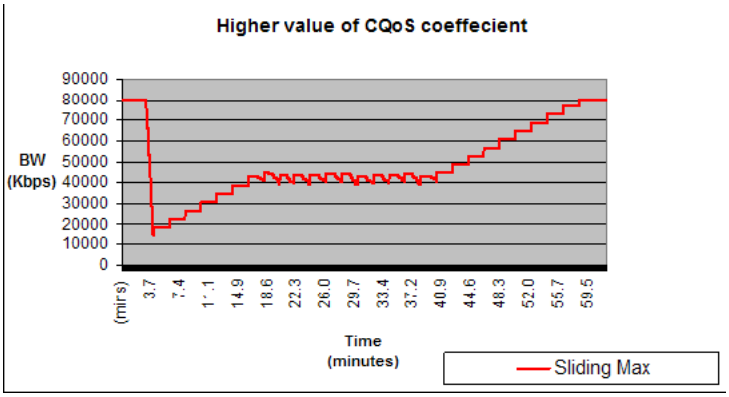


**Figure 21: Effect of a high CQoS coefficient**

Other configurable coefficients used in the calculation are the QoS Coefficient (CQoS), QoS Response Time Increase (ZQRT), and QoS Response Time Interval (ZQRTI). The coefficients CQoS, Cr, Cd, Cpl, and Cj control the rate of bandwidth decrease, while ZQRT and ZQRTI control the rate of bandwidth increase.

The Call Admission Control Validity Time Interval (CACVT) is used to control the length of time that records from a Call Server are saved in the Bandwidth Management table. If no calls occur between two Call Servers within the configured time, the Call Server is removed from the table. For example, if Call Server A has Call Server B in the table, and no call is placed between A and B for the CACVT time, then Call Server A removes all Call Server B records in the table.

## Feature interactions

Virtual Office IP Phones are not subject to bandwidth limitations. They may not have the correct zone information configured. They can also be controlled by a Call Server that is not responsible for the particular zone. Thus, Bandwidth Management is not possible for these phones.

## Feature packaging

The Adaptive Network Bandwidth Management feature requires the following packages.

- QoS Enhanced Reporting (PVQM) package 401
- Call Admission Control (CAC) package 407

**Important:**

Package 401, QoS Enhanced Reporting (PVQM), is required if the R value from the Phase II IP Phones is reported and used to calculate the QoS level for the zones.

# VoIP network voice engineering considerations

It may be necessary to calculate CCS between zones to determine if the network can support the required call volume.

For more information, see the following:

- Network Bandwidth Management on page 25
- *Communication Server 1000M and Meridian 1 Large System Planning and Engineering (NN43021-220)*

## Determine interzone and intrazone bandwidth values

The Call Server uses the values shown in Table 6: Bandwidth estimates used by Call Admission Control on page 85 when calculating the bandwidth each call uses in a zone. The Call Server uses the values in the TLAN Bandwidth columns and subtracts the value from the available zone bandwidth to determine if a zone has sufficient bandwidth for the call.

**Important:**

Do not change, load, or transfer codec lists onto a node during active call processing. Complete changes to codec lists during scheduled maintenance windows when the system is idle.

Call Admission Control (CAC) mechanisms on the Call Server assume average bandwidth utilization for Voice Activity Detection (VAD) codecs.

**Table 6: Bandwidth estimates used by Call Admission Control**

| | | | | TLAN Bandwidth (half-duplex, payload/RTP/UDP/IP/ Ethernet) | | Base WAN Bandwidth (full-duplex, payload/RTP/UDP/IP) | |
|---|---|---|---|---|---|---|---|
| **CODEC type** | **Packet duration (ms)** | **Voice payload (bytes)** | **VAD** | **Peak bandwidth (kbit/s)** | **Average bandwidth (kbit/s)** | **Peak bandwidth (kbit/s)** | **Average bandwidth (kbit/s)** |
| G.711 (64 kbit/s) | 10 | 80 | Off | 252.80 | 252.80 | 96.00 | 96.00 |
| | 20 | 160 | Off | 190.40 | 190.40 | 80.00 | 80.00 |
| | 30 | 240 | Off | 169.60 | 169.60 | 74.67 | 74.67 |
| G.729A (8 kbit/s) | 10 | 10 | Off | 140.80 | 140.80 | 40.00 | 40.00 |
| | 20 | 20 | Off | 78.40 | 78.40 | 24.00 | 24.00 |
| | 30 | 30 | Off | 57.60 | 57.60 | 18.67 | 18.67 |
| | 40 | 40 | Off | 47.20 | 47.20 | 16.00 | 16.00 |
| | 50 | 50 | Off | 40.96 | 40.96 | 14.40 | 14.40 |
| G.729AB (8 kbit/s) | 10 | 10 | On | 140.80 | 84.48 | 40.00 | 24.00 |
| | 20 | 20 | On | 78.40 | 47.04 | 24.00 | 14.40 |
| | 30 | 30 | On | 57.60 | 34.56 | 18.67 | 11.20 |
| | 40 | 40 | On | 47.20 | 28.32 | 16.00 | 9.60 |
| | 50 | 50 | On | 40.96 | 24.58 | 14.40 | 8.64 |
| G.723.1 (6.3 kbit/s) | 30 | 24 | Off | 54.40 | 54.40 | 17.07 | 17.07 |
| G.723.1 (5.3 kbit/s) | 30 | 24 | Off | 54.40 | 54.40 | 17.07 | 17.07 |

**Important:**

Secure Real-Time Transport Protocol (SRTP) adds 10 extra bytes per media packet. This is not significant in the calculation of bandwidth.

The TLAN Bandwidth values contain the total IP and Ethernet packet overhead of 78 bytes, including the 8-byte preamble and minimum 12-byte inter-packet gap. Ensure to include the TLAN Bandwidth values in your bandwidth calculations to give a true indication of the bandwidth used. The Call Server assumes that all calls are made over a half-duplex Ethernet network.

The Call Server is unaware of the particulars of the WAN facility and always uses the values shown in the TLAN Bandwidth columns.

The columns labeled Base WAN Bandwidth provide the data for the payload plus IP overhead without the Ethernet interface overhead. This data provides the basis for any WAN bandwidth

calculations. The overhead associated with the particular WAN facility (for example, Frame Relay) is added to the base value to determine the total bandwidth used. The values shown are for a half-duplex link, so if the WAN facility is half-duplex, the values should be doubled. This should be considered when entering the intrazone and interzone bandwidth values for a zone in LD 117.

The IP/UDP/RTP header size is 40 bytes.

## Calculate the bandwidth amount

Calculate the bandwidth amount to enter into the bandwidth zone table as described below.

### Calculating the bandwidth amount for the bandwidth zone table

1. Determine the number of calls that the network can support for the chosen codec.
2. Multiply the half-duplex Ethernet bandwidth by the value determined in step 1 on page 86.
3. Enter the value determined in step 2 on page 86 in the Call Server bandwidth zone table.

Ensure that the efficiency of the network transporting VoIP is taken into account when you enter the amount of zone bandwidth available. For more information, see the efficiency example in Bandwidth and data network switch efficiency on page 110.

## Determine intrazone bandwidth

Use the following steps to determine intrazone bandwidth.

**Important:**

Determination of intrazone bandwidth is not normally required as a large amount of bandwidth is normally available within a local network, so an arbitrarily large value can be entered for the interzone available bandwidth.

If required, interzone bandwidth is calculated using the same procedure as for intrazone bandwidth.

### Determining intrazone bandwidth

1. Determine the VoIP codec and packet duration to use for interzone calls.
2. Determine the network duplex, Layer 2 protocol, and Layer 2 protocol header size between zones.
3. Determine the total available bandwidth for voice on the data network.
4. Calculate the per-call bandwidth to use for the codec (from step 1 on page 86) over the Layer 2 network (from step 2 on page 86).

Per-call bandwidth for a particular Layer 2 network: (1000 / Packet Duration [ms]) x (Voice payload Bytes) + IP / UDP / RTP Size (Bytes) + Layer two Protocol Header Size [Bytes]) x 8

Alternatively, see VoIP Bandwidth Demand Calculator on page 136.

5. Calculate the number of calls the network can handle, by dividing the total bandwidth available for voice over the Layer 2 network (from step 3 on page 86) by the real per-call bandwidth use for the codec (from step 4 on page 86).
6. Determine the half-duplex Ethernet bandwidth for one call for the codec (from step 1 on page 86) to use.

   See Table 6: Bandwidth estimates used by Call Admission Control on page 85.
7. Calculate the bandwidth value to enter into the Call Server Bandwidth Management zone, by multiplying the half-duplex Ethernet bandwidth (from step 6 on page 87) by the number of calls the network can handle.

### Determine interzone bandwidth

The following example is based on Bandwidth Management of G.729A interzone traffic over a 512 kbit/s Frame Relay network.

### Example of determining interzone bandwidth calculation

1. Codec = G.729A, 20ms.
2. Network type = Full duplex Frame Relay with 6-byte header.
3. Total bandwidth available = 512 kbit/s * 0.9 = 460.8 kbit/s .

   0.9 is an estimate of the efficiency of a random Frame Relay router. The actual efficiency may vary. See calculating data network switch efficiency in Bandwidth and data network switch efficiency on page 110.
4. G.729A per call bandwidth on a full duplex frame relay network = (1000 / 20) * (20 + 40 + 6) * 8 = 26400 bps = 26.4 kbit/s.
5. Total calls possible = 460.8 kbit/s / 26.4 kbit/s = 17 calls.
6. G.729A half-duplex Ethernet per call bandwidth = 78.4 kbit/s.
7. Call Server bandwidth value = 78.4 kbit/s * 17 calls = 1333 kbit/s. Enter 1333 kbit/s in the Call Server.

**Important:**

The use of IP Call Recording doubles the bandwidth requirements of the call. For remote users connecting to the IP Call Recorder server through a WAN connection, the impact of the bandwidth usage to the QoS should be considered. In this case, the IP Call Recorder server must provide the QoS parameters when instructing the IP Phone to echo the voice data. For more information about the Feature Interactions for IP Call Recording, see *Automatic Call Distribution Fundamentals (NN43001-551)* .

## Viewing bandwidth statistics

Use the prt intrazone and prt interzone commands in LD 117 to display the bandwidth statistics in the Call Server. For more information about these commands, see *Software Input Output*

— *Maintenance (NN43001-711)* . For examples on the output of these commands, see Figure 22: Sample output for prt intrazone command on page 88 and Figure 23: Sample output for prt interzone command on page 88 .

```
=> prt intrazone

|Zone|State| Type  |Strategy|MO/  | Bandwidth |  Usage   | Peak |
|    |     |       |        |BMG/|    kbps   |   kbps   |   %  |
|    |     |       |        |VTRK|           |          |      |
|----|-----|-------|--------|----|-----------|----------|------|
|   2| ENL |SHARED |   BQ   |  MO|      10000|       190|     3|
|-------------------------------------------------------------|
|  44| ENL |SHARED |   BQ   | BMG|      10000|         0|     1|
|-------------------------------------------------------------|
 Number of Zones configured = 2
```

**Figure 22: Sample output for prt intrazone command**

```
=> prt interzone

|Near end |Far end  |State| Type  |Stra|MO/ |QoS|Bandwidth  | Sliding |  Usage  |Peak|  Calls  |  Alarm  |
|         |         |     |       |tegy|BMG/|Fac|Configured |   max   |         |    |         |         |
|         |         |     |       |    |VTRK|tor|           |         |         |    |         |         |
|---------|---------|-----|-------|----|----|---|-----------|---------|---------|----|---------|---------|
|Zone|VPNI|Zone|VPNI|     |       |    |    | % |   kbps    |  kbps   |  kbps   | %  |   Cph   |   Aph   |
|----|----|----|----|-----|-------|----|----|---|-----------|---------|---------|----|---------|---------|
|   2|    |    |    | ENL |SHARED | BB | MO|   |      10000|         |       78|   1|         |         |
|-------------------------------------------------------------------------------------------------------|
|   2|   1|  33|   1| ENL |SHARED | BB | MO|100|      10000|         |       78|   1|        1|        0|
|-------------------------------------------------------------------------------------------------------|
|  33|    |    |    | ENL |SHARED | BB|BMG|   |      10000|         |       78|   1|         |         |
|-------------------------------------------------------------------------------------------------------|
|  33|   1|   2|   1| ENL |SHARED | BB|BMG|100|      10000|         |       78|   1|        1|        0|
|-------------------------------------------------------------------------------------------------------|
 Number of Zones configured = 1

Note:  The Far end and VPNI fields are displayed only when Adaptive Bandwidth Management is enabled in LD 117.
```

**Figure 23: Sample output for prt interzone command**

# Tandem Bandwidth Management

Bandwidth utilization for the branch office is tracked at the main office and can be displayed in LD 117 using the prt interzone command. To provide the correct bandwidth utilization to the main office Call Server, when a branch office is calling another node in the network, the calls must be tandemed through the main office Call Server in both the inbound and outbound direction.

If you enter the main office Gateway endpoint identifier in the Tandem Endpoint field for each branch office gateway configured on the NRS, it tandems only in the outbound direction from each branch office (from branch office to main office).

To tandem calls through the main office in the inbound direction (from main office to branch office), use the dialing plan capabilities of the Communication Server 1000 to first route the call to the main office. The main office appends a prefix to the dialed number and the number is routed to the branch office.

Tandem all branch office calls through the main office, so the main office can monitor the bandwidth used at each branch office.

The Tandem Bandwidth Management feature applies to the branch office and the Adaptive Bandwidth Management feature. Specifically, the feature applies to calls made to and from the branch office from either telephones registered locally at the branch office (digital, analog [500/2500-type] telephones, and IP Phones) or trunks at the branch office to another node in the network. The feature does not apply when you use branch office IP Phones registered with the main office (for example, Normal Mode).

## Codec negotiation

Codec refers to the voice coding and compression algorithm used by DSPs. Each codec has different QoS and compression properties.

IP Peer Networking supports the per call selection of codec standards, based on the type of call (interzone or intrazone). IP Peer Networking supports the following codecs with supported payload sizes (the default value is in bold).

**Table 7: Supported codecs**

| Codec | Payload size |
|---|---|
| G.711 A/mu-law | 10 millisecond (ms), 20 ms, and 30 ms |
| G.729 A | 10 ms, 20 ms, 30 ms, 40 ms, and 50 ms |
| G.723.1 | 30 ms, although it can limit the number of DSP channels available |
| T.38 for fax | Supported for fax calls on gateway channels |
| G.711 Clear Channel | Supported on the MC32S and DSP d/bs (Mindspeed) and not on the MC32 cards |

The G.XXX series of codecs are standards defined by the International Telecommunications Union (ITU).

By default, the G.711 codec must be supported at both ends of a call. Codec configuration is performed for each node and is independent of the signaling gateway (SIP or H.323) that is used on the node. T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far-end does not support the T.38 codec.

If a Communication Server 1000E system is used, the same payload sizes for the same codec type should be configured on all Internet Protocol Media Gateway (IPMG) cabinets in a system; otherwise, Time Division Multiplexing (TDM) to TDM calls between IPMG cabinets are not successful.

If more than one codec is configured, the minimum payload size among the configured codecs is used for the SIP Trunk Gateway codec negotiation.

For more information about the codecs that are supported for IP phones, see *IP Phones Fundamentals, NN43001-368* and *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

**Important:**

Nortel recommends that you configure the same payload size for all codecs in the same node. The payload size on the Communication Server 1000 system must be configured to 30 ms to work with the SRG.

Ensure common codecs across the network, especially in tandem calls across different protocols, for example, H.323 tandem to SIP or SIP to H.323. The Session Description Protocol (SDP) transparency helps in this case; however, when you tandem through different trunks over different protocols, codecs must match.

## SIP example

If a G.711 20 ms codec and G.729 30 ms codec are configured, then codec negotiation uses the minimum payload size of 20 ms. That is, the G.711 20 ms codec and the G.729 20 ms codec are used. Instead, Nortel recommends that both G.711 and G.729 codecs be configured as 20 ms.

When a G.729 30 ms codec is configured, the G.729 10ms/20ms/30ms codecs are supported.

IP Peer Networking performs codec negotiation by providing a list of codecs that the devices can support. Use Communication Server 1000 Element Manager to configure the list of codec capabilities.

The codec preference sequence sent over SIP/H.323 depends on the bandwidth policy selected for the Virtual Trunk zone and the involved telephones. For Best Quality, the list is sorted from best to worst voice quality. For Best Bandwidth, the list is sorted from best to worst bandwidth usage.

The G.711 codec delivers toll quality audio at 64 kbit/s. The G.711 codec is optimal for speech quality, as it has the smallest delay and is resilient to channel errors. However, the G.711 codec uses the largest bandwidth.

The G.729A codec provides near toll quality voice at a low delay. The G.729A codec and G.729AB codecs use compression at 8 kbit/s.

The G.723.1 codec provides the greatest compression compared to the previously described codecs.

Payload default values need to be changed if the customer wants to communicate with a third-party gateway that does not support the above default payload sizes. Otherwise, IP Peer calls to or from the third-party gateway are not successful.

If the payload sizes are configured higher than the default values (for example, to support a third-party gateway), then the local IP calls are affected by higher latency because the codec configuration applies to both IP Peer calls and local IP (IP Line) calls.

If a Communication Server 1000E system is used, the same payload sizes for the same codec type should be configured on all IPMG cabinets in a system. Otherwise, TDM to TDM calls between IPMG cabinets are not successful.

## G.711 A-law and mu-law interworking

In case the far end uses a different Pulse Code Modulation (PCM) encoding law for its G.711 codec, systems configured as G.711 A-law also include G.711 mu-law on their codec preferences list. Systems configured as G.711 mu-law include G.711 A-law as their last choice. Therefore, encoding law conversion is performed between systems with different laws.

## Codec selection

For every Virtual Trunk call, a codec must be selected before the media path can be opened. When a call is set up or modified (that is, media redirection), one of two processes occurs:

- The terminating node selects a common codec and sends the selected codec to the originating node.
- The codec selection occurs on both nodes.

Each node has two codec lists – its own list and the far end list. To select the same codec on both nodes, it is essential to use the same codec selection algorithm on both nodes. Before the codec selection occurs, the following conditions are met:

- Each codec list contains more than one payload size for a given codec type (depending on the codec configuration).
- Each codec list is sorted by order of preference (the first codec in the near end list is the near end most preferred codec, the first codec in the far end list is the far end preferred codec).

## Bandwidth Management and codecs

Bandwidth Management defines the codecs to use for intrazone calls and interzone calls.

Administrators use Bandwidth management to define codec preferences for IP Phone to IP Phone calls controlled by the same Communication Server 1000 system within the same zone (intrazone calls). Administrators use different codec preferences for calls between an IP Phone on the Communication Server 1000 system to a Virtual Trunk (potentially an IP Phone on another Communication Server 1000 system) or calls to IP Phones in another zone (interzone calls).

For example, you may prefer high quality speech (G.711) over high bandwidth within one system, and lower quality speech (G.729AB) over lower bandwidth to a Virtual Trunk. Such a mechanism can be useful when a system is on the same LAN as the IP Phones it controls, but the other systems are on a different LAN (connected through a WAN).

Usage of bandwidth zones for Virtual Trunks are different than IP Phone bandwidth usage. For Virtual Trunks, a zone number is assigned in the Route Data Block (LD 16). The zone number determines codec selection for interzone and intrazone calls (Best Quality).

Bandwidth usage for Virtual Trunks is accumulated in its zone to block calls that exceed the bandwidth availability in a specific zone. However, the amount of bandwidth required to complete a given call is not known until both call endpoints negotiate which codec to use. The bandwidth used to calculate the usage of a Virtual Trunk call is determined by the preferred codec of the device that connects to the Virtual Trunk. If the device is an IP Phone, the bandwidth calculations use the preferred codec of the IP Phone, based on the codec policy defined for the zones involved (Best Quality). The bandwidth calculations use the preferred codec of the Voice Gateway Media Card for connections between a circuit-switched device (for example, a PRI trunk) and a Virtual Trunk.

## Codec selection algorithms

When the codec lists meet the above conditions, one of the following codec selection algorithms selects the codec to be used:

- H.323 Master/Slave algorithm
- SIP Offer/Answer model
- Best Bandwidth codec selection algorithm

If a SIP trunk call is between a Communication Server 1000 system and other third-party gateway/SIP clients (for example, MCS 5100), then the codec selection does not guarantee that the same codec is selected for a call from endpoint A to endpoint B and for a call from endpoint B to endpoint A. This different codec selection makes it difficult for Bandwidth Management. However, calls between two Communication Server 1000 systems have the same codec selection decision, regardless of who originated the call.

### H.323 Master/Slave algorithm

In the case of a Virtual Trunk call between Nortel and third-party equipment, the H.323 Master/Slave algorithm is used.

The codec selection algorithm proposed by the H.323 standard involves a Master/Slave negotiation initiate each time two nodes exchange their capabilities. The Master/Slave information decides that one node is Master and the other node is Slave. The outcome of the Master/Slave negotiation is not known in advance; it is a random result. One node could be Master and then Slave (or vice versa) during the same call.

### Algorithm details

The H.323 Master/Slave algorithm operates in the following manner:

- The Master node uses its own codec list as the preferred one and finds a common codec in the far end’s list. In other words, the Master gets the first codec in its list (for example, C1), checks in the far end’s list if it is a common codec; if it is, C1 is the selected codec.

Otherwise, it gets the second codec in its list and verifies it against the far end, and so on.

- The Slave node uses the far end's list as the preferred one and finds in its own list the common codec.

### Issues caused by the H.323 Master/Slave algorithm

The issues caused by the Master/Slave algorithm are due to the random nature of the Master/Slave information. You cannot predetermine the codec used during a Virtual Trunk call.

The following are the issues associated with the H.323 Master/Slave algorithm:

- After an on-hold and off-hold scenario (which triggers Master/Slave negotiation), the codec used for the restored call might be different than the one used before on-hold, because the Master/Slave information can change.
- When using Fast Start codec selection, a call from Telephone 1 (node 1) to Telephone 2 (node 2) can use a different codec than a call from Telephone 2 (node 2) to Telephone 1 (node 1), because the terminating end is always Master.
- For tandem calls, the Master/Slave information is not relevant. The Master/Slave information is designed for use between two nodes only, not between three or more nodes as it makes the codec selection for tandem calls more complex and inefficient.

To solve the previous issues, use another codec selection algorithm, not based on the unpredictable Master/Slave information. Because any change to the Master/Slave algorithm implies a change to the H.323 standard, the new codec algorithm is used for Virtual Trunk calls between Nortel equipment.

## SIP Offer/Answer model

The SIP codec negotiation is based on the Offer/Answer model with Session Description Protocol (SDP).

The following three cases of codec negotiation are supported:

- The calling user agent sends an SDP offer with its codec list in the invite message with a sendrecv attribute. In this case, the called user agent selects one codec and sends the selected codec in an SDP answer. The SDP answer is included in the 200 OK message (response to the INVITE) with the sendrecv attribute as the preferred method of operation.
  - The calling user agent sends an SDP offer with its codec list in the invite message with a sendrecv attribute. The called user agent returns more than one codec in the SDP answer. In the case that many codecs are included in the response, the calling user agent picks the first compatible codec from the called user agent list, and sends a new SDP offer with a single codec to lock it in.
  - If the SDP of the calling user agent is not present in the INVITE message, then the called user agent sends its codec list in an SDP offer in the 200 OK message, with the sendrecv attribute. The calling user agent selects one codec and sends it in an SDP answer inside the ACK message, with a sendrecv attribute.

For more information, see RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP).

# Best Bandwidth codec selection algorithm

The Best Bandwidth codec selection algorithm solves the issues caused by the H.323 Master/Slave algorithm. The Best Bandwidth algorithm selects one common codec based on two codec lists. Every time the selection is done with the same two lists, the selected codec matches.

The Best Bandwidth codec decision is based on the codec type only, it does not consider the fact that some codecs, while generally using less bandwidth, can consume more bandwidth than others at certain payload sizes.

Best Bandwidth is also applicable to SIP.

## Algorithm details

The selected codec is the type considered as the best bandwidth codec type. To determine if one codec type has better bandwidth than another, see the rule as summarized in Table 8: Best Bandwidth algorithm : codec type on page 94.

**Table 8: Best Bandwidth algorithm : codec type**

| | G.711 A law | G.711 mu-law | G.729 A | G. 729 AB | G. 723.1 |
|---|---|---|---|---|---|
| G.711 A-law | G.711 A-law | G.711 mu-law | G.729 A | G. 729 AB | G. 723.1 |
| G.711 mu-law | G.711 mu-law | G.711 mu-law | G.729 A | G. 729 AB | G. 723.1 |
| G.729 A | G.729 A | G.729 A | G.729 A | G. 729 AB | G.729 A |
| G. 729 AB | G. 729 AB | G. 729 AB | G. 729 AB | G. 729 AB | G. 729 AB |
| G. 723.1 | G. 723.1 | G. 723.1 | G.729 A | G. 729 AB | G. 723.1 |
| The SRG 50 does not support G.723 codec. | | | | | |

## Feature interaction

The SRG operates with Communication Server 1000 similar to MG 1000B, but with a limitation on codec selection policy. Calls between branch IP Phones and branch analog phones are based on the interzone policy rather than the intrazone policy defined in the Communication Server 1000 main office. The zone table is updated based on the intrazone policy.

The net result of this limitation is that calls between branch IP Phone users and the branch PSTN, or between the IP Phones and branch analog phones, always use a Best Bandwidth codec. However, the calls are accounted for as Best Quality. This may impact the perception of call quality in this scenario, but it will not result in early call blocking. There is no impact to codec selection or bandwidth usage tracking for calls that require WAN bandwidth.

The SRG 50 does not support the G.723 codec.

# Bandwidth Management parameters

The following information describes Bandwidth Management parameters.

## Zones

Bandwidth Management zones are configured for each endpoint on a Call Server. The Network Bandwidth zone number determines if a call is an intrazone call or an interzone call. After that is determined, the proper codec and bandwidth limit is applied to the call.

All of the endpoints on one Call Server are configured with a zone number to identify them as belonging to a unique geographic location in the network. In addition, Virtual Trunks are configured with a zone number that is different from the endpoint zone numbers in the Call Server.

An IP Peer network is divided into different Bandwidth Management zones. Each IP Phone, Virtual Trunk, or Voice Gateway DSP channel is assigned to a Bandwidth Management zone. All IP Phones, 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. Voice Gateway DS Channel zone must be the same channel zone as the Route zone this channel belongs to. Channel zone is automatically populated by the Route zone and cannot be manually configured in LD 14. 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 are treated identically. Each IP Phone is assigned to a zone during configuration. The branch office feature enables IP Phones located in more than one geographic location to have dialing plan behaviors localized to the telephone location, rather than the Call Server location.

IP Phones at a branch office are configured within a unique zone. In the main office Call Server, IP Phones 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 a NRS as a long-distance call. Zone configuration data enables the main office Call Server to modify the dialed digits for these types of calls initiated from an MG 1000B telephone. The NRS then provides the endpoint information to route the call to the branch office.

Different zone numbers are assigned to different MG 1000B systems.

Codec selection occurs as described in Codec selection on page 91.

## Zone Assignments

Nortel recommends the following when assigning bandwidth zones based on geographic location:

- Each location is assigned with a unique bandwidth zone
- IP and VGW resources that are local to the same location, are configured in a same bandwidth zone
- Virtual trunk resources are configured in a separate bandwidth zone
- Use the same zone number for Virtual trunk resources for all Call servers within the same network (for example, Main Office and or Branch Office configuration or MG 1000B groups or call servers within one LAN). The reason for this is because the Virtual Trunk zone is not factored into the decision of the Call server whether the call is treated as a INTRAZONE or INTERZONE.
- Both intra- and interzone Virtual Trunks should be configured with Best Quality (BQ) codec and with maximum available bandwidth, such as 1 000 000 kbit/s.

The following table shows an example of a system with geographic redundancy that is distributed among three locations. Zone table is configured once at Location 1 and then the database is to be distributed among the systems automatically by Geographic Redundancy.

**Table 9: Single system in a network – Communication Server 1000E system with Survivable Media Gateway**

| | | |
|---|---|---|
| Location 1: (Primary Communication Server 1000E with High Availability Redundant System) | Zone = 1 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 2: (Secondary 1 MG 1000E system) | Zone = 2 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 3: (Secondary 2 MG 1000E system) | Zone = 3 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| | VTRK Zone = 10 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BQ (Best Quality) |

The following table shows an example of main office and Branch Office system in the network that are distributed among three locations.

**Table 10: Single system in a network – Communication Server 1000E main office system with MG 1000B and SRG**

| | | |
|---|---|---|
| Location 1: (Main Office CS1000E system) | Zone = 1 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 2: (Branch Office MG 1000B system) | Zone = 2 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 3: (Branch Office SRG system) | Zone = 3 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| | VTRK Zone = 10 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BQ (Best Quality) |

The following table shows an example of systems with geographic redundancy, and main and Branch Office systems in the network that are distributed among six locations. Zone table is configured once at Location 1 and then database is to be distributed among the Systems by Geographic Redundancy means automatically.

**Table 11: Multiple systems in a network**

| | | |
|---|---|---|
| Location 1: (Primary Communication Server 1000E with High Availability Redundant System) | Zone = 1 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 2: (Secondary 1 MG 1000B system) | Zone = 2 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 3: (Secondary 2 MG 1000B system) | Zone = 3 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 4: (Main Office Communication Server 1000E system) | Zone = 4 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |
| Location 5: (Branch Office MG 1000B system) | Zone = 5 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Quality) |
| Location 6: (Branch Office SRG system) | Zone = 6 | Intra BW = 1000000 Intra BW Strategy = BQ (Best Quality) Inter BW = 1000000 Inter BW Strategy = BB (Best Bandwidth) |

## Zone based digit manipulation

For branch office users or SRG 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 MG 1000B PSTN trunk or SRG PSTN trunk, rather than receive the same routing as nonbranch users in the main office.

To achieve the different routing, 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. A branch user and a main user 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 or SRG 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 or SRG users undergo different routing. Some applications include:

- routing all branch office or SRG user calls to the MG 1000B or SRG PSTN trunk
- routing branch office or SRG user local calls to the MG 1000B PSTN trunk
- routing all branch office or SRG user calls to the main office PSTN trunk
- routing branch office or SRG user long distance calls to the main office PSTN trunk

Special considerations apply when a single Access Code is used for both on-net and off-net calls, especially with UDP. Normally, the routing of on-net and off-net calls differs. The Call Server ESN Special Number provisioning and Gatekeeper Numbering Plan Entry provisioning should be used to provide this different routing.

Use standard procedures when you do not share a single Access Code (you use one Access Code exclusively for UDP on-net dialing). For more information, see *Dialing Plans Reference, NN43001-283*.

For a given branch office, there can be more than one zone defined at the main office so different branch office or SRG users may receive different routing treatments.

The combination of zone based digit manipulation and Communication Server 1000 routing capabilities can be used to achieve many other routing outcomes for branch office or SRG user calls.

## CLID composition

Digital manipulation is commonly used for digit insertion, deletion, and for call type conversion before out-pulsing the digits to the Virtual Trunk.

The IP Special Number (ISPN) parameter in the ESN data block ensures the Calling Line ID (CLID) is formed correctly when a call type (CLTP) is converted from its original type (such as International, National, or SPN) to CDP/UDP/SPN format. Conversion to CDP/UDP/SPN format ensures that the call type stays in the Private/Special Number domain.

The ISPN parameter is configured in LD 86. By default, it is configured to NO.

If ISPN is NO, the CLID is formed based on the CTYP parameter of the DMI data block, and INST digits are inserted.

If ISPN is YES, the CLID is formed based on the call type before digit manipulation. INST digits are inserted, and the CLID is considered an IP Special Number. The call type before digit manipulation is determined as follows:

- If the call type before digit manipulation is SPN (Special Number), it is converted to a value corresponding to the CLTP parameter in the Special Number Translations data block, as shown in Table 11.

  **Table 12: Mapping between from CTYP parameter in SPN block to call type before digit manipulation**

| CLTP parameter | Call type before digit manipulation |
|---|---|
| LOCL | Local PSTN |
| NATL | National PSTN |
| INTL | International PSTN |

- If the call type before digit manipulation is not SPN (Special Number), it is not changed.

## CLID verification

Use the CLIDVER prompt in LD 20 to verify that the CLID has been properly composed and configured. This command simulates a call, without actually making the call, and generates a report of the properties of the call.

## Vacant Number Routing

Vacant Number Routing (VNR) is mandatory in a branch office. 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 are tried, in the configured sequence. If all alternate routes fail, the call is blocked.

VNR enables a branch office to route calls through the NRS, or other alternate routes with minimal configuration. Instead of changing the numbering trees and steering codes at each location, all the routing information resides 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 NRS. The NRS 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 are 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 IP Phone (the Call Server updates this information on the telephone). The date and time display on the IP Phone is determined by the Call Server to which the telephone connects.

The branch office feature allows branch offices to reside in regions with a different time zone than the main 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 MG 1000B telephones display the correct time of the branch office, rather than that of the main office.

## MG 1000B IP Phone calls to a local PSTN

When an MG 1000B IP Phone in Normal Mode dials a local PSTN number, the call is processed by the main office Call Server. The dialed digits are modified according to the dialing plan information configured in the zone for the MG 1000B IP Phone.

The call is configured to be routed over the Virtual Trunk to the branch office. The MG 1000B call server 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 calls, and that Access Code is associated with a branch office zone, all calls (local and long distance) are routed through that branch office.

## Special Number (SPN) for emergency services

Use a Special Number (SPN) for access to emergency services to use the digit manipulation capabilities configured for the MG 1000B zone as follows:

- If the branch user is 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 to access emergency services, a conflict occurs in the NRS. The conflict 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 NRS as an SPN. In the NRS, the SPNs have their own separate numbering plan. The call is routed to the MG 1000B Call Server and sent out to the MG 1000B PSTN.
- If the Branch User is in Local Mode (or an analog [500/2500-type] or digital telephone at the MG 1000B), 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.

For more information about Emergency Services, see *Branch Office Installation and Commissioning, NN43001-314*

## Emergency Services

Support for access to emergency services by Branch Users in Normal Mode is configured at the main office.

The key difference between the main office user and the branch 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—normally an emergency trunk in the main office, and in each of the branch offices. An emergency call that originates from an IP Phone must route from the main office Call Server to the SRG or MG 1000B CP PM so that the call can be sent on the SRG or MG 1000B PSTN Trunks.

In Normal Mode, an IP Phone must have a Virtual Trunk available and configured between the main office and branch office to complete an emergency services call.

**Important:**

Do not route ESA calls to a node that has no direct ESA trunks.

## LAN/WAN bandwidth requirements

The LAN/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 LAN/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

Signaling and background tasks that use LAN/WAN bandwidth include:

- NRS polling
- NRS database synchronization
- Endpoint registration requests to NRS
- Lamp Audit
- IP Phone Keep Alive messages
- Call signaling to and from IP Phones

The maximum bandwidth required for the above tasks is approximately 13 kbit/s. This is insignificant when compared to the bandwidth requirement for the expected voice traffic.

When you determine the LAN/WAN bandwidth requirement for a branch office, expected voice traffic should be the major factor. For more information about network performance measurement, see Network Performance Measurement on page 122.

The data rate for a LAN is the total bit rate. The total subnet traffic is measured in Erlangs. An Erlang is a telecommunications traffic measurement unit used to describe the total traffic volume of one hour. Network designers use these measurements to track network traffic patterns. For more information about traffic information, see *Communication Server 1000M and Meridian 1 Large System Planning and Engineering, NN43021-220* and *Branch Office Installation and Commissioning, NN43001-314*.

## Calculation tables

**Table 13: Full Duplex Ethernet bandwidth for one channel (one Erlang)**

| codec | Payload | Full Duplex Ethernet |
|---|---|---|
| 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 14: Traffic capacity at P.01, P.005, and P.001 GOS**

| Device | P.01 | P.005 | P.001 |
|---|---|---|---|
| MC (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 15: LAN/WAN bandwidth for one channel (one Erlang)**

| codec | Payload | LAN/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 |
| G.729A | 20 ms | 12 kbit/s |
| G.729A | 30 ms | 9 kbit/s |

## Calculating TLAN subnet bandwidth for IP Phone traffic

Incremental bandwidth required on the TLAN subnet to carry given voice traffic.

Calculate the data rate:

Total traffic in Erlangs x 95 kbit/s

22 x 95 kbit/s = 2090 kbit/s = 2.09 Mbit/s

One Erlang of TDM 64 kbit/s channel becomes 95 kbit/s packets after G.711 codec transcoding, which adds overhead. See Table 15: LAN/WAN bandwidth for one channel (one Erlang) on page 103 if another type of codec is used. Requirement: TLAN subnet bandwidth 2.02 Mbit/s.

## Calculating MG 1000B with Virtual Trunk LAN/WAN

Assuming G.711/30 ms for the LAN/WAN, the traffic distribution is as follows:

1. Calculate the MC traffic:

   MC traffic = 180 CCS

   One MC 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 14: Traffic capacity at P.01, P.005, and P.001 GOS on page 103) is sufficient to handle the Virtual Trunk traffic.

3. Calculate the incremental LAN/WAN bandwidth:

   - LAN/WAN traffic = IT traffic to MOR + Analog traffic to IPPT

     = 252 + 72

     = 324 CCS

   - LAN/WAN bandwidth = 324/36 x 37 kbit/s (from Table 15: LAN/WAN bandwidth for one channel (one Erlang) on page 103 for G.711 codec with 30 ms payload)

     = 333 kbit/s

     See Table 15: LAN/WAN bandwidth for one channel (one Erlang) on page 103 for other codecs or payload sizes.

# Branch office conference engineering

## With no local conference

Two parties at a branch office use IP Phones to call each other , and then add a third-party from the same branch office. The conference calls use a LAN/WAN to reach the conference bridge at the main office. See Table 15: LAN/WAN bandwidth for one channel (one Erlang) on page 103 for bandwidth requirements if the codec, payload, or both differ from the assumptions in the following branch office conference scenarios.

The calculated conference LAN/WAN bandwidth is added to the normal LAN/WAN requirement between the branch office and the main office for Internet Telephony Gateway (ITG) trunks or Virtual Trunks.

## 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 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 IP Phones x CCS for each telephone Conference traffic (TCON) = TCCS x 0.07 CCS = TCCS x 0.07/36 Erlangs
2. Calculate LAN/WAN bandwidth:

   For a G.729A/30 ms codec: LAN/WAN kbit/s = TCON (erlangs) x 9 kbit/s

   For a G.711/30 ms codec: LAN/WAN kbit/s = TCON (erlangs) x 37 kbit/s

### 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 LAN/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 LAN/WAN bandwidth: For a G.729A/30 ms codec: LAN/WAN kbit/s = TCON (erlangs) x 9 kbit/s For a G.711/30 ms codec: LAN/WAN kbit/s = TCON (erlangs) x 37 kbit/s

   Use other bandwidth data from Table 15: LAN/WAN bandwidth for one channel (one Erlang) on page 103 if the codec and payload differ from those listed above.

### With local conference Integrated Conference Bridge 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 LAN/WAN traffic and does not require a LAN/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 LAN/WAN calculation directly and are not included in this document.

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 LAN/WAN to the main office. To leave or retrieve a message, the connection requires LAN/WAN bandwidth.

### Calculating branch office traffic and LAN/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 hold time of a voice message: 40 seconds 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 MG 1000B traffic in CCS = 10% x Total MG 1000B CCS traffic/36 (Erlangs)
2. Calculate LAN/WAN bandwidth: For a G.729A/30 ms codec: LAN/WAN kbit/s = VMT (erlangs) x 9 kbit/s For a G.711/30 ms codec: LAN/WAN kbit/s = VMT (erlangs) x 37 kbit/s

## Dialing plan

The following information describes the preparation and process necessary to configure a dialing plan for PSTN access to SRG users in normal mode.

## Prerequisites to configure the dialing plan

Perform the following tasks before you configure the dialing plan for PSTN access to branch office or SRG users in Normal Mode.

- At the main office, configure the Virtual Trunk to enable calls that originate on MG 1000B or SRG IP Phones in Normal Mode to reach the branch office. For more information, see *IP Peer Networking Installation and Commissioning, NN43001-313*.
- At the main office, configure trunks for access to the PSTN.
- At the branch office, configure the Virtual Trunk to enable calls that originate on MG 1000B or SRG IP Phones in Normal Mode to reach the branch office. For more information, see *IP Peer Networking Installation and Commissioning, NN43001-313*.
- 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.
- At the main office, configure routing for PSTN access.
- At the branch office, configure routing to enable calls made from TDM or IP Phones in Local Mode to access the PSTN.
- At the branch office, configure Vacant Number Routing (VNR).
- Configure IP Phones with the same zone number at both the main office and the branch office. Nortel 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.

## Configuration

Perform the following tasks to configure the dialing plan for MG 1000B PSTN access:

- At the main office:
  - Configure the ZACB property for the branch office zone.
  - Configure the ZDP property for the branch office zone.

- Configure the Route List Index.
- Configure the ESN Special Number and Digit Manipulation.

• Configure the NRS:

- Access NRS Manager.
- Select an endpoint.
- Configure the Numbering Plan Entry for the branch office.

• At the branch office:

- Configure the Route List Index.
- Configure ESN.

For more information about configuring the dialing plan, see Configuring Dialing Plan on page 236.

## Branch office dialing plan

As IP Phone users can be located at a branch office equipped with an MG 1000B Core, the routing of calls to the local gateway is important (especially when toll charges apply to calls made from the central Call Server that controls the telephone). The administrator can configure digit manipulation through zone attributes for IP Phones to select a main office or branch office that provides PSTN access local to the destination of the call.

Calls from the PSTN to users within the network can be routed with the various ESN numbering plan configurations or the VNR feature. This routing enables small sites, such as a branch office, to require minimal configuration to route calls through other Call Servers or through the NRS.

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 User to be routed to the desired local PSTN facilities.

**Important:**

Outgoing calls can include local and, optionally, long distance calls.

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

The SRG supports only one dialing plan option at a time. CDP and UDP dialing plan options cannot be configured at the same time in the same system.

For more information about branch office features that support the various PSTN interfaces, see *Electronic Switched Network Reference — Signaling and Transmission, NN43001-280*. For more information about CDP, see *Dialing Plans Reference, NN43001-283*. For more

information about other Numbering Plan options, see *Communication Server 1000E Overview, NN43041-110*.

## Zone parameters

Zone parameters must be configured at both the main office Call Server and MG 1000B Call Server. The main office procedure is similar to an IP Peer Network configuration.

# Abbreviated Dialing

The Abbreviated Dialing feature is implemented with a pretranslation group assigned to every telephone. All IP Phones in the same Bandwidth Management zone use the same pretranslation group. TDM telephones, which share the same dialing plan with IP Phones in a Bandwidth Management zone, also use the same pretranslation group.

Virtual Office Login always requires that the full DN be entered. Users cannot use the abbreviated DN for the Virtual Login to an IP Phone.

The called telephone display always shows the full length DN of the calling party.

Nortel recommends the following configuration of Abbreviated Dialing in the main office and branch offices.

- The numbering plan at both the main office and branch office must have six or seven digits, including IP Phones in Local Mode.
- All MG 1000B IP Phones are in a different Bandwidth Management zone than the main office IP Phones.
- Each Bandwidth Management zone has a unique pretranslation group number assigned to it.
- Calling Line Identification (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 you design 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.

# Abbreviated dialing

With the Abbreviated Dialing feature, users in the same geographic location (the Main Office or the Branch Office) can call one another with a DN shorter than the configured DN.

This feature is implemented with a pre-translation group assigned to every telephone. All IP Phones in the same bandwidth management zone use the same pre-translation group. TDM telephones, which share the same dialing plan with IP Phones in a bandwidth management zone, also use the same pre-translation group. The following table provides sample values to explain the functionality of Abbreviated Dialing.

**Table 16: Sample values for Abbreviated Dialing**

| | Main Office | Branch Office |
|---|---|---|
| Location code | 70 | 71 |
| DN | 70300 | 713000 |

Abbreviated dialing works as follows:

- An IP Phone 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 MG 1000B IP Phone, 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 IP Phone 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 MG 1000B IP Phone, 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 an MG 1000B 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.
- Calling Line Identification (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.

# Bandwidth and data network switch efficiency

Note the maximum packets per second forwarding rates of the platforms. The rate determines the switch efficiency and the actual throughput the platform is capable of supporting.

## Example

For 64-byte packets and a 10-Mbit/s link, the maximum forwarding rate is 14 880 packets per second.

Bandwidth throughput is: (64 B / P) * (8 b / B) * (14 ,880 P / S) = 7.62 Mbit/s

A similar calculation is required for the WAN switches used.

**Note:**

Efficiency of an Ethernet switch is taken from the Performance Specifications section of the Ethernet switch manual.

# Network design assessment

Ensure you fully understand the design of an existing data network before you implement a VoIP network. This section describes key issues to consider when you create a new converged voice and data network.

For example, assess the network for such things as:

- the distribution of protocols in the network
- the level of QoS on the network
- the link speeds, link types, and link utilization
- the traffic flows in the network

Some of the tools used to assess the VoIP network are described (see Available traffic tools on page 120), as well as examples of logical connection diagrams for small, medium, and large campus networks (see Figure 24: Campus network reference model on page 113).

**⚠ Warning:**

Before a Communication Server 1000 system can be installed, a network assessment must be performed and the network must be VoIP ready.

If the minimum VoIP network requirements are not met, the system does not operate properly.

# Network modeling

Network analysis can be difficult or time consuming if the intranet and the CS 1000 system installation are large. Commercial network modeling tools can analyze "what if" scenarios predicting the effect of topology, routing, and bandwidth changes to the network. These modeling tools work with an existing network management system to load current configuration, traffic, and policies into the modeling tool. Network modeling tools can help to analyze and test the recommendations given in this document to predict how delay and error characteristics impact the network.

## Physical and logical network diagrams

To determine VoIP readiness, diagrams of both the data and voice infrastructure (physical and logical) are required. These diagrams are valuable when determining the platforms deployed in the network as well as the logical design, such as the IP addressing architecture, link speeds, and connectivity.

**Note:**

Network diagrams are typically created using SNMP Network Management Systems (NMS). NMS provides graphical views from physical connections between LANs and WANs to the logical connections of a Virtual LAN (VLAN).

From a voice perspective, the numbering plan and Call Detail Record (CDR) help to determine calling patterns in a multisite environment.

Knowledge of routing of circuit switched trunking facilities helps to determine utilization and bandwidth requirements for a VoIP deployment.

## Application requirements

Table 17: Common application performance parameters on page 112 lists the various QoS performance parameters required by some common applications. If these parameters are mixed over a common use IP network and QoS technologies are not used, the traffic can experience unpredictable behavior.

**Table 17: Common application performance parameters**

| Application | Relative bandwidth demand | Sensitivity to | | |
|---|---|---|---|---|
| | | Delay | Jitter | Packet Loss |
| VoIP | Low | High | High | High |
| Video Conferencing | High | High | High | Med |
| Streaming Video on Demand | High | Med | Med | Med |
| Streaming Audio | Low | Med | Med | Med |
| Web browsing (eBusiness) | Med | Med | Low | High |
| Email | Low | Low | Low | High |
| File Transfer | Med | Low | Low | High |

## Sample IP network model

The Communication Server 1000 and Meridian 1 systems are VoIP servers suited for typical campus network designs.

In most cases, the system is connected logically to the server layer, as the server layer is engineered for high availability and security.

For more information about security management, see *Security Management Fundamentals, NN43001-604*.

A large amount of available bandwidth at the server level, though not required by the Call Server, helps to ensure satisfactory VoIP QoS.

Nortel recommends QoS mechanisms for all layers to ensure that voice traffic obtains a level of service greater than the level of service for the best effort data traffic.

Physical connectivity, VLANs, and subnets for the core server components are configured at the server layer, following existing server layer design and conforming to the core server configuration requirements.

Alternately, if campus distributed Media Gateway systems are used, they are connected at the distribution layer. The core IP network can be configured with multiple VLANs and subnets to meet the core server configuration requirements.

The following are planned based on the access and distribution layers configuration:

- VLANs
- subnets
- QoS mechanisms for the IP Phones, such as DiffServ and 802.1Q

## Typical network topology

Figure 24: Campus network reference model on page 113 provides a reference model for a campus network.

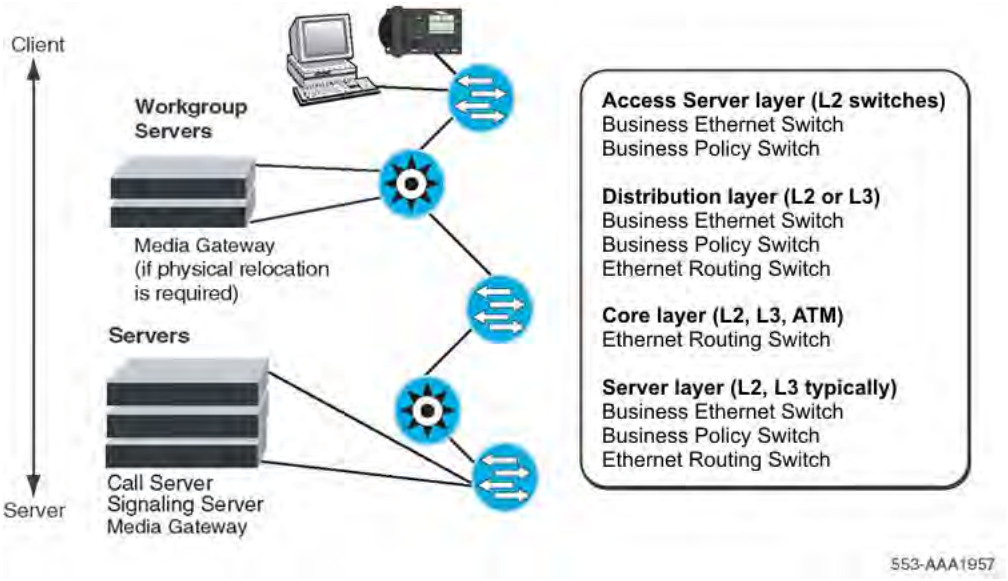


**Figure 24: Campus network reference model**

Figure 25: Small campus network example on page 114, Figure 26: Midsize campus network example on page 114, and Figure 27: Large campus network example on page 115 show examples of logical connection diagrams for small, medium, and large campus networks. Other network designs can be used. The actual design implemented depends on many factors, including physical locations, size, and scalability.

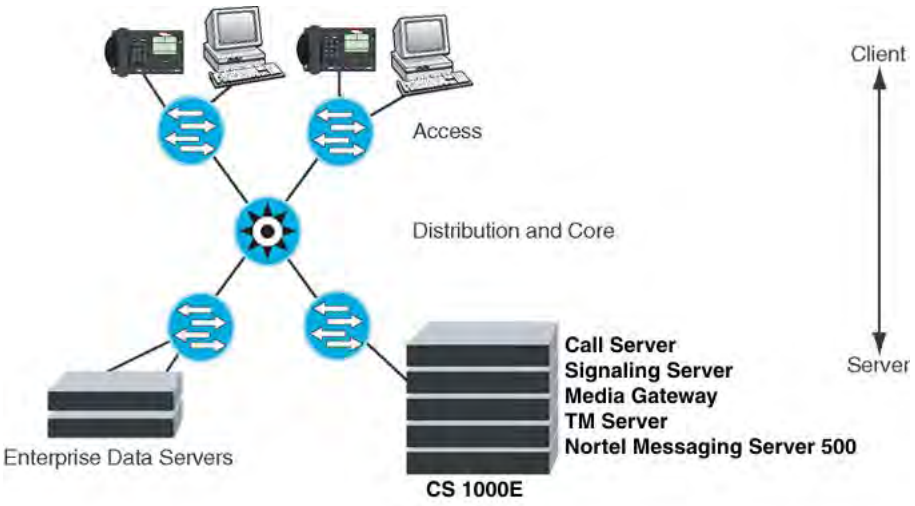


**Figure 25: Small campus network example**

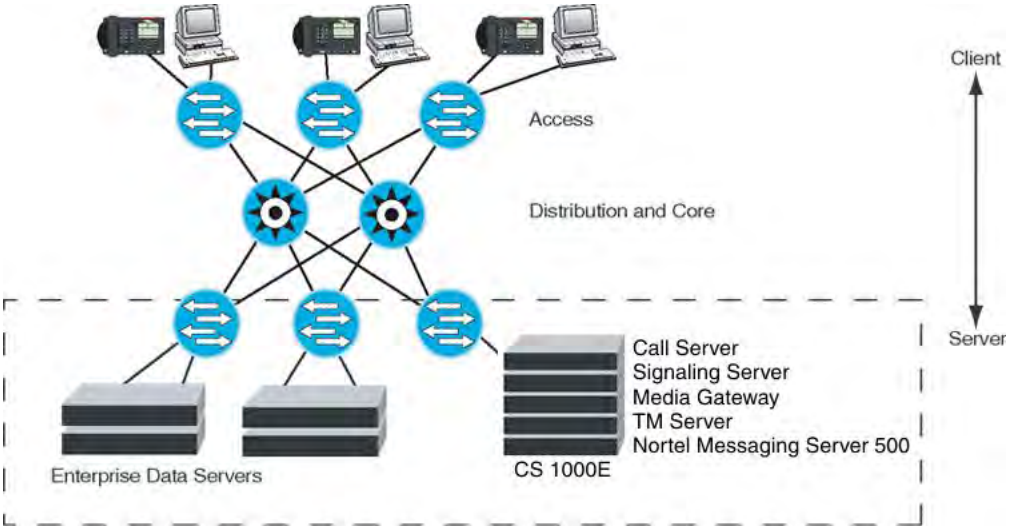


**Figure 26: Midsize campus network example**

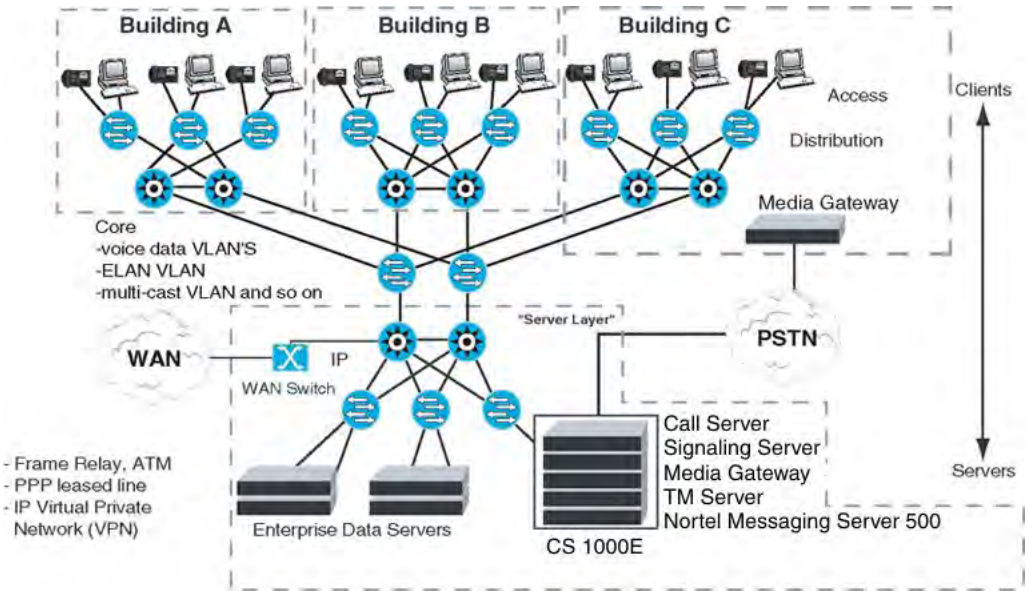


**Figure 27: Large campus network example**

**Important:**

Nortel strongly recommends that a network be designed to accommodate a larger VoIP deployment than what you install. Ensure that network administrators monitor network data traffic on a regular basis.

## Network Modeling tools

Contact a Nortel sales representative if help is needed to choose a suitable Network Modeling solution.

After you determine the network topology, evaluate the LAN and WAN platforms installed in the network.

If shared media is on the LAN, install Layer 2 switching as a minimum requirement. If there is a Layer 2 switched edge with a Layer 3 core, assess the bandwidth of the network.

The elements of a LAN/Campus network usually consist of the following:

- 100 Mbit/s bandwidth to the desktop
- high performance closet switching
- devices such as the Business Policy Switch (BPS) connected to the core network
- multigigabit riser connections
- devices such as the Passport 8600 in the core

These campus networks require only the simplest QoS mechanisms. These types of devices can take advantage of DiffServ from end-to-end.

If VoIP traffic travels on the WAN, high bandwidth can be achieved with networks connected through high speed point-to-point Digital Signal Level 3 (DS3) links or through ATM/SONET services of Optical Carrier 3 (OC-3) and higher. All optical networks with gigabit Ethernet also provide high bandwidth transport.

### Campus platforms

Document the platforms used in the campus and the following information for each switch:

- vendor
- switch model number
- hardware versions
- software versions

Typically, campus networks should be designed with high bandwidth edge switches with multigigabit Ethernet connections to a switched Layer 3 IP network.

Riser access links and Layer 3 capacity are critical areas. If the desktop switching platform provides 24 connections at 100 Mbit/s and has only four 100 Mbit/s links, a significant bottleneck can occur at the riser. Serialization and queueing delays can become an issue that requires the application of QoS mechanisms, such as 802.1Q/802.1p and/or DiffServ.

Nortel recommends migrating 100 Mbit/s riser links to Gigabit Ethernet.

**Important:**

All VoIP servers and IP Phones must be connected to Layer 2 switches.

Shared media hubs are not supported. Shared media hubs are low bandwidth devices and do not support QoS mechanisms.

## Link speeds

Link speeds in a WAN environment are usually low compared to a LAN. When you consider VoIP in a WAN environment, link speeds under 1 Mbit/s result in the serialization delay of VoIP packets, which can impair deployment. When small VoIP packets travel over a network that typically include packet sizes up to 1500 bytes, these larger packets introduce variable delay (jitter) in the network. This impacts voice quality.

To address delay on a WAN, implement the following:

- protocol prioritization
- traffic shaping (for Frame Relay)
- DiffServ
- fragmentation and interleaving (larger packet sizes incur higher serialization delays and introduce jitter into the VoIP stream)

Other vendor devices include alternative mechanisms.

If link speed and packet size are considered, the serialization delay introduced can be predicted. For more information, see Serialization delay on page 147 .

**Important:**

Nortel strongly recommends that you begin with an MTU size of 232 bytes for links under 1 Mbit/s, and adjust upwards as needed.

Some applications do not perform well with an adjusted MTU, so caution must be used when utilizing MTU.

# Link types

Identify and document the link types used in the network. A number of different link types are available in the network and each can have an impact on VoIP.

A typical campus network can have 100 Mbit/s of bandwidth going to the desk, with multigigabit riser links. Because bandwidth is plentiful, peak link utilization is the most important issue. If link utilization is averaged, it may not be accurate. A minimum of Layer 2 switching is required, with no shared media.

## Point-to-Point links (PPP)

Point-to-Point (PPP) links are direct point-to-point links, and give the network operator maximum control over QoS. PPP links provide dedicated bandwidth and flexible termination points.

## Frame Relay

Frame Relay (FR) networks provide flexibility when the requirements include a full meshed topology. The FR networks have a lower overall cost, with respect to meshed designs.

Frame Relay networks are based on a shared access model, where Data Link Connection Identifier (DLCI) numbers are used to define Permanent Virtual Circuits (PVCs) in the network.

QoS in a Frame Relay network is achieved by specifying a Committed Information Rate (CIR) and using separate PVC's. CIR is the level of data traffic (in bits) that the carrier agrees to handle, averaged over a period of time.

The CIR on the voice traffic PVC must be configured for the total peak traffic, because any traffic that exceeds the CIR is marked Discard Eligible (DE) and can be dropped by the carrier. This is not an acceptable condition for VoIP traffic, as real time data carrying packetized voice cannot be retransmitted.

Ensure you understand the design of the carrier network, how much traffic is currently being transported, and if any type of Service Level Agreement (SLA), other than CIR, is offered.

The WAN access platform in the network can help ensure that VoIP traffic does not exceed the CIR on the PVC. Protocol prioritization, traffic shaping, and fragmentation can insure that the VoIP traffic is transmitted first and does not exceed the CIR on the PVC.

### Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) can provide a Constant Bit Rate (CBR) service, by dedicating a channel with a fixed bandwidth based on the applications needs.

Using ATM as a transport for VoIP adds overhead associated with ATM. A G.711 codec with 20 millisecond (ms) voice payload, when the associated TCP, UDP, and RTP header information is added, can become a 200-byte frame.

Using ATM for transport requires that you segment the frame to fit into multiple cells. This adds an additional 10 to 15 percent of overhead. The G.729 codec significantly reduces the frame size to 60 bytes, so codec selection is crucial for the WAN.

### Virtual Private Network

A Virtual Private Network (VPN) uses the public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. Encryption and other security mechanisms are used to ensure that only authorized users can access the network and that the data cannot be intercepted.

For more information about security management, see *Security Management Fundamentals, NN43001-604*.

## Link utilization assessment

To support VoIP over WAN links, it is important to assess link utilization. There are several ways to gather statistical information on a WAN link. Tools, such as an existing network management system, should have the ability to poll routers through SNMP and collect the statistics over a period of time about use of a given WAN link.

Other methods of assessment include the use of imbedded Remote Monitoring (RMON) and external RMON probes installed to gather statistical information, including link utilization.

Over low bandwidth connections, the amount of VoIP traffic should be limited to a percentage of the bandwidth of the connection. Use the limit to minimize the maximum queueing delay that the VoIP traffic experiences over low bandwidth connections.

When you use distributed or survivable media gateways, ensure you monitor and reengineer the link utilization on a regular basis. For information about estimating ELAN traffic, see the following documents:

- *Communication Server 1000M and Meridian 1 Small System Planning and Engineering, NN43011-220*
- *Communication Server 1000M and Meridian 1 Large System Planning and Engineering, NN43021-220*
- *Communication Server 1000E Planning and Engineering , NN43041-220*

For more information about Bandwidth Management of VoIP calls, see VoIP Bandwidth Management zones on page 73.

## Assess link use

WAN links are the highest repeating expenses in the network and they often cause capacity problems. Unlike LAN bandwidth, which is virtually free and easily implemented, WAN links take time to finance, provision, and upgrade, especially inter-LATA (Local Access and Transport Area) and international links. For these reasons, it is important to determine the state of WAN links in the intranet before you install the network.

**Important:**

The use of QoS mechanisms that prioritize voice over data traffic effectively increases the amount of bandwidth available to voice traffic.

Perform the following steps to assess the link utilization.

### Assessing link utilization

1. Obtain a current topology map and link utilization report of the intranet.
2. Visually inspect the topology map to reveal which WAN links are likely to deliver IP Line traffic, alternately, use the Traceroute tool (see Network performance measurement tools on page 124).
3. Determine the current utilization of the WAN links and note the reporting window that appears in the link utilization report.

   For example, link use can be averaged over a week, a day, or an hour.
4. Obtain the busy period (peak hour) use of the link.
5. As WAN links are full duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.
6. Assess how much spare capacity is available.

   Enterprise intranets are subject to capacity planning policies that ensure capacity usage remains below a predetermined level.

   For example, a planning policy states that the use of a 56 kbit/s link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, perhaps 80%. The carrying capacity of the 56 kbit/s link is 28 kbit/s, and for the T1 link is 1.2288 Mbit/s. In some organizations, the thresholds can be lower than that used in this example;

in the event of link failures, there needs to be spare capacity for traffic to be rerouted.

7. Obtain the QoS parameters (in addition to the physical link capacity), especially the Committed Information Rate (CIR) for Frame Relay and Maximum Cell Rate (MCR) for ATM.

   Some WAN links can be provisioned on top of Layer 2 services, such as Frame Relay and ATM; the router-to-router link is actually a virtual circuit, which is subject to a physical capacity and a logical capacity limit.

8. The difference between the current capacity, and its allowable limit, is the available VoIP capacity.

   For example, a T1 link used at 48% during the peak hour, with a planning limit of 80%, has an available capacity of about 492 kbit/s.

# Traffic flows in the network

Identify traffic flows in the network by using an existing Network Management System (NMS) or another passive tool, such as a packet sniffer. These tools identify protocol distribution in the network and traffic flow between devices. RMON probes and devices with embedded RMON capability can also help the network designer determine where traffic flows occur.

Assess traffic flows over a period of time (a week or longer depending on the complexity of the network). Observe the peak times of the day, the week, and the month to determine the highest periods of use.

After traffic flows are identified, determine bandwidth requirements using tools such as a VoIP bandwidth calculator. Ask your Nortel representative for the VoIP bandwidth calculator spreadsheet. For more information, see VoIP Bandwidth Demand Calculator on page 136.

## Available traffic tools

There are many tools available to assess network traffic, such as:

- Traceroute
- Call Detail Record
- Traffic study
- Network Diagnostic Utilities (See Network Diagnostic Utilities on page 214.)

### Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. The router must instead throw away the packet and return to the originating IP address an ICMP time exceeded message. Traceroute uses the message by sending an IP datagram with a TTL of 1 to the specified destination host.

The first router to handle the datagram sends back a time exceeded message. This identifies the first router on the route. Traceroute then sends out a datagram with a TTL of 2, which

causes the second router on the route to return a time exceeded message (and so on) until all hops have been identified. The traceroute IP datagram has a UDP Port number unlikely to be in use at the destination (usually > 30 000), which causes the destination to return a port unreachable ICMP packet, thereby identifying the destination host.

Traceroute can be used to measure roundtrip times to all hops along a route, thereby identifying bottlenecks in the network.

### Call Detail Record

Obtain a Call Detail Record (CDR) to locate the VoIP traffic flows in the network. The CDR can help identify the network routes that VoIP will use.

The peak values for time of day, day of week, and day of month must be considered to ensure consistent voice quality.

For more information, see *Call Detail Recording Fundamentals, NN43001-550*.

### Traffic study

Traffic is a measurement of specific resource activity level. LD 02 has been reserved to schedule and select the traffic study options.

A network traffic study provides information, such as:

- the amount of call traffic on each choice in each route list
- the number of calls going out on expensive routes in each route list
- queueing activity (off-hook queueing and call back queueing) and the length of time users queue on average

For more information about traffic studies, see the following resources:

- *Traffic Measurement Formats and Output Reference, NN43001-750*.
- LD 02 in *Software Input Output Reference — Administration, NN43001-611*.

## Service level agreements

As part of a service level agreement, the service provider should guarantee a certain amount of bandwidth.

Whether a home user on a cable or DSL connection, or a large network customer using Frame Relay, the service provider must guarantee bandwidth for VoIP.

Guaranteed bandwidth in Frame Relay, for example, is known as Committed Information Rate (CIR). The guaranteed bandwidth must be sufficient to accommodate all of the network traffic. Ensure that the CIR rate contracted is received when you lease a connection.

Exercise caution if service level agreements are not available.

# Network planning

Perform the following actions before you configure Bandwidth Management in a Communication Server 1000 network:

- Main Office and Branch Office need to have the same VPNI setting to ensure correct bandwidth management control by the Main Office. Another reason to have the same VPNI setting across call servers is to support bandwidth management for Network Wide Virtual Office (NWVO). Also, two systems within the same LAN would require the same VPNI setting to ensure INTRAZONE call treatment.
- Choose unique Bandwidth zone numbers for all Call Servers in the network to use when configuring the endpoints (telephones and gateways) on the Call Server.
- Choose the same zone number for Virtual trunk resources for all Call servers within the same network (for example, Main Office and Branch Office configuration or MG 1000B groups or call servers within one LAN).
- Choose the codecs to enable on each Call Server.
- Identify the interzone codec strategy (BB or BQ) for each zone in the network.
- Identify the intrazone codec strategy (BB or BQ) for each zone in the network.
- Calculate the bandwidth available for intrazone calls for each zone in the network.
- Calculate the available bandwidth for interzone calls for each zone in the network.
- Calculate the available bandwidth for intrazone calls.

**⚠ Caution:**

**Service Interruption**

If the network is planned so IP Phones use a different route to the main office than the MG 1000B Terminal Proxy Server (TPS), a fault condition can occur. When the MG 1000B TPS can ping the main office but the IP Phone cannot ping the main office due to a network outage, an IP Phone 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.

# Network Performance Measurement

This section describes the criteria required to achieve excellent voice quality.

## Performance criteria

To achieve excellence in voice quality you need the following elements:

- a properly engineered network
- good network equipment and redundancy
- adequate bandwidth for peak usage
- use of QoS mechanisms
- ongoing monitoring and maintenance

If the previous elements are not present, VoIP performance suffers.

The network should also meet the following specifications:

- End-to-end packet delay: Packet delay is the point-to-point, one-way delay between the time a packet is sent to the time it is received at the remote end. It is comprised of delays at the Voice Gateway Media Card, Internet Telephone, and the IP network. To minimize delays, the IP Telephony node and Internet Telephonemust be located to minimize the number of hops to the network backbone or WAN.

  **Important:**

  Nortel recommends an end-to-end delay of <= 50 ms on the IP network to ensure good voice quality. The 50 ms does not include the built-in delay of the Voice Gateway Media Card and IP Phone.

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

  **Important:**

  For high-quality voice transmission, the long term average packet loss between the IP Phones and the Voice Gateway Media Card TLAN network interface must be < 1%, and the short term packet loss must not exceed 5% in any 10-second interval.

  **Important:**

  Nortel strongly recommends that you use the G.711 codec with the following configuration:

  - end-to end delay less than 150 ms one way (network delay + packetization delay + jitter buffer delay < 150)
  - packet loss less than 0.5% (approaching 0%)
  - maximum jitter buffer setting for IP Phone as low as possible (maximum 100 ms)

Packet loss on the ELAN network interface can cause

- communication problems between the Call Server and the Voice Gateway Media Cards
- lost SNMP alarms
- other signaling related problems

**Important:**

Because the ELAN network is a Layer 2 Switched LAN, the packet loss must be zero. If packet loss is experienced, its source must be investigated and eliminated. For reliable signaling communication on the ELAN network interface, the packet loss must be < 1%.

## Proactive Voice Quality management

Proactive Voice Quality management (PVQ) allows the user to monitor the voice quality of Voice over Internet Protocol (VoIP) calls on an ongoing basis and detect specific problems when they occur. Alarms and traffic reports are used to implement this.

Four metrics on voice quality are collected on every call: packet loss, latency, jitter, and R-value. The metrics are analyzed to determine if an alarm should be generated. The metrics are also aggregated and reported, along with other information, in Traffic Report 16.

The R-level metric is calculated only for those IP Phones equipped with a firmware version of 2.0 or higher.

A PVQ alarm is generated whenever a metric exceeds a given threshold. The thresholds are user defined in LD 117 at a Call Server and propagate throughout the system. Listed in order of increasing severity, the threshold levels include: good, warning, and unacceptable.

The following types of PVQ alarms exist:

- Alarms generated on a per zone basis (zone based) — generated if the aggregate metrics for a particular zone, such as a branch office, exceeds a warning or unacceptable threshold. These alarms are generated by the Call Server.
- Alarms generated on a per call basis — each call is monitored and an alarm generated if any metric meets or exceeds a warning or unacceptable threshold. These alarms are generated by the Signaling Server.

The user can configure a Notification Level to control when and how often an alarm is generated. This capability is useful when many alarms are generated, but most are minor and relate to potential system capacity issues rather than voice quality. It is also useful when a user wants to monitor a particular area of a network, such as a branch office. Notification levels are defined in LD 117.

## Network performance measurement tools

Ping and traceroute are standard IP tools that are usually included with a network host TCP/IP stack. QoS measurement tools and packages are commonly available that include delay

monitoring tools, which include features like timestamping, plotting, and computation of standard deviation. For information about network performance measurement tools, see

- QoS monitoring and reporting tools on page 213
- Proactive Voice Quality management on page 124
- *IP Phones Fundamentals, NN43001-368*

The following measuring tools are based on the Internet Control Messaging Protocol (ICMP):

- Ping — sends ICMP echo requests
- Traceroute — sends packets to unequipped port numbers and processes to create ICMP destination unavailable messages

Both ping and traceroute are basic measuring tools that can be used to assess the IP Line network and are standard utilities that come with most commercial operating systems. Ping is used to measure the round trip delay of a packet and the percentage of packet loss. Traceroute breaks down delay segments of a source destination pair and any hops in between to accumulate measurements.

There are several third-party applications that perform data collection similar to ping and traceroute, but also analyze data and plot performance charts. The use of ping and traceroute to collect data for manual analysis is labor intensive; however, they provide information as useful as the more sophisticated applications.

The following network performance evaluation overview assumes that the ping program is available on a PC, or a network management tool is available to collect delay and loss data and to access the LAN that connects to the router to the intranet.

### Evaluating network performance

1. Use ping or an equivalent tool to collect round-trip delay (in ms) and loss (in%) data.
2. Divide the delay (determined in step 1 on page 125) by 2 to approximate one-way delay and add 93 ms to adjust for ITG processing and buffering time.
3. Use a QoS chart, or Table 32: QoS levels on page 161, to predict the QoS categories: Excellent, Good, Fair or Poor.
4. If a customer wants to manage the QoS in a more detailed fashion, rebalance the values of delay compared to loss by adjusting system parameters, such as preferred codec, payload size, and routing algorithm, to move the resulting QoS among different categories.
5. If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

## Network availability

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

Network availability is dependent on the availability of a survivable, redundant network. A redundant network should include the following elements to ensure survivability:

- redundant devices, such as
  - interfaces
  - processor cards
  - power supplies in routers and switches
- resilient networking protocols
- multiple physical connections, such as copper or fiber
- backup power sources

## Media Security

Media Security enables two endpoints capable of Secure Real-Time Transport Protocol (SRTP) connections to engage in secure media exchanges. For calls that pass over IP systems only, Media Security can provide end-to-end encryption of the call if both endpoints can support SRTP connections. If you configure Media Security to use the Media Security Always CoS, it blocks any calls that cannot be encrypted.

When you assess the reliability of the network, be aware that the Media Security feature, if configured to use the Media Security Always CoS, can block a call if any of the following conditions is valid:

- One of the telephones in the call is an IP Phone registered on the same Call Server as the other endpoint, but does not support Media Security.
- One of the telephones in the call is a nonIP phone on the same Call Server as the other endpoint, but a Voice Gateway TN resource that supports SRTP is not available.
- One of the telephones in the call is configured to use the Media Security Always CoS, and the trunk is an H.323 trunk or a SIP trunk configured to use the Media Security Never CoS.
- One of the telephones in the call is configured to use the Media Security Always CoS, and the far end is an IP Phone, media gateway, or media server that does not support Media Security or is incompatible with the SRTP key exchange protocol used by Communication Server 1000 SIP Virtual Trunk (VTRK) Gateway.

You can use the Traffic Reports available in LD 2 to determine the cause of a call failure if you suspect Media Security is blocking calls, as shown in Table 18: Traffic reports for blocked calls on page 127.

**Table 18: Traffic reports for blocked calls**

| Counter | Meaning | Description |
|---|---|---|
| cfnp | Calls failed due to near end policy. | A high value for this counter indicates that call attempts are being made between Media Security Always (MSAW) and Media Security Never (MSNV) types of devices. |
| cfnr | Calls failed due to near end resources. | This counter indicates the number of calls that fail because secure Digital Signal Processors (DSP) are not available. |

For more information about Traffic Reports in LD 2, see *Traffic Measurement Formats and Output Reference , NN43001-750*. If you suspect calls are being blocked because of Media Security policy restrictions imposed by your system security administrator, contact the security administrator responsible for Media Security configuration policies on your system.

For more information about Media Security, including further recommendations about configuration, see *Security Management Fundamentals, NN43001-604*.

## Determine QoS expectations

The users of corporate voice and data services expect these services to meet some perceived Quality of Service (QoS) that influences network design. The goal is to design and allocate enough resources in the network to meet the needs of the users. QoS metrics or parameters are what quantifies the needs of the user of the service.

In the context of a Meridian 1 and CS 1000M system, Figure 28: QoS parameters on page 128 shows the relationship between users and services.

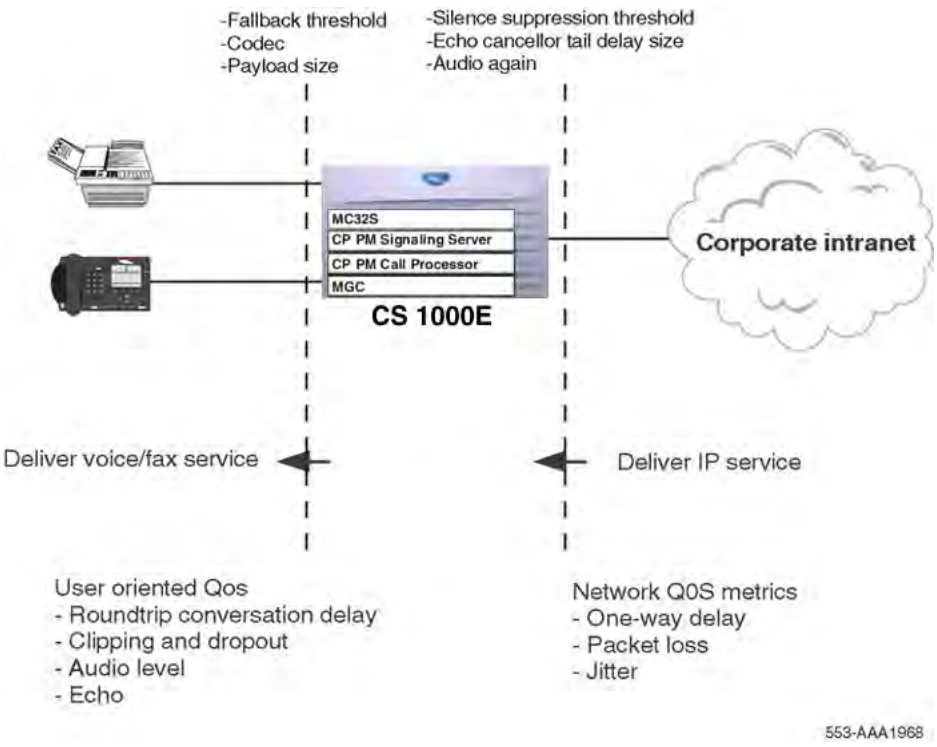


**Figure 28: QoS parameters**

In Figure 28: QoS parameters on page 128, consider the following two interfaces:

- The Meridian 1, including the IP Trunk 3.0 (or later) nodes, interfaces with the end users. Voice services offered by the Meridian 1 must meet user oriented QoS objectives.
- The IP Trunk 3.0 (or later) nodes interface with the intranet. The service provided by the intranet is best effort delivery of IP packets, not guarantee QoS for real-time voice transport. IP Trunk 3.0 (or later) translates the QoS objectives determined by the end-users into IP oriented QoS objectives. The guidelines call these objectives intranet QoS objectives.

The QoS level is a user oriented QoS metric that takes one of four settings – Excellent, Good, Fair, or Poor – that indicate the quality of voice service. IP Trunk 3.0 (or later) periodically calculates the prevailing QoS level per site pair, based on measurement of the following:

- one-way delay
- packet loss
- codec

**Important:**

Nortel strongly recommends that G.711 codec be used over high bandwidth connections, and used any time that call quality is high priority. Where call quality is high priority, sufficient bandwidth must be provided for the VoIP application. The Best Quality (BQ) codec is usually chosen and configured as G.711 within the zone configuration (intrazone).

Use the G.729 codec to compress voice traffic over low bandwidth connections when bandwidth considerations take precedence over call quality. The Best Bandwidth (BB) codec is usually chosen and configured to G.729A or G.729AB between zones (interzone).

Codec details are then configured on the Signaling Server through Communication Server 1000 Element Manager.

Figure 29: QoS levels with G.729A/AB codec on page 130, Figure 30: QoS level with G.711 codec on page 131, and Figure 31: QoS level with G.723 codec on page 131 are derived from the ITU T G.107 Transmission Rating Model. These diagrams show the operating regions in terms of one-way delay and packet loss for each codec. Note that among the codecs, G.711 A-law/G.711 mu-law delivers the best quality for a given intranet QoS, followed by G.729AB, G.723.1 6.4 kbit/s, and G.723.1 5.3 kbit/s. These graphs determine the delay and error budget for the underlying intranet so it delivers a required quality of voice service.

Fax is more susceptible to packet loss than is the human ear, in that quality starts to degrade when packet loss exceeds 4%. Nortel recommends that fax services be supported with IP Trunk 3.0 (or later) that operates at the Excellent or Good QoS level. Avoid offering fax services between two sites that can guarantee no better than a Fair or Poor QoS level.

## G.729AB codec

The G.729 uses less bandwidth than the G.711. If minimizing bandwidth demand is a priority, and the customer is willing to accept lesser voice quality, a G.729AB codec can be used.

Extreme care must be taken in the network design if using the G.729AB codec. The G.729AB codec has the same requirements as the G.711 codec.

Figure 29: QoS levels with G.729A/AB codec on page 130 shows the QoS levels with a G.729A/AB codec.

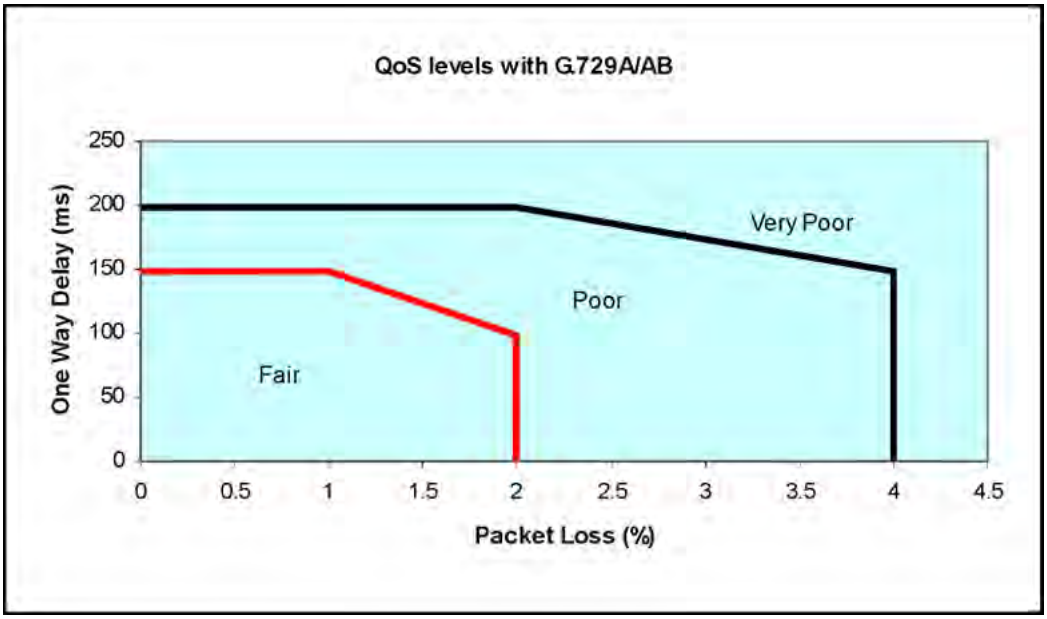


**Figure 29: QoS levels with G.729A/AB codec**

## G.711 codec

Nortel recommends that you use the G.711 codec.

Figure 30: QoS level with G.711 codec on page 131 shows the QoS levels with a G.711 codec.

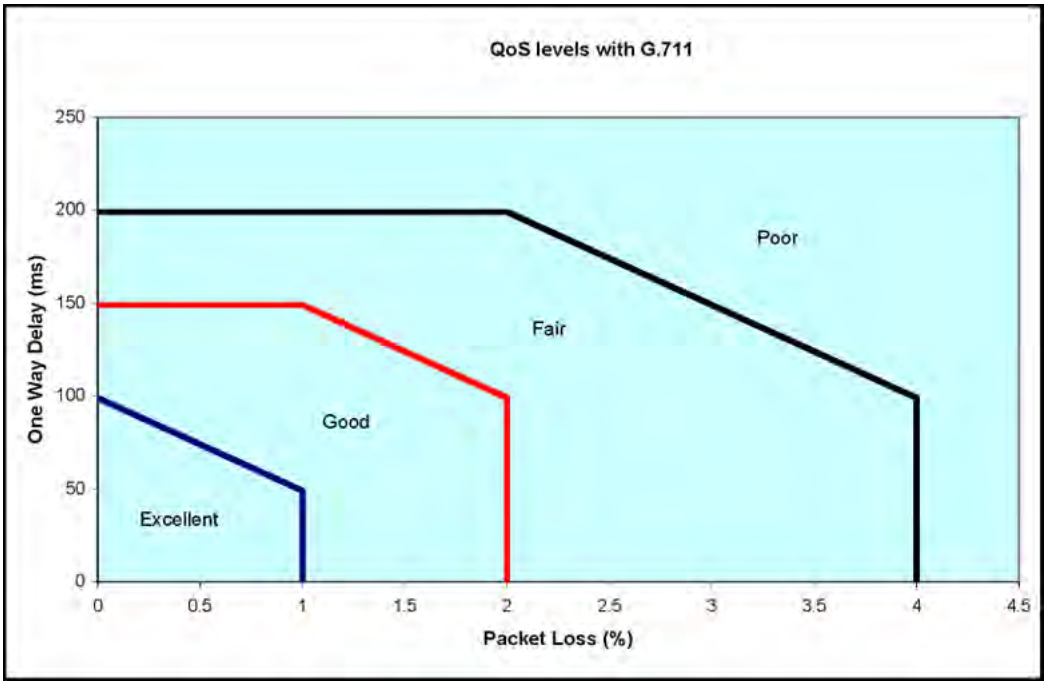


**Figure 30: QoS level with G.711 codec**

## G.723 codec

Figure 31: QoS level with G.723 codec on page 131 shows the QoS levels with a G.723 codec.

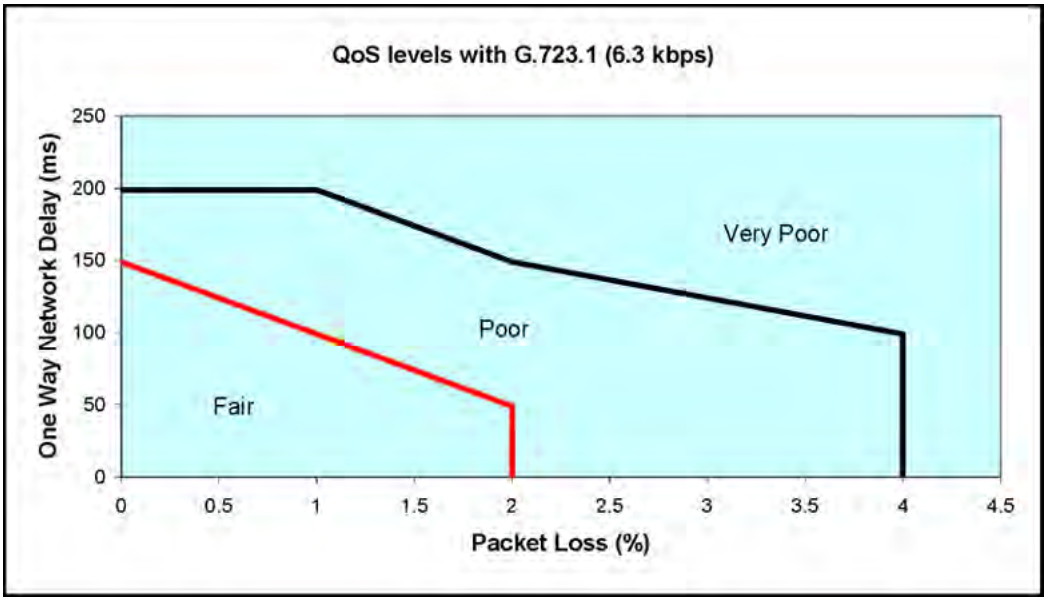


**Figure 31: QoS level with G.723 codec**

# Bandwidth

Bandwidth is the most significant parameter that affects QoS. There are two types of bandwidth:

- Available Bandwidth
- Guaranteed Bandwidth

**Important:**

The use of QoS mechanisms that prioritize voice over data traffic effectively increases the amount of available bandwidth to voice traffic.

## Available Bandwidth

Many network operators oversubscribe the bandwidth on their network to maximize the return on their network infrastructure or leased bandwidth.

Oversubscribing bandwidth means that the bandwidth a user subscribes to is not always available. All users compete for Available Bandwidth. The amount of bandwidth available to a user depends on the amount of traffic from other network users at any given time.

## Guaranteed Bandwidth

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

This can be accomplished in several ways. Sometimes, the network operator separates the subscribers by different physical or logical networks, such as Virtual Local Area Networks (VLANs) or Virtual Circuits.

In other cases, the Guaranteed Bandwidth traffic shares the same infrastructure as the Available Bandwidth traffic. This is often seen where network connections are expensive, or where the bandwidth is leased from other service providers. When both types of subscribers share the same infrastructure, the network must prioritize Guaranteed Bandwidth traffic over Available Bandwidth traffic. This ensures that when network traffic is heavy, the Guaranteed Bandwidth subscriber SLA is met.

## Bandwidth calculations

You must forecast the hundreds of call seconds for each hour (CCS) of traffic that the CS 1000 and Meridian 1 systems processes through the IP Line network. CCS traffic generated by an

IP Phone is similar to that of a digital telephone. The procedures in this section calculate the bandwidth required to support given amounts of traffic.

### Prerequisites for calculating VoIP traffic requirements

- determine the CCS/CCS rating of IP Phone

  For more information, see *Communication Server 1000M and Meridian 1 Large System Planning and Engineering, NN43021-220*.
- determine the number of IP Phones
- determine the number of subnets/servers accessed by the IP Phones

  Base all traffic data on busy hour requirements.
- calculate total LAN bandwidth requirement
- calculate WAN bandwidth requirement for each subnet or server/router
- consider the impact of incremental IP Line traffic on routers and LAN resources in the intranet. LAN segments can become saturated, and routers can experience high CPU use. Consider rerouting scenarios in a case where a link is down.

### Calculating LAN traffic

To calculate the total LAN requirement, total all sources of traffic destined for the Internet Telephony network using the same LAN.

Use the following procedures to calculate LAN traffic.

1. Add the following items to calculate the total subnet traffic (in Erlangs):

   - number of IP Phones x (CCS ÷ CCS rating)
   - number of voice gateways on the Voice Gateway Media Card
   - number of WAN connections

   **Important:**

   Each source of traffic has a different CCS rating. Calculate the subnet traffic for each source of traffic and add the amounts for the total.
2. Use the number of Erlangs to calculate the equivalent number of lines by using the calculator at the following Web site:

   http://www.erlang.com/calculator/erlb

   Assume a blocking factor of 1% (0.010).
3. Find the LAN bandwidth usage (kbit/s) in based on the codec used for the traffic source.
4. Calculate the bandwidth of a subnet using the following calculation:

   Subnet bandwidth = Total number of lines × LAN bandwidth usage
5. Repeat 1 on page 133 to 4 on page 133 for each subnet.
6. Calculate the total LAN traffic by adding the total bandwidth for each subnet calculation.

### Calculating LAN bandwidth

The following example calculates LAN bandwidth assuming half-duplex links.

Using G.729AB 30 ms, LAN bandwidth usage is 57.6 kbit/s.

The formula is:

Number of Erlangs = Number of IP Phones × (CCS ÷ 36)

1. Subnet A: 28 Internet Telephones, average 6 CCS ÷ IP Phone

   Subnet A total Erlangs = 28 × 6 ÷ 36 = 4.66 Subnet A bandwidth = 4.66 × 57.6 kbit/s = 268.4 kbit/s

2. Subnet B: 72 IP Phones, average 5 CCS ÷ Internet Telephone

   Subnet B total Erlangs = 72 × 5 ÷ 36 = 10 Subnet B bandwidth = 10 × 57.6 = 576 kbit/s

3. Subnet C: 12 IP Phones, average 6 CCS ÷ IP Phone

   Subnet C total Erlangs = 12 × 6 ÷ 36 = 2 Subnet C bandwidth = 2 × 57.6 = 115.2 kbit/s

4. Calculate the LAN Bandwidth by finding the sum of all subnet bandwidths:

   LAN Bandwidth = 268.4 + 576 + 115.2 = 959.6 kbit/s

### Calculating WAN traffic

For data rate requirements for the intranet route, calculation is based on duplex channels. The data rate for a WAN is the duplex data rate. For example, 128 kbit/s on the LAN is equal to a 64 kbit/s duplex channel on the WAN. Use the following procedure to calculate data rate requirements for the intranet route. The effects of Real-time Transport Protocol (RTP) header compression by the router are not considered in these calculations but must be included where applicable.

Use the following procedures to calculate WAN traffic.

1. Calculate the total subnet traffic using the following formula:

   Total subnet traffic = Number of IP Phones x CCS/Internet Telephone.

2. Convert to Erlangs:

   Total CCS / 36 (on the half-duplex LAN)

3. Find WAN bandwidth usage (kbit/s) from the WAN Base Bandwidth columns.
4. Calculate bandwidth for each subnet = Total Erlangs x WAN bandwidth usage.
5. Multiply bandwidth of each subnet by 1.3 to adjust for traffic peaking.
6. Repeat the procedure for each subnet.
7. Adjust WAN bandwidth to account for WAN overhead depending on the WAN technology used:

   - ATM (AAL1): multiply subnet bandwidth x 1.20 (9 bytes overhead/44 bytes payload)

- ATM (AAL5): multiply subnet bandwidth x 1.13 (6 bytes overhead/47 bytes payload)
- Frame Relay: multiply subnet bandwidth x 1.20 (6 bytes overhead/30 bytes payload – variable payload up to 4096 bytes)

**Important:**

Each WAN link must be engineered to be no more than 80% of its total bandwidth if the bandwidth is 1536 kbit/s or higher (T1 rate). If the rate is lower, up to 50% loading on the WAN is recommended.

### Calculating WAN bandwidth

The following is an example of calculating the WAN bandwidth.

1. Subnet A: 36 IP Phones, average 6 CCS/Internet Telephone
   - Total Erlangs = 36 x 6/36 = 6
   - For G.729AB 50 ms, WAN bandwidth usage is 14.4 kbit/s.
   - Subnet A WAN bandwidth = 14.4 x 6 = 86.4 kbit/s
   - Subnet A WAN bandwidth with 30% peaking

     = 86.4 x 1.3

     = 112.32 kbit/s
2. Subnet B: 72 IP Phones, average 5 CCS/IP Phone
   - Total Erlangs = 72 x 5/36 = 10
   - Subnet B WAN bandwidth = 14.4 x 10 = 144 kbit/s
   - Subnet B WAN bandwidth with 30% peaking

     = 144 x 1.3

     = 187.2 kbit/s
3. Subnet C: 12 IP Phones, average 6 CCS/IP Phone
   - Total Erlangs = 12 x 6/36 = 2
   - Subnet C WAN bandwidth = 14.43 x 2 = 28.8 kbit/s
   - Subnet C WAN bandwidth with 30% peaking

     = 28.8 x 1.3

     = 37.44 kbit/s
4. If the WAN is known to be an ATM network (AAL1), the estimated bandwidth requirements are:
   - Subnet A WAN bandwidth with ATM overhead

     = 112.32 x 1.2

     = 134.78 kbit/s.

- Subnet B WAN bandwidth with ATM overhead

  = 187.2 x 1.2

  = 224.64 kbit/s
- Subnet C WAN bandwidth with ATM overhead

  = 37.44 x 1.2

  = 44.93 kbit/s

**Important:**

Bandwidth values can vary slightly depending on the transport type.

### VoIP Bandwidth Demand Calculator

The VoIP Bandwidth Demand Calculator is a Microsoft Excel based tool that quickly determines the bandwidth requirements for a given link.

The VoIP Bandwidth Demand Calculator uses the following variables:

- number of trunks
- packetization interval
- codec (G.711, G.729, and G.723)
- link type (Frame Relay, PPP, ATM, Ethernet)
- link speed

Ask a Nortel representative for the VoIP Bandwidth Demand Calculator spreadsheet. Use the parameters in the spreadsheet and the bandwidth calculator to determine the bandwidth requirement for each client.

## Silence Suppression engineering considerations

Silence Suppression/Voice Activity Detection (VAD) results in average bandwidth savings over time, not immediately. For normal conversations, Silence Suppression creates a 40% savings in average bandwidth used. For example, a single G.729AB voice packet will still consume 30 kbit/s of bandwidth, but the average bandwidth used for the entire call would be approximately 23 kbit/s.

Calculate the average bandwidth using the formula:

Codec bandwidth from Table 6: Bandwidth estimates used by Call Admission Control on page 85 x 0.6

When voice services with multichannel requirements are extensively used in an VoIP network, such as Conference, Music-on-hold, and Message Broadcasting, additional voice traffic peaks to the IP network generated due to the simultaneous voice-traffic bursts on multiple channels on the same links.

## Queueing

Over engineering network bandwidth does not necessarily solve voice quality problems, as IP network traffic is inherently bursty in nature. At any time, a burst of packets can enter a switch. If the number of packets received in that instant is greater than the capacity of the queue for the transmitting port, then packets are lost. This situation is particularly serious on slow connections.

If a queue is busy (though not necessarily full), voice packet traffic can back up and jitter can occur if voice packets are not prioritized. Network QoS mechanisms are based on assigning different priorities to multiple queues. A voice queue is assigned a higher priority. If a specific queue is assigned only to voice traffic, then there is less chance that voice packets are discarded because the queue is too full. Network delay is reduced, as voice packets are transmitted first to minimizes delay, jitter, and loss. Perceived voice quality is greatly improved.

## Estimate network loading caused by VoIP traffic

An efficient VoIP network design requires an understanding of traffic and the underlying network that carries the traffic. To determine the network requirements of the specific system, the technician must perform the following steps.

### Prerequisites

Before bandwidth estimation can begin, obtain the following network data:

- A network topology and routing diagram.
- A list of the sites where the Communication Server 1000 Release 5.5 nodes are to be installed.
- List the sites with VoIP traffic, and the codec and frame duration (payload) to be used.
- Obtain the offered traffic in CCS for each site pair; if available, separate voice traffic from fax traffic (fax traffic sent and received).
- In a network with multiple time zones, use the same real-time busy hour varying actual clock hours at each site that yields the highest overall network traffic. Traffic to a route is the sum of voice traffic plus the larger of one-way fax traffic either sent or received.

### Determining network requirements

1. Estimate the amount of traffic processed by the Meridian 1 or Communication Server 1000 system through the IP Line network.

   See *Communication Server 1000M and Meridian 1: Large System Planning and Engineering , NN43021-220*.

2. Assess if the existing corporate intranet can adequately support voice services.

   See Configuration on page 227.

3. Organize the IP Line network into zones that represent different topographical areas of the network that are separated according to bandwidth considerations.
4. Ensure that appropriate QoS measures are implemented across the network to prioritize voice packets over data traffic.

## Example: multinode engineering

Table 19: Example: Traffic flow in a 4-node Communication Server 1000 network on page 138 summarizes traffic flow of a 4-node Communication Server 1000 network.

**Table 19: Example: Traffic flow in a 4-node Communication Server 1000 network**

| Destination Pair | Traffic in CCS |
|---|---|
| Santa Clara/Richardson | 60 |
| Santa Clara/Ottawa | 45 |
| Santa Clara/Tokyo | 15 |
| Richardson/Ottawa | 35 |
| Richardson/Tokyo | 20 |
| Ottawa/Tokyo | 18 |

The codec selection is on a per-call basis. During call setup negotiation, only the type of codec available at both destinations is selected. When no agreeable codec is available at both ends, the default codec G.711 is used.

For this example, assume that the preferred codec to handle VoIP calls in this network is G.729AB.

Table 20: Example: Incremental WAN bandwidth requirement on page 138 summarizes the WAN traffic in kbit/s for each route. The recommended incremental bandwidth requirement is included in the column adjusted for 30% traffic peaking in busy hour. This assumes no correlation and no synchronization of voice bursts in different simultaneous calls. This assumes some statistical model of granularity and distribution of voice message bursts due to Silence Suppression.

**Table 20: Example: Incremental WAN bandwidth requirement**

| Destination Pair | CCS on WAN | WAN traffic in kbit/s | Peaked WAN traffic (x1.3) in kbit/s |
|---|---|---|---|
| Santa Clara/Richardson | 60 | 18.7 | 24.3 |
| Santa Clara/Ottawa | 45 | 14.0 | 18.2 |
| Santa Clara/Tokyo | 15 | 4.7 | 6.1 |
| Richardson/Ottawa | 35 | 10.9 | 14.2 |
| Richardson/Tokyo | 20 | 6.2 | 8.1 |
| Ottawa/Tokyo | 18 | 5.6 | 7.3 |

The Santa Clara/Richardson information is calculated as follows:

- The total traffic on this route is 60 CCS. To use the preferred codec of G.729AB with a 30 ms payload, the bandwidth on the WAN is 11.2 kbit/s.
- WAN traffic is calculated by: (60/36)*11.2 = 18.7 kbit/s.
- Increasing this number by 30% gives a peak traffic rate of 24.3 kbit/s. This is the incremental bandwidth required between Santa Clara and Richardson to carry the 60 CCS voice traffic during the busy hour.

Assume that 20 CCS of the 60 CCS between Santa Clara and Richardson is fax traffic. Of the 20 CCS, 14 CCS is from Santa Clara to Richardson, and 6 CCS is from Richardson to Santa Clara. What is the WAN data rate required between those two locations?

- Traffic between the two sites can be broken down to 54 CCS from Santa Clara to Richardson, and 46 CCS from Richardson to Santa Clara, with the voice traffic 40 CCS (60 – 20) being the two-way traffic.
- The bandwidth requirement calculation would be:

  (40/36)*11.2 + (14/36)*33.6 = 25.51 kbit/s

  Where 14 CCS is the larger of two fax traffic parcels (14 CCS versus 6 CCS).
- After adjusting for peaking, the incremental data rate on the WAN for this route is 33.2 kbit/s.
- If you compare this number with 24.3 kbit/s when all 60 CCS is voice traffic, it appears that the reduction in CCS due to one:way fax traffic (20 CCS versus 14 CCS) does not compensate for the higher bandwidth requirement of a fax compared to a voice call (33.7 kbit/s versus 11.2 kbit/s).

At this point, you have enough information to load the VoIP traffic on the intranet.

After you have made a prediction on the amount of traffic on a specific link, R4-R5 is required. The R4-R5 link support the Santa Clara/Richardson, Santa Clara/Tokyo, and the Ottawa/Tokyo traffic flows; the other VoIP traffic flows do not route over R4-R5. For more information, see *Communication Server 1000M and Meridian 1 Large System Planning and Engineering, NN43021-220* and traceroute measurements. The summation of the three flows yields 93 CCS or 24 kbit/s as the incremental traffic that R4-R5 must support.

Total the traffic flow for every site pair to calculate the load at each endpoint. The following diagram shows the load on an individual link.

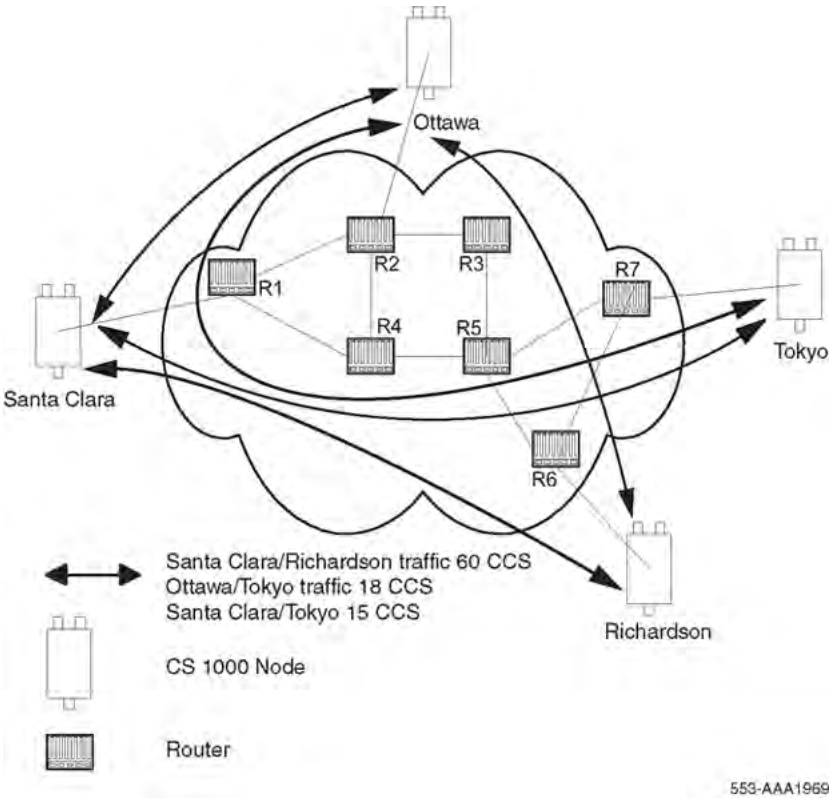


**Figure 32: Network load with VoIP traffic**

## Route Link Traffic estimation

Routing information for all source destination pairs must be recorded as part of the network assessment. This is done using the traceroute tool. An example of the output is shown below.

```
Richardson3% traceroute santa_clara_itg4
traceroute to santa_clara_itg4 (10.3.2.7), 30 hops max, 32 byte packets
     r6 (10.8.0.1) 1 ms  1 ms  1 ms
     r5 (10.18.0.2) 42 ms  44 ms  38 ms
     r4 (10.28.0.3) 78 ms  70 ms  81 ms
     r1 (10.3.0.1) 92 ms  90 ms  101 ms
    santa_clara_itg4 (10.3.2.7) 94 ms  97 ms  95 ms
```

The traceroute program is used to check if routing in the intranet is symmetric for each source destination pair. Use the **–g** loose source routing option as shown in the following command example:

```
Richardson3% traceroute :g santa_clara_itg4 richardson3
```

A trace route command (rTraceRoute) is available at the Signaling Server command line interface (CLI). This command traces a route from a remote IP Phone to another endpoint in the IP network.

The traceroute tool identifies the intranet links that transmit VoIP traffic. For example, if traceroute of four site pairs yield the results shown in Table 21: Traceroute identification of intranet links on page 141, then the load of VoIP traffic per link can be computed as shown in Table 22: Route link traffic estimation on page 141.

**Table 21: Traceroute identification of intranet links**

| Site pair | Intranet route |
|---|---|
| Santa Clara/Richardson | R1-R4-R5-R6 |
| Santa Clara/Ottawa | R1-R2 |
| Santa Clara/Tokyo | R1-R4-R5-R7 |
| Richardson/Ottawa | R2-R3-R5-R6 |

**Table 22: Route link traffic estimation**

| Links | Traffic from |
|---|---|
| R1-R4 | Santa Clara/Richardson<br>+Santa Clara/Tokyo + Ottawa/Tokyo |
| R4-R5 | Santa Clara/Richardson<br>+Santa Clara/Tokyo + Ottawa/Tokyo |
| R5-R6 | Santa Clara/Richardson<br>+Richardson/Ottawa |
| R1-R2 | Santa Clara/Ottawa + Tokyo/Ottawa |
| R5-R7 | Santa Clara/Tokyo + Ottawa/Tokyo |
| R2-R3 | Richardson/Ottawa |
| R3-R5 | Richardson/Ottawa |

## Link capacity

For each link, Table 23: Computation of link capacity as compared to ITG load on page 142 compares the available link capacity to the additional IP Trunk 3.0 (or later) load. For example, on link R4-R5, there is enough available capacity (492 kbit/s) to accommodate the additional 24 kbit/s of VoIP traffic.

**Table 23: Computation of link capacity as compared to ITG load**

| Link | | Utilization (%) | | Available capacity (kbit/s) | Incremental IP Trunk 3.0 (or later) load | | Sufficient capacity? |
|---|---|---|---|---|---|---|---|
| End points | Capacity (kbit/s) | Threshold | Used | | Site pair | Traffic (kbit/s) | |
| R1-R2 | 1536 | 80 | 75 | 76.8 | Santa Clara/ Ottawa + Ottawa/ Tokyo | 21.2 | Yes |
| R1-R4 | 1536 | 80 | 50 | 460.8 | Santa Clara/ Tokyo + Santa Clara/ Richardson + Ottawa / Tokyo | 31.4 | Yes |
| R4-R5 | 1536 | 80 | 48 | 492 | Santa Clara/ Richardson + Ottawa/ Tokyo + Santa Clara/ Tokyo | 31.4 | Yes |

Some network management systems have network planning modules that compute network flows in the manner previously described. These modules provide detailed and accurate analysis, as they consider actual node, link, and routing information. The modules also help assess network resilience by conducting link and node failure analysis. By simulating failures and reloading network and recomputed routes, the modules indicate where the network is out of capacity during failures.

## Insufficient link capacity

If there is not enough link capacity, implement one or more of the following options:

- Use the G.723 codec series. Compared to the default G.729AB codec with 30 ms payload, the G.723 codecs use 9% to 14% less bandwidth.
- Upgrade the bandwidth.

## Other intranet resource considerations

Bottlenecks caused by nonWAN resources are not frequent. For a complete assessment, consider the impact of incremental VoIP traffic on routers and LAN resources in the intranet.

Perhaps the VoIP traffic is traversing LAN segments that are saturated, or traversing routers whose CPU utilization is high.

## Delay

Delay is defined as the amount of time required for application data to reach its intended destination. Delay causes significant Quality of Experience (QoE) issues with voice and video applications. Other applications, such as Fax transmissions, with excessive delay causes the application to time out and fail.

Some applications can compensate for specified amounts of delay, but after that amount is exceeded, QoS is compromised. VoIP and gateways also provide delay compensation by using local buffering.

Delay can be fixed or variable. Variable delay is also known as jitter.

Some contributions to fixed (baseline) delay are as follows:

- Application based delay, such as:
  - voice codec processing
  - jitter buffer delay
- Serialization delay — Delay of the voice packet at each hop of the physical network, which depends on link speed (a fixed, constant value for each link).
- Propagation delay — Delay caused by the finite speed at which electronic signals can travel through a transmission medium.

In VoIP, end-to-end delay on a call is the total time elapsed from speaking into an transmitter at one end to hearing the reconstructed sound on a receiver at the other end. Delay has a significant impact on the quality of a voice call. Most listeners can detect delay greater than 100 ms. Delay becomes annoying at the following levels:

- for G.711 codec, 250 ms
- for G.729AB codec, 150 ms

Figure 33: Sources of packet delay on page 144 shows the sources of packet delay.

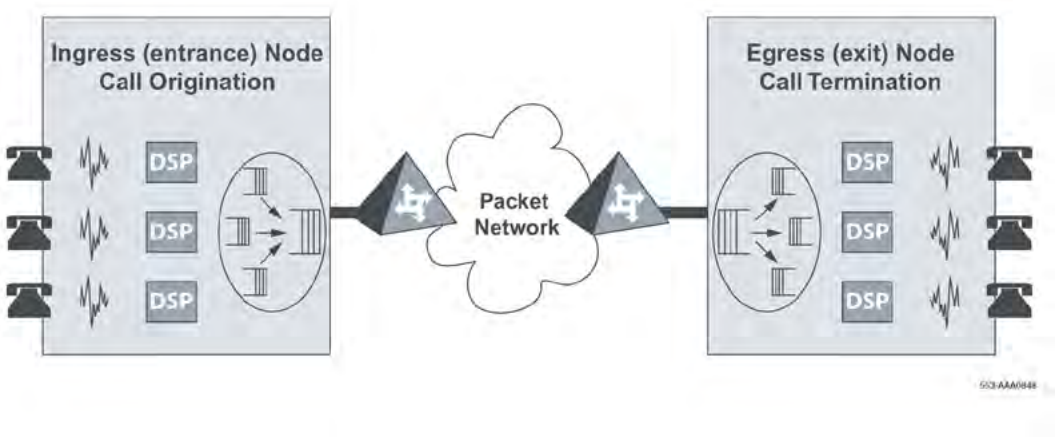


**Figure 33: Sources of packet delay**

Table 24: Delay characteristics of voice traffic on page 144 lists the network elements where delay occurs, and the type of that delay.

**Table 24: Delay characteristics of voice traffic**

| Packet action | Network element | Delay type |
|---|---|---|
| Entrance (ingress) node audio processing | Voice codec algorithmic processing | fixed delay |
| | Voice payload packetization | fixed delay |
| Entrance (ingress) node packet queueing | Packet contention for network port | variable delay |
| Data network transmission | LAN and WAN link speeds | fixed delay (per network segment type) |
| | Propagation over the network | fixed delay (per transmission distance) |
| | Packet contention at network nodes | variable delay |
| Exit (egress) node packet queueing | Packet contention for network port | variable delay |
| | Packet jitter buffer | fixed delay |
| Exit (egress) node audio processing | Voice decoder processing | fixed delay |

**Important:**

The previous table does not account for enhanced applications, such as packet encryption, tunnelling, and Virtual Private Networks (VPN), which add delay due to the buffering of the extra payload, additional Digital Signal Processing (DSP), and repacketization. These contribute to extra delay and should be included in a delay analysis.

## Effects of delay on voice quality

The overall delay budget for a voice call from the time one party speaks, to the time the voice is heard by the listener, should not exceed 150 ms for good quality voice over land line connections; although 250 ms is often tolerated for G.711 calls, if there is no packet loss the amount of delay is often longer, but unavoidable, for satellite and other types of wireless connections.

Studies show that as the 150-ms delay budget is exceeded, users perceive the delay as poor voice quality, especially for the compressed codecs. Every time a VoIP packet passes through a device or network connection, delay is introduced. A significant amount of delay is introduced over low bandwidth connections.

## Measuring end-to-end network delay

End-to-end delay and error characteristics of the intranet must be measured so the technician can configure realistic voice quality expectations for intranet voice services.

The basic tool used in IP networks to measure end-to-end network delay is the ping program. Ping takes a delay sample by sending an ICMP packet from the host of the ping program to a destination server, and waits for the packet to make a round trip.

Some implementations of ping support the -v option for setting the TOS. CS 1000 allows the 8-bit DiffServ/TOS field to be configured to any value specified by the IP network administrator for QoS management purposes. For example, a decimal value of 36 is interpreted as TOS Precedence = Priority and Reliability = High. If the -v option is not used, and if ping measurements are made on an intranet that uses prioritization based on the TOS field, the round trip time (rtt) measured is higher than the actual delay of voice packets. See Queueing on page 137.

**Important:**

Ensure that the DiffServ bytes are configured to their intended operational values before taking measurements.

CS 1000 also has a utility called remote ping (rPing) so an IP Phone can ping an IP address. The rPing command can be run from the Signaling Server OAM command line interface (CLI). See Network Diagnostic Utilities on page 214.

To ensure the delay sample results are representative of the IPLine_Node1:

1. Attach the ping host to a healthy LAN segment.
2. Attach the LAN segment to the router intended to support the IP Telephony node.
3. Choose a destination host by following the same critical guidelines as for the source host.

The size of the ping packets can be any number; the default is 60 bytes.

Sample ping output:

```
IPLine_Node1% ping -s subnetA 60
```

```
PING subnetA (10.3.2.7): 60 data bytes
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=100ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=102ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=95ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=94ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=112ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
^? --- IPLine_Node1 ping Statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip (ms) min/avg/max = 94/96/112
```

Ping results can vary.

### Assessment of sample ping output

**Important:**

The round-trip time (rtt) is indicated by the time field.

The rtt from the PING output varies as you can only obtain a delay characteristic of the intranet from repeated rtt sampling. To obtain a delay distribution, the ping tool can be embedded in a script that controls the frequency of the ping probes and timestamps and stores the samples in a raw data file. The file can then be analyzed later using a spreadsheet or another application. The technician can also check if the intranet network management software includes delay measurement modules that can obtain a delay distribution for a specific route.

Delay characteristics vary depending on the site pair and the time-of-day. The site pair is defined as the measurement between the host IP Line and the remote subnet, for example, IP Line to subnet A in Figure 27: Large campus network example on page 115. The assessment of the intranet must include taking delay measurements for each IP Line site pair. If there is a significant variation of traffic on the intranet, include ping samples during the intranet peak hour. For a complete assessment of delay characteristics of the intranet, obtain ping measurements over a period of at least one week.

## Components of delay

End-to-end delay is caused by many components, such as:

- Propagation delay
- Serialization delay
- queueing delay
- Routing and hop count
- IP Trunk 3.0 (or later) system delay

### Propagation delay

Propagation delay is affected by the mileage and medium of links traversed. Within an average size country, one-way propagation delay over terrestrial lines is under 18 ms; within the U.S., the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long haul and transoceanic circuits, use the rule-of-thumb of 1 ms per 100 terrestrial miles.

If a circuit goes through a satellite system, estimate each hop between earth stations to contribute 260 ms to the propagation delay.

### Serialization delay

Serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is calculated using the following formula:

8 * (IP packet size in bytes) / (link bandwidth in kbit/s)

Table 25: Serialization delay characteristics (in ms) for different packet sizes and link speeds on page 147 shows the serialization delay (in ms) for different packet sizes and link speeds.

**Table 25: Serialization delay characteristics (in ms) for different packet sizes and link speeds**

| Link speed in Kbit/s | Packet size | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 40 bytes | 80 bytes | 88 bytes | 136 bytes | 184 bytes | 232 bytes | 280 bytes | 520 bytes | 1 KB | 1.48 KB |
| 56 | 5.7 | 11.4 | 12.5 | 19.4 | 26. | 33.1 | 40.0 | 74.2 | 146.2 | 211.4 |
| 64 | 5.0 | 10.0 | 11.0 | 17.0 | 23.0 | 29.0 | 35.0 | 65.0 | 128.0 | 185.0 |
| 128 | 2.5 | 5.0 | 5.5 | 8.5 | 11.5 | 14.5 | 17.5 | 32.5 | 64.0 | 92.5 |
| 256 | 1.2 | 2.5 | 2.7 | 4.2 | 5.7 | 7.2 | 8.7 | 16.2 | 32.0 | 46.2 |
| 384 | 0.8 | 1.6 | 1.8 | 2.8 | 3.8 | 4.8 | 5.8 | 10.8 | 21.3 | 30.8 |
| 1000 | 0.3 | 0.6 | 0.7 | 1.0 | 1.4 | 1.8 | 2.2 | 4.1 | 8.1 | 11.8 |
| 1540 | 0.2 | 0.4 | 0.4 | 0.7 | 0.9 | 1.2 | 1.4 | 2.7 | 5.3 | 7.6 |
| 2048 | 0.1 | 0.3 | 0.5 | 0.71 | 0.9 | 1.09 | 2.0 | 4.0 | 4.0 | 5.7 |
| 10000 | 0.03 | 0.06 | 0.07 | 0.1 | 0.1 | 0.18 | 0.2 | 0.4 | 0.8 | 1.1 |
| 100000 | 0.003 | 0.006 | 0.007 | 0.01 | 0.015 | 0.019 | 0.022 | 0.04 | 0.08 | 0.1 |
| 150000 | 0.002 | 0.004 | 0.005 | 0.007 | 0.01 | 0.012 | 0.013 | 0.028 | 0.05 | 0.079 |

Table 26: Serialization delay on page 148 shows the serialization delay for voice packets on a 64 kbit/s and 128 kbit/s link. The serialization delay on higher speed links are considered negligible.

**Table 26: Serialization delay**

| Codec | Frame duration | Serialization delay over 64 kbit/s link (ms) | Serialization delay over 128 kbit/s link (ms) |
|---|---|---|---|
| G.711A/ G.711U | 10 ms | 14.00 | 0.88 |
| | 20 ms | 24.00 | 1.50 |
| | 30 ms | 34.00 | 2.13 |
| G.729A/ G.729AB | 10 ms | 5.25 | 0.33 |
| | 20 ms | 6.50 | 0.41 |
| | 30 ms | 7.75 | 0.48 |
| G.723.1 5.3 kbit/s | 30 ms | 6.50 | 0.41 |
| G.723.1 6.3 kbit/s | 30 ms | 7.00 | 0.44 |

## Queueing delay

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

p*p*(average intranet packet in bytes) / (1-p) / (link speed in kbit/s)

where p is the link utilization level.

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

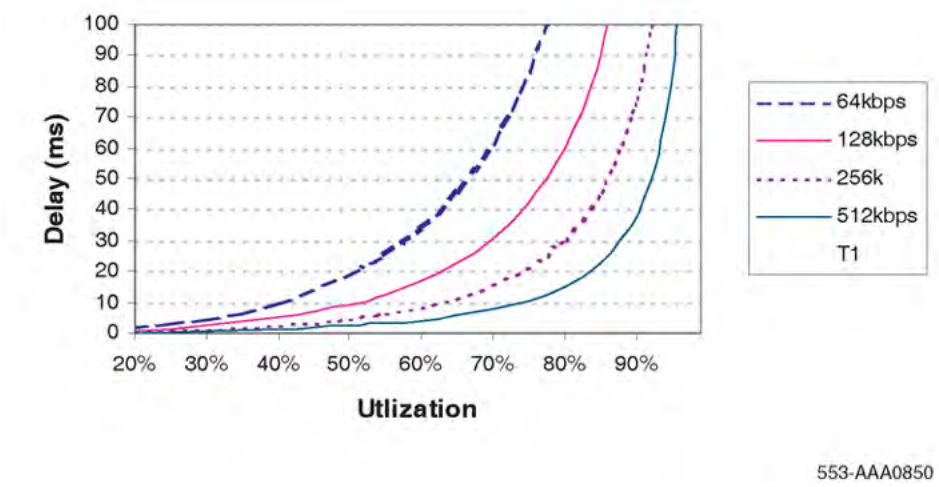


**Figure 34: Queueing delay of various links**

The previous figure shows queueing delays can be significant for links with bandwidth under 512 kbit/s. Higher speed links can tolerate much higher utilization levels.

### Routing and hop count

Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design at many levels, such as the architecture, topology, routing configuration, link, and speed.

### VoIP system delay

Together, the transmitting and receiving IP Trunk 3.0 (or later) nodes contribute a processing delay of about 33 ms to the end-to-end delay. This is the amount of time required for the encoder to analyze and packetize speech, and is required by the decoder to reconstruct and depacketize the voice packets.

There is a second component of delay that occurs on the receiving IP Trunk 3.0 (or later) node. For every call that terminates on the receiver, there is a jitter buffer which serves as a holding queue for voice packets arriving at the destination ITG. The purpose of the jitter buffer is to smooth out the effects of delay variation, so that a steady stream of voice packets can be reproduced at the destination. The default jitter buffer delay for voice is 60 ms.

### Other delay components

Other delay components, considered minor, are as follows:

- Router (transit) processing delay

  The time it takes to forward a packet from one link to another on the router. In a healthy network, router processing delay is a few milliseconds.

- LAN segment delay

The transmission and processing delay of packets through a healthy LAN subnet takes one or two milliseconds.

## Other measurement considerations

If the intranet capacity is tight and the VoIP traffic significant, consider making intranet measurements under load. Load can be applied using traffic generator tools. The amount of load should match the IP Trunk offered traffic estimated in Prerequisites on page 137.

## Reducing delays

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

- Upgrading link capacity — to reduce the serialization delay of the packet, and also reduce link utilization and queueing delay. Before you upgrade a link, the technician must check both routers connected to the link and ensure compliance with router configuration guidelines.
- Implementing QoS mechanisms

To determine the links to upgrade, list all intranet links that support the IP Line traffic. This can be derived from the traceroute output for each site pair. Use the intranet link utilization report and note the links used most often and the slowest links. Estimate the link delay of suspect links using the traceroute results.

### Example

A 256 kbit/s link from router1 to router2 has a high utilization. The following traceroute output traverses this link:

```
IPLine_Node1% traceroute SubnetA
traceroute to SubnetA (10.3.2.7), 30 hops max, 32 byte packets
  router1 (10.8.0.1) 1 ms 1 ms  1 ms
  router2 (10.18.0.2) 42 ms  44 ms  38 ms
  router3 (10.28.0.3) 78 ms  70 ms  81 ms
  router4 (10.3.0.1) 92 ms  90 ms  101 ms
  SubnetA (10.3.2.7) 94 ms  97 ms  95 ms
```

The average rtt time on the example link is 40 ms. The one-way link delay is 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of the link delay is due to queueing.

## Adjusting ping statistics

Ping statistics measure the intranet prior to CS 1000 installation, the measurement does not take into consideration the expected load created by CS 1000 users.

### One-way and round-trip

Ping statistics are based on round-trip measurements, while QoS metrics in the Transmission Rating model are one-way. Halve the delay and packet error ping statistics to ensure the comparison is valid.

### Adjustment due to IP Line processing

Ping statistics are measured from ping host to ping host. Transmission Rating QoS metrics are from end user to end user, and include components outside the intranet. The ping statistic for delay needs to be further modified by adding 93ms to account for the processing and jitter buffer delay of the nodes.

There is no need to adjust error rates.

If the intranet measurement barely meets the round-trip QoS objectives, the technician must be aware of the possibility that one-way QoS is not being met in one of the directions of flow. This can apply even if the flow is on a symmetric route due to asymmetric behavior of data processing services.

## Reducing hop count

Consider the current network topology and whether a more efficient design which reduces hop count can be implemented. Reducing hops reduces fixed and variable IP packet delay, improves VoIP QoS and can also simplify end-to-end QoS engineering for packet delay, jitter, and packet loss.

## Recording routes

The traceroute tool records routing information for all source destination pairs as part of the network assessment. An example of traceroute output is shown below:

```
ipline_node1% traceroute subnetA
traceroute to subnetA 10.3.2.7, 30 hops max, 32 byte packets
1  r6 (10.8.0.1) 1 ms  1 ms  1 ms
2  r5 (10.18.0.2) 42 ms  44 ms  38 ms
3  r4 (10.28.0.3) 78 ms  70 ms  81 ms
4  r1 (10.3.0.1) 92 ms  90 ms  101 ms
5  subnetA (10.3.2.7) 94 ms  97 ms  95 ms
```

Traceroute is also used to verify whether routing in the intranet is symmetric for each source destination pair. This is done using the **-g** loose source routing option, for example:

```
ipline_node1% traceroute -g subnetA ipline_node1
```

For information about the rTraceRoute command, see Network Diagnostic Utilities on page 214.

## Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation can overlook a substantially better route. A high delay variation can be caused by routing instability, incorrectly configured routing, inappropriate load splitting, or frequent changes to the intranet. Severe asymmetrical routing results in one site perceiving a poorer QoS than another.

The traceroute program can be used to uncover routing anomalies. Then routing implementation and policies can be audited and corrected.

# Jitter

Jitter (also known as variable delay) is the variation in the amount of time it takes for consecutive packets to travel from sender to receiver. There is a fixed baseline delay (the absolute fastest time for a voice packet to pass through the network), and a variation in packet flow. The variation in the delay is jitter.

The primary cause of jitter (variable delay) is contention (competition for network access), also known as queueing delay. Variable delays are affected by the amount of network traffic.

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

Some settings on devices such as VoIP gateways and IP Phones can compensate for a finite (specified) amount of jitter.

If an adaptive jitter buffer is used, delay is kept to a minimum during periods of low jitter. The adaptive buffer can adjust to high levels of jitter, within a limited range, during periods of high traffic volume. If the network becomes congested, jitter and packet loss can become undefined, and real-time interactive applications can become unusable.

Voice applications require the voice packets to be fed to the decoder at a constant rate. If the next voice packet does not arrive in time to take its turn to be decoded, the packet is considered lost. Packet Loss Concealment (PLC) attempts to smooth over the lost voice packet. PLC replays the previous voice packet until the next voice packet arrives. A PLC algorithm can repair losses of 40-60 ms. Longer gaps in the signal must be muted. If jitter is high, whole groups of packets can be late or lost, and output can contain muted segments.

All networks have some jitter, due to differences in delay at each network node, as packets are queued. If jitter is contained within specified limits, QoS can be maintained.

In VoIP, jitter is the total amount of variable delay encountered during the end-to-end processing of voice packets.

Jitter buffers are used on the receive side of a call to smooth out small variations in the packet time of arrival. This allows data to be unpacked and sent to the decoder as a constant stream. As all buffering increases end-to-end delay, jitter buffer length (duration) must be kept to a

minimum. If a network has been engineered to have minimal jitter, the jitter buffer can be very small.

The following factors contribute to the total variation in delay:

- packet contention during node queueing
- network conditions, such as routing and transmission queueing
- router and switch (statistical multiplexer) performance under load
- link speed
- voice and data packet size
- exit (egress) queue buffer size

Queueing delay occurs at the exit port of every device on the network.

Call Admission Control (CAC) performs packet admission and blocking functions. Voice packets are admitted to the network when the network can adequately support them. The packets are denied admission when the network cannot support them as defined in the Service Level Agreement.

When voice and data packets share a low speed WAN connection (< 1 Mbit/s), the larger data packets introduce queueing delay to the smaller voice packets waiting to queue onto the WAN connection. Therefore, the smaller voice packets do not arrive at the same fixed time interval as they are transmitted from their source. The arrival time of the voice packets varies because interjected data packets of varying sizes introduce a varying amount of jitter (queueing delay).

## Late packets

Packets that arrive outside the window allowed by the jitter buffer are discarded by IP Line. To determine which ping samples to ignore, calculate the average one-way delay based on all the samples.

To calculate late packets, double the value of the nominal jitter buffer setting. For example, assume:

- the average one-way delay is 50 ms
- the jitter buffer is configured to a nominal (or average) value of 40 ms
- the maximum value is 2 x 40 + 50 = 130 ms

Therefore, any packet with a one-way delay of greater than 130 ms is late, and must be added to the total number of packets lost.

## Adjusting jitter buffer size

The jitter buffer parameters directly affect end-to-end delay. Lowering the voice playout settings decreases one-way delay, but there is less waiting time for voice packets that arrive late.

Jitter buffer is configured on the voice gateway channels of the Voice Gateway Media Card, and are sent out to IP Phones. The jitter buffer size is configured on the DSP Profiles:

- in the IP Telephony application
- in the selected codec in Element Manager

The jitter buffer is statically configured and is the same for all devices in the network. The jitter buffer size range is 0-200 ms. The default jitter buffer value is 50 ms. However, the jitter buffer setting that is used on the Voice Gateway Media Card is a multiple of the codec frame size. The setting is automatically adjusted to be greater than or equal to the jitter buffer value configured in the DSP Profile tab. As each call is set up, the jitter buffer for each device is configured to the nearest whole number increment of the selected codec frame size.

For example, if the jitter buffer value is configured as the default 50 ms in the DSP Profiles, but a 20 ms codec is used, the jitter buffer value is configured to 60 ms, which is the nearest whole number increment.

50 ms / 20 ms = 2.5 2.5 rounded up to the nearest whole number increment is 3 3 x 20 ms = 60 ms

If the jitter buffer value is configured as zero, the depth of the jitter buffer is configured to the smallest value the device can support. In practice, the optimum depth of the jitter queue is different for each call. For telephones on a local LAN connection, a short jitter queue is desirable to minimize delay. For telephones several router hops away, a longer jitter queue is required.

Lowering the jitter buffer size decreases the one-way delay of voice packets. If the setting for the jitter buffer size is too small, packets are discarded unnecessarily. Discarded packets result in poor speech quality and can be heard as clicks or choppy speech.

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

- Check the delay variation statistics.

  Obtain the one-way delay distributions that originate from all source IP Line sites.

- Compute the standard deviation of one-way delay for every flow.

  Some traffic sources with few hop counts yield small delay variations, but it is the flows that produce great delay variations that should be used to determine whether it is acceptable to resize the jitter buffer.

- Compute the standard deviation(s) of one-way delay for that flow.

  Do not configure the jitter buffer size smaller than 2 seconds.

The IP Phone firmware must also be configured for jitter buffers. However, instead of specifying the jitter buffer size in ms, it is configured with the number of frames to be held in the jitter buffer, such as 1, 2, or 3.

**Important:**

To achieve maximum voice quality, Nortel strongly recommends that IP Phone firmware be configured with a jitter buffer size of 3; however, a well engineered network can function with a jitter buffer size of 2, which increases perceived voice quality.

## Jitter buffers

When voice and data packets share a high speed connection (> 1 Mbit/s), the jitter introduced by the WAN connection becomes insignificant. The jitter in high speed networks is affected by the buffer size of a router and the load/congestion in the router. Jitter buffers are designed to smooth out irregular packet arrival by collecting incoming packets and holding them in a buffer long enough to allow the slowest packets to arrive. The packets are then played in the correct sequence. Jitter buffers solve the late and lost packet problem, but add to total end-to-end delay.

## Jitter measurement tools

After a CS 1000 system has been installed, the average jitter experienced by IP Phones or media cards may be monitored on a per call basis by using the RTPTraceShow command from the signaling server CLI. The CS 1000 system can also be configured to transmit SNMP alarms an average jitter level is exceeded.

# Packet loss

Packet loss is the number of packets lost during transmission. It is usually measured as a percentage of the total packets exchanged.

## Physical medium loss

Loss can occur due to errors created by the physical medium used to transmit the data.

Most land line connections have very low loss, measured in Bit Error Rate (BER). Wireless connections, such as satellite, mobile, or fixed wireless networks have a high BER. The BER can vary due to the following:

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

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

## Congestion loss

Congestion loss consists of true loss (buffer overflow at router queues) and late packets. Loss also occurs when congested network nodes drop packets. The majority of packet loss is caused by congestion.

VoIP uses User Datagram Protocol (UDP). UDP is a connectionless protocol which, unlike TCP, cannot retransmit lost packets. A packet is sent from the source to the destination with no means to determine if that packet was received or not.

If a network becomes congested to the point that packets are lost, voice quality is degraded. Traffic is discarded if the transmit queue of an uplink has less available bandwidth than the total amount of bandwidth trying to use that link. This situation is also known as a bottleneck.

Congestion can lead to packet loss. Mechanisms to avoid network congestion can be used. One such mechanism is called Random Early Discard (RED), which deliberately drops packets after the network traffic reaches a specified threshold. The dropped packets cause TCP to reduce its window size and send fewer packets, thus reducing network traffic. RED provides congestion control only for applications or protocols that have the TCP-like ability to reduce network traffic.

UDP packets dropped in a network cannot be retransmitted. Flow rates are not adjusted by devices that communicate through UDP.

Without discard priorities, you must separate packets into different queues in a network node to provide different levels of service. This is expensive to implement, as only a limited number of hardware queues (usually eight or fewer) are available on networking devices. Though some devices have software based queues, their increased use reduces network node performance.

With discard priorities, although packets are placed in the same queue, they are divided into virtual subqueues, determined by their assigned discard priority. For example, if a product supports three discard priorities, the product queue provides three subqueues and; therefore, three QoS levels.

Packets are usually lost due to a router dropping packets when links are congested.

Individual packets that are delayed much more than the baseline delay (variable delay) are referred to as jitter. Excess jitter causes packet loss that can result in choppy or unintelligible speech.

Packet loss occurs

- during network congestion
- as a result of misconfigured LAN settings
- as a result of misconfigured clock settings
- if bit errors in the network

**Important:**
To achieve maximum voice quality, Nortel strongly recommends that packet loss = 0%.

Packet Loss Concealment (PLC) is used to minimize the noticeable effects of packet loss.

## Measuring end-to-end packet loss

After a CS 1000 installation, check RTPTraceShow and PVQM SNMP alarms.

The ping program also reports whether the ICMP packet successfully completed its round trip. Use the same ping host configuration to measure end-to-end error, and in making delay measurements, use the same packet size parameter.

Multiple ping samples must be used when sampling for error rate. Packet loss rate (PLR) is the error rate statistic collected by multiple ping samples. To be statistically significant, at least 300 samples must be used. Obtaining an error distribution requires that you run ping over a long period of time.

## Packet Loss Concealment

The term codec stands for coder/decoder. A codec executes a compression algorithm (a specialized computer program) that reduces the number of bytes required to encode digital data. This reduces packet size and bandwidth requirements. As well, smaller packets are less likely to be lost.

Codecs designed for packet networks, such as G.729, have built-in Packet Loss Concealment (PLC). PLC minimizes the impact of lost packets on an audio signal, by mixing in synthesized speech derived from previous packets.

When a speech codec operates in normal mode, a receiver decodes packets and sends the output to an audio port. A PLC algorithm saves a copy of the recent audio output, which is used to create a signal to replace the missing speech if lost data is encountered. How this information is used depends on the PLC algorithm. Some simple algorithms smooth over gaps in the signal to remove clicks. Other algorithms replay an earlier packet to fill in the gap. More sophisticated algorithms tweak the replacement signal to make it sound natural. The best algorithms can repair a 20 to 40 ms gap with little audible distortion. The PLC operates constantly, generating speech to replace the next packet in the event it is lost. The use of a PLC adds a small fixed delay to the call baseline delay.

PLC is necessary to achieve acceptable IP speech quality.

## Reducing packet loss

Packet loss in intranets is generally related to congestion in the network. Bottlenecks in links occur with high packet loss due to packets dropped because they arrive faster than the link

can transmit them. The task of upgrading highly utilized links can remove the source of packet loss on a particular flow. An effort to reduce hop count gives fewer opportunities for routers and links to drop packets.

Other causes of packet loss, not related to queueing delay, are as follows:

- Poor link quality — the underlying circuit could have transmission problems, high line error rates, and be subject to frequent outages. The circuit might possibly be provisioned on top of other services, such as X.25, Frame Relay, or ATM. Check with the service provider for information.
- Overloaded CPU — this is a commonly monitored statistic collected by network management systems. If a router is overloaded, it constantly performs processing intensive tasks, which impede the router from forwarding packets. Determine the CPU utilization threshold and check if a suspect router conforms to it. The router may need to be reconfigured or upgraded.
- Saturation — routers can be overworked when configured with too many high capacity and high traffic links. Ensure that routers are dimensioned according to vendor guidelines.
- LAN saturation — packets may be dropped on under engineered or faulty LAN segments.
- Jitter buffer too small — packets that arrive at the destination, but too late to be placed in the jitter buffer, should be considered lost packets.
- Frame slips — ensure that clocks are synchronized correctly.

## Network delay and packet loss evaluation example

From ping data, calculate the average one-way delay (halved from ping output and adding 93 ms IP Trunk 3.0 (or later) processing delay) and standard deviation for latency. Perform a similar calculation for packet loss without adjustment.

Add a standard deviation to the mean of both delay and loss for planning purposes. A customer might want to know whether traffic fluctuation in their intranet reduces the user QoS.

Table 27: Sample measurement results for G.729A codec on page 159 provides a sample measurement of network delay and packet loss for the G.729A codec between various nodes.

**Table 27: Sample measurement results for G.729A codec**

| Destination pair | Measured one-way delay (ms) | | Measured packet loss (%) | | Expected QoS level (See Table 32: QoS levels on page 161 ) | |
|---|---|---|---|---|---|---|
| | Mean | Mean+s | Mean | Mean+s | Mean | Mean+s |
| Santa Clara/ Richardson | 171 | 179 | 1.5 | 2.1 | Excellent | Good |
| Santa Clara/ Ottawa | 120 | 132 | 1.3 | 1.6 | Excellent | Excellent |
| Santa Clara/ Tokyo | 190 | 210 | 2.1 | 2.3 | Good | Good |
| Richardson / Ottawa | 220 | 235 | 2.4 | 2.7 | Good | Good |

As an example, the delay and loss pair of traffic from Santa Clara to Richardson (171 ms and 1.5%) will meet the excellent criterion, but their counterpart with standard deviation (179 ms and 2.1%) can achieve only good QoS.

In contrast, the site pair Santa Clara/Ottawa has both QoS levels of mean and mean+s falling in the excellent region. The customer has more confidence that during peak traffic period, the excellent service level is likely to be upheld (better than 84% chance under the assumption of Normal distribution).

## Estimate voice quality

The perceived quality of a telephone call depends on many factors, such as codec characteristics, end-to-end delay, packet loss, and the perception of the individual listener.

The E-Model Transmission Planning Tool produces a quantifiable measure of voice quality based on relevant factors. For more information about the E-Model and its application, see the ITU-T recommendations E.107 and E.108.

A simplified version of the E-Model is applied to provide an estimate of the voice quality that the user can expect, based on various configuration choices and network performance metrics.

The simplified E-Model is as follows:

R = 94 – Ic – Id – Ip

- Ic = (see Table 28: Impairment factors of codecs on page 160)
- Id = delay impairment (see Table 29: Impairment factors due to network delay on page 160)
- Ip = packet loss impairment (see Table 30: Impairment factors due to packet loss on page 161)

**Important:**

This model takes into account some characteristics of the IP Phone and; therefore, the impairment factors are not identical to those shown in the ITU-T standards.

See Table 31: R value translation on page 161 for the translation of R values into user satisfaction levels.

**Table 28: Impairment factors of codecs**

| Codec | Codec impairment (Ic) (ms frames) |
|---|---|
| G.711 | 0 |
| G.711 a-law | 8 |
| G.711 mu-law | 0 |
| G.723.1 | 4 |
| G.729A G.729AB | 18 |
| G.729A/AB | 11 - 20 or 30 |
| G.729A/AB | 16 - 40 or 50 |
| G.723.1 (5.3 kbit/s) | 19 |
| G.723.1 (6.3 kbit/s) | 15 |

**Table 29: Impairment factors due to network delay**

| Network delay* (ms) | Delay impairment (Id) |
|---|---|
| 0–49 | 0 |
| 50–99 | 5 |
| 100–149 | 10 |
| 150–199 | 15 |
| 200–249 | 20 |
| 250–299 | 25 |
| * Network delay is the average one-way network delay plus packetization and jitter buffer delay. | |

**Table 30: Impairment factors due to packet loss**

| Packet loss (%) | Packet Lose Impairment (Ip) |
|---|---|
| 0 | 0 |
| 1 | 4 |
| 2 | 8 |
| 4 | 15 |
| 8 | 25 |

**Table 31: R value translation**

| R Value (lower limit) | MOS | User Satisfaction |
|---|---|---|
| 90 | 4.5 | Very satisfied |
| 80 | 4.0 | Satisfied |
| 70 | 3.5 | Some users dissatisfied |
| 60 | 3.0 | Many users dissatisfied |
| 50 | 2.5 | Nearly all users dissatisfied |
| 0 | 1 | Not recommended |

Use Table 32: QoS levels on page 161 to estimate the voice quality level based on performance measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10 ms, respectively. The techniques used to determine and apply the information in this table are proprietary to Nortel.

**Table 32: QoS levels**

| Network delay (ms) | Packet loss (%) | Voice quality level | | |
|---|---|---|---|---|
| | | G.711 20 | G.729A/AB 30 | G.723.1 (6.3 kbit/s) 30 |
| 0 – 49 | 0 | excellent | good | fair |
| 49 | 1 | excellent | fair | fair |
| 49 | 2 | good | fair | fair |
| 49 | 4 | fair | poor | poor |
| 49 | 8 | poor | not recommended | not recommended |
| 50 – 99 | 0 | excellent | fair | fair |
| 99 | 1 | good | fair | fair |
| 99 | 2 | good | fair | poor |

| Network delay (ms) | Packet loss (%) | Voice quality level | | |
|---|---|---|---|---|
| | | G.711 20 | G.729A/AB 30 | G.723.1 (6.3 kbit/s) 30 |
| 99 | 4 | fair | poor | poor |
| 99 | 8 | poor | not recommended | not recommended |
| 100 – 149 | 0 | good | fair | fair |
| 149 | 1 | good | fair | poor |
| 149 | 2 | fair | poor | poor |
| 149 | 4 | fair | poor | not recommended |
| 149 | 8 | poor | not recommended | not recommended |
| 150 – 199 | 0 | fair | poor | poor |
| 199 | 1 | fair | poor | good |
| 199 | 2 | fair | poor | fair |
| 199 | 4 | poor | not recommended | not recommended |
| 199 | 8 | not recommended | not recommended | not recommended |
| 200 – 249 | 0 | poor | not recommended | not recommended |
| 249 | 1 | poor | not recommended | not recommended |
| 249 | 2 | poor | not recommended | not recommended |
| 249 | 4 | not recommended | not recommended | not recommended |
| 249 | 8 | not recommended | not recommended | not recommended |
| 250 – 299 | 0 | poor | not recommended | not recommended |
| 299 | 1 | poor | not recommended | not recommended |
| 299 | 2 | poor | not recommended | not recommended |
| 299 | 4 | not recommended | not recommended | not recommended |
| 299 | 8 | not recommended | not recommended | not recommended |

**Note:**

The QoS levels are equivalent to the following MOS values: excellent = 4.5, good = 4, fair = 3, poor = 2, and not recommended = less than 2.

## Sample scenarios

The following examples provide sample scenarios.

### Scenario 1

A local LAN has the following characteristics:

- G.711 codec
- 20 ms network delay
- 0.5% packet loss

To calculate R = 94 - Ic - Id - Ip, use Table 28: Impairment factors of codecs on page 160, Table 29: Impairment factors due to network delay on page 160, and Table 30: Impairment factors due to packet loss on page 161:

- G.711 codec: Ic = 0
- 20 ms network delay: Id = 0
- 0.5% packet loss: Ip = 2

Then:

R = 94 - 0 - 0 - 2 R = 92

Use the values in Table 32: QoS levels on page 161, a value of 92 means the users are very satisfied.

### Scenario 2

A campus network has the following characteristics:

- G.711 codec
- 50 ms delay
- 1.0% packet loss

To calculate R = 94 - Ic - Id - Ip, use Table 28: Impairment factors of codecs on page 160, Table 29: Impairment factors due to network delay on page 160, and Table 30: Impairment factors due to packet loss on page 161:

- G.711 codec: Ic = 0
- 20 ms network delay: Id = 5
- 0.5% packet loss: Ip = 4

Then:

R = 94 - 0 - 5 - 4 R = 85

Use the values in Table 32: QoS levels on page 161, a value of 85 means that the users are satisfied.

### Scenario 3

A WAN has the following characteristics:

- G.729 codec
- 30 ms network delay
- 2% packet loss

To calculate R = 94 - Ic - Id - Ip, use Table 28: Impairment factors of codecs on page 160, Table 29: Impairment factors due to network delay on page 160, and Table 30: Impairment factors due to packet loss on page 161:

- G.711 codec: Ic = 11
- 20 ms network delay: Id = 5
- 0.5% packet loss: Ip = 8

Then:

R = 94 - 11 - 5 - 8 R = 70

Use the values in Table 32: QoS levels on page 161, a value of 70 means some users are dissatisfied.

## Expected voice quality evaluation

At the end of measurement and analysis, there should be a good indication if the corporate intranet in its present state can deliver adequate voice and fax services. Looking at the Expected QoS level column in Table 27: Sample measurement results for G.729A codec on page 159, the QoS level for each site pair can be gauged.

In order to offer voice and fax services over the intranet, keep the network within Good or Excellent QoS level at the Mean+s operating region. Fax services should not be offered on routes that have only Fair or Poor QoS levels.

If the expected QoS levels on some or all routes fall short of Good, evaluate the options and costs to upgrade the intranet. Estimate the reduction in one-way delay that must be achieved to raise the QoS level. You can raise QoS levels through a link upgrade, topology change, or an implementation of QoS in the network.

A decision can be made to keep costs down and accept a temporary Fair QoS level for a selected route. In this case, having made a calculated trade-off in quality, carefully monitor the QoS level, reset expectations with the end users, and be receptive to user feedback.

**Important:**

Nortel strongly recommends a minimum R-value of 70.

# LAN design

This section describes the requirements to create and maintain a robust, redundant server network.

## CS 1000 configurations

A CS 1000 system has 3 basic configurations designed to meet varying network requirements:

- The “Normal” configuration (this configuration is also known as a Routed configuration) suitable to larger installations which deploy multiple ELAN subnets or multiple CS 1000 systems within the same UCM Security Domain.
- The “Small” configuration suitable for single system installations with a single ELAN subnet interconnecting all of the CS 1000 dependent elements.
- The “Managed Services” configuration which is suited to installations where complete isolation between the ELAN or “Signaling and Management Network” and the various “Enterprise Networks” is required.

Due to the requirement to ensure communication between the UCM security server and elements located on multiple ELAN subnets, configurations involving non-routable or non-extended ELAN subnets require the configuration of separate security servers for each ELAN subnet. An example of this is the pre-Release 6.0 customer network configuration, where main and branch office ELANs are segregated from each other, as shown in the following figure.

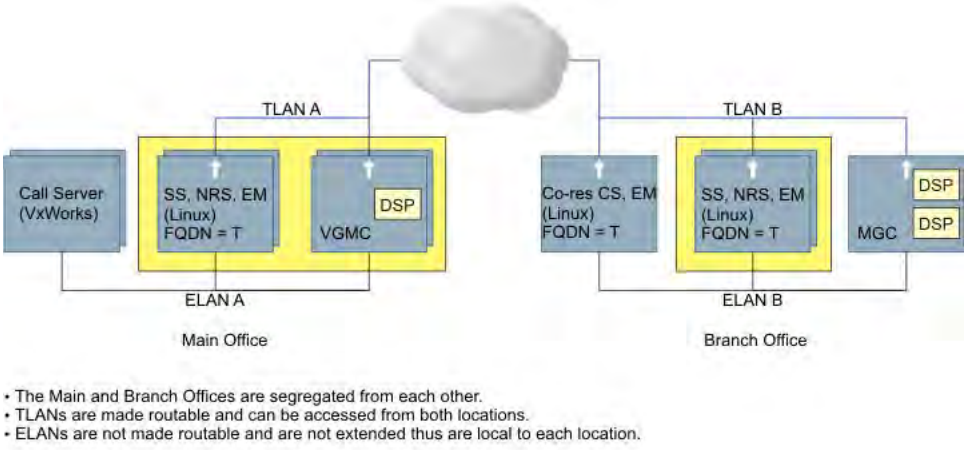


**Figure 35: Pre-Release 6.0 customer network configuration**

When upgrading to Release 6.0 or higher, if it is still desired that the ELANs remain segregated (non-routable or non-extended), you must configure separate UCM primary security servers for each location, as shown in the following figure.

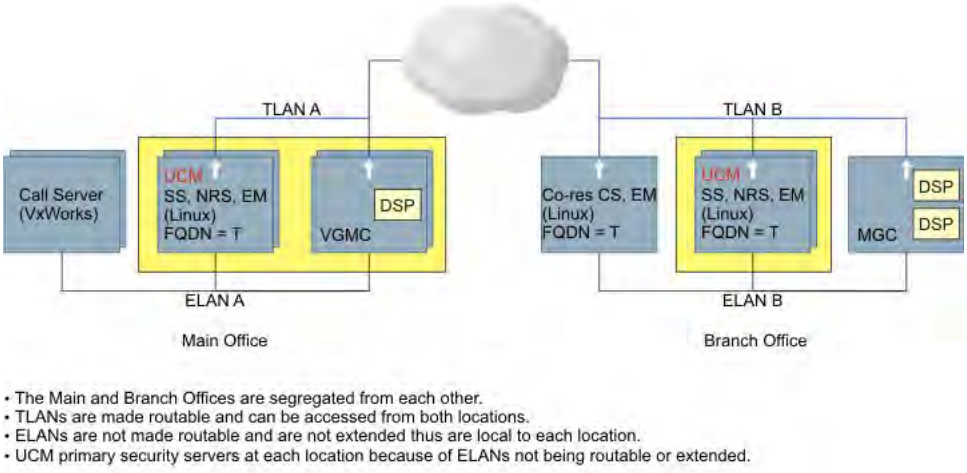


**Figure 36: Release 6.0 and later customer network configuration**

## Normal configuration

The Normal (or Routed) configuration, shown in Figure 37: Normal configuration on page 166, is similar to existing CS 1000 installations where all TLAN subnets are routed to a single Enterprise Network. Normal configuration requires that the ELAN or Intra-System Signaling and Management Network be routed to/from the Enterprise Network. A firewall is recommended between the networks to protect the intra-system signaling on the ELAN. The TLAN subnets should be separate from other subnets in the enterprise network and it is recommended that these subnets be isolated from the enterprise network using firewalls.

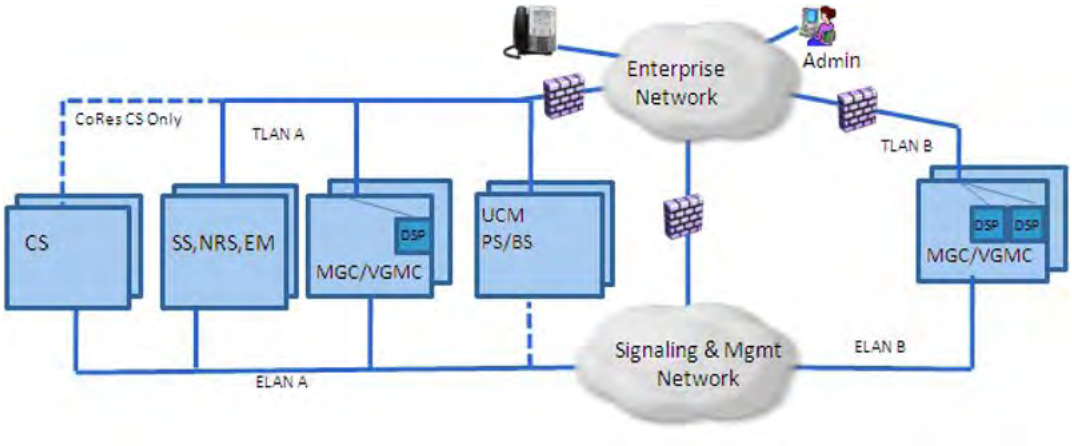


**Figure 37: Normal configuration**

When installing a CS 1000 system in the Normal configuration, all members of the system are registered with the UCM security domain using the TLAN IP address (or FQDN) of the UCM Primary Security server. The FQDN of each member is associated with the TLAN IP address of the member. Installation steps as currently documented in the NTP documents is followed.

On CS 1000 systems which deploy more than one ELAN subnet, static routes must be created on the CS 1000 elements to ensure that the data traffic between CS 1000 elements and between the CS 1000 elements and external systems or elements is routed properly via the correct network. The required routing is shown in Configuration of Static IP Routes on page 170.

## Small configuration

The Small configuration (see Figure 38: Small configuration on page 167) is intended for small systems where there is a single Call Server with a single ELAN subnet linking all of the CS 1000 elements, including the UCM Primary Security Server. No routing is required between the ELAN subnet and the TLAN / Enterprise Network. The characteristics of systems using this configuration are:

- UCM Security Domain consists of a single Call Server system (can be High Availability)
- Single ELAN subnet, no routing required
- No SNMP Management required (only available via ELAN)

Management access is via the Enterprise Network (TLAN). A VxWorks call server deployed in this configuration must use the EM Virtual Terminal application for network access to the command line.

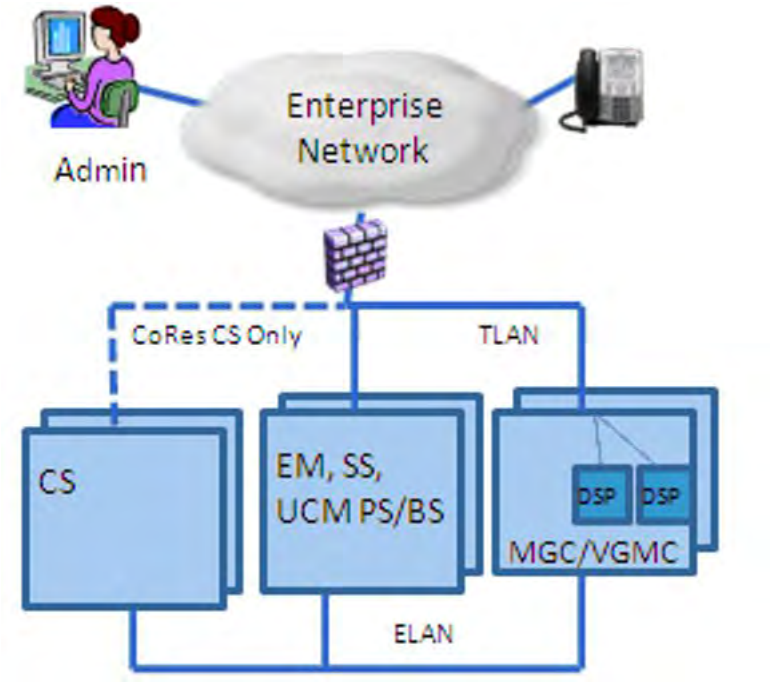


**Figure 38: Small configuration**

When installing a CS 1000 in Small configuration (see Figure 38: Small configuration on page 167), the Linux elements register to the UCM Security Domain using the TLAN IP (or FQDN) of the UCM Primary Security Server. VxWorks elements such as Media Cards or Media Gateway Controllers or VxWorks Call Servers register to the UCM Security Domain using the

ELAN IP address of the UCM Primary Security Server. The LD 117 REGISTER UCMSECURITY SYSTEM command can be used to register the Call Server and dependent MGCs and Media Cards to the UCM Security Domain, however, when prompted for the IP address of the UCM Primary Security Server, its ELAN IP address must be specified which may be different than the default value that is displayed (Linux Co-Resident case).

In the Small configuration, there is only a single ELAN subnet and therefore no additional static routes are required for correct routing.

## Managed Services configuration

The Managed Services configuration is intended for networks where there are multiple isolated customer networks or where the higher security of complete isolation of the Enterprise Network (TLANs) from the Signaling and Management Network (ELANs) is required. In this configuration all management, including access to UCM is available only via the Signaling and Management Network (ELANs). Management access from the enterprise network(s) requires VPN access to the Signaling and Management Network.

In the Managed Services configuration, as shown in Figure 39: Managed services configuration on page 168, the management interfaces on the UCM primary, backup and Linux member servers will be referenced using the FQDNs as in the other configurations; however in this configuration the FQDNs will be assigned to the ELAN IP addresses of the primary, backup and Linux member servers.

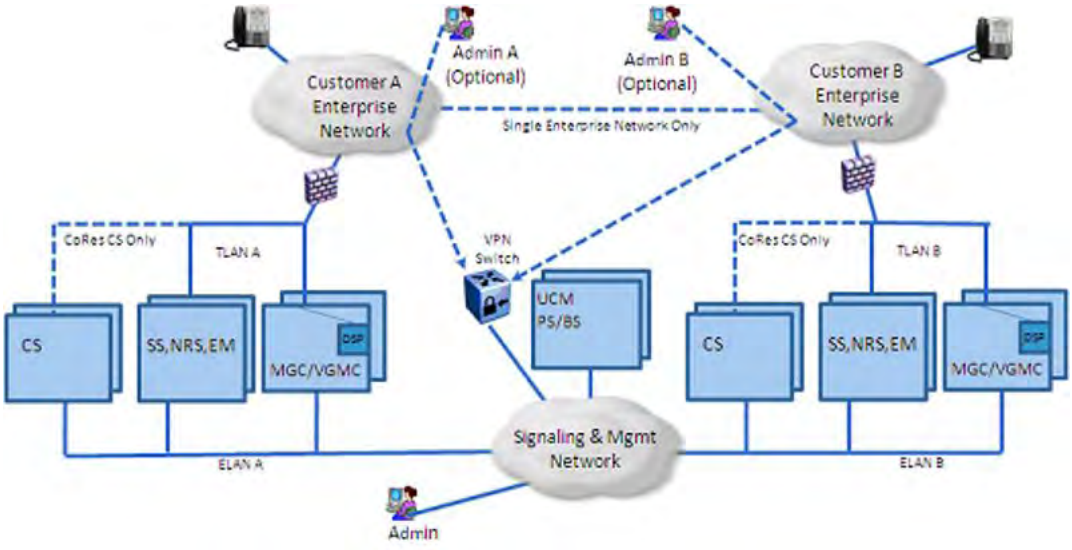


**Figure 39: Managed services configuration**

The characteristics of systems using the Managed Services configuration are:

- Complete isolation between Signaling and Management Network (ELANs) and Enterprise Network (TLANs)
- May have multiple ELANs making up the Signaling & Management Network
- May have multiple TLANs in a Customer Enterprise network

- May have multiple, isolated Customer Enterprise Networks typically with one or more telephony nodes or CS 1000 systems
- Primary management access is via the isolated Signaling and Management Network or via VPN access from the Enterprise Network(s)
- SNMP Management access requires direct or VPN access to the Signaling and Management Network (ELANs)

When installing Linux members of a CS 1000 System in the Managed Services configuration, complete the following procedure.

### Installing Linux members in the Managed Services configuration

1. Install Nortel Linux Base using the normal procedure on UCM primary, backup or Linux member servers
2. In the DNS server, if using, assign FQDNs to be associated with the IP addresses assigned to the ELAN interfaces on the UCM Primary, backup or Linux member servers. If not using a DNS server, these assignments should be added to the "hosts" file on any systems that are accessing these elements. This may need to be done in advance of Step 1 to ensure sufficient DNS propagation time.
3. Prior to performing the security setup of the newly installed UCM Primary, backup or Linux member servers, execute the command opt/nortel/base/bin/fqdnreassign from the CLI of the Linux Element using the root account. This will associate the FQDN entered during installation with the ELAN IP address instead of the default TLAN IP address.
4. Restart the server.
5. Configure the required static routes on the server. See Configuration of Static IP Routes on page 170.
6. Perform the security configuration, specifying the FQDN (or ELAN IP) of the UCM Primary Server. This will map to the IP address of the UCM Primary on the Signaling & Management Network (ELAN).

To ensure that the data traffic between CS 1000 elements and between the CS 1000 elements and external systems or elements is routed properly via the Signaling & Management Network, static routes must be created on the CS 1000 elements. The required routing is shown in Configuration of Static IP Routes on page 170.

## Hybrid Managed Services configuration

The Hybrid Managed Services configuration is intended for networks that contain a mixture of systems in the Normal configuration and systems in the Managed Services configuration. For systems that are on the Normal side, either complete call server systems or individual IP telephony nodes, are configured similar to the Normal configuration. On the Normal side there must be only one Customer Enterprise Network and this network must have routing configured between it and the Signaling and Management network. The systems on the Managed Services side, either complete call server systems or individual IP telephony nodes, are configured similar to the Managed Services Configuration where there are one or more isolated customer networks and there is no routing configured between these Customer Networks and the Signaling & Management network. The UCM Primary and Backup Servers must be

installed with their FQDN on either Signaling & Management network or on the Normal side customer network and can be co-resident with other applications on the appropriate side. See Figure 40: Hybrid Managed Services configuration on page 170.

In this configuration all management, including access to the UCM Primary Server, is accessible from either the Normal side customer network A or via the Signaling and Management Network. Management access from the Managed Services side customer networks requires VPN access to the Signaling and Management Network.

In the Hybrid Managed Services Configuration, the management interfaces on the UCM primary, backup and Linux member servers will be referenced using the FQDNs as in the other configurations; however in this configuration the FQDNs will be assigned to the ELAN IP addresses of the Linux member servers on the Managed Services side. See Figure 40: Hybrid Managed Services configuration on page 170.

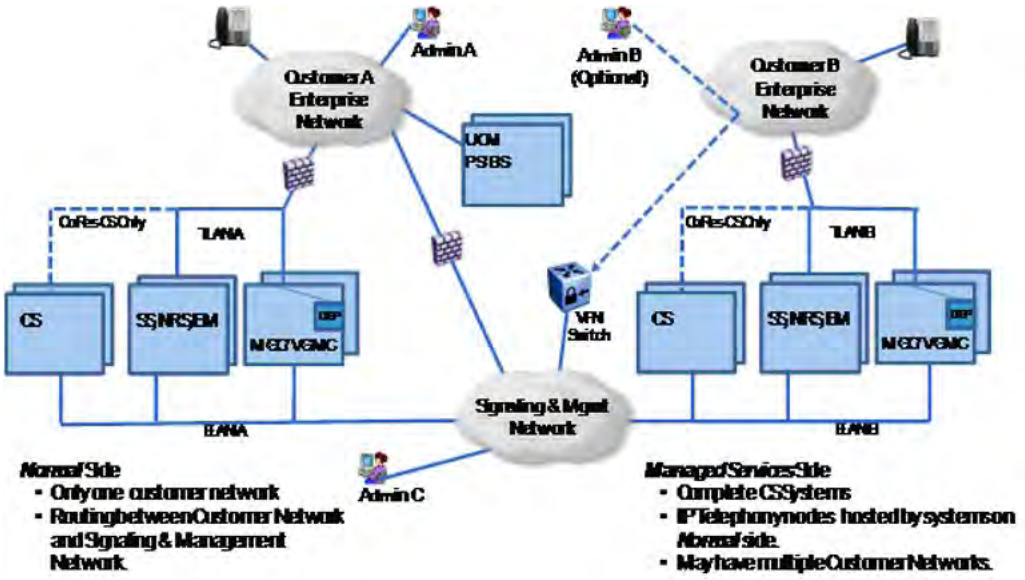


**Figure 40: Hybrid Managed Services configuration**

When installing the Hybrid Managed Services Configuration, the UCM Primary, Backup and Linux Member servers on the Normal side are installed as in the Normal Configuration and Linux Member servers on the Managed Services side are installed following the procedures for the Managed Services Configuration. All VxWorks based elements including MGCs, VGMCs and any VxWorks based Call Servers are registered to the FQDN of the UCM Primary Server (or the IP address corresponding to the FQDN).

## Configuration of Static IP Routes

To ensure the signaling and management data traffic flows over the correct networks, static IP routes must be added to the various CS 1000 elements. The required routing is shown in Table 33: Static IP Route Configuration for Normal Configuration on page 171. In all cases, routes are not required when the destination is on the same ELAN subnet as the member. In many situations, use of network routes, such as to each other ELAN subnet or possibly to the entire range of ELAN subnets can be used to reduce the number and maintenance of the manual

routes, however this depends upon the particular IP address ranges assigned to the ELAN subnets.

- All routes are created to direct the traffic to the ELAN gateway.
- Unless specified, the IP address associated with the FQDN of the element is used.
- Asymmetrical routing (e.g. request/response via different networks) may be blocked by some firewalls. Appropriate routing as indicated must be configured to avoid these conditions.
- Correct use of ISSS to secure management and signaling traffic requires this traffic to be on the designated networks and may not function properly without the appropriate routing configuration.

**Table 33: Static IP Route Configuration for Normal Configuration**

| Element Type For Linux elements, this is based on UCM role (primary, backup, member) and deployment manager packages | Destination(s) | Comments |
|---|---|---|
| UCM Primary, UCM Backup | | Default route uses TLAN. |
| HA CS (VxWorks) (Created using LD 117 commands) | All (0.0.0.0/0) | Only a single network interface therefore default route can be used, but must be configured. |
| Co-Res CS (Linux) | ELAN addresses of MGCs, VGMCs, GR CSs, EM, SSs, SIPLs, TM, CallPilot, and Contact Center. | If using the AML Link splitting feature on a co-resident SS, routing to applications using this interface may not be required. Default route uses TLAN. |
| EM (Created using Linux Base Manager) | ELAN addresses of Call Server and dependent elements (CS, MGC, VGMC, SS and SIPL) | Default route uses TLAN. |
| Signaling Server, SIPL (Created using Linux Base Manager) | ELAN address of EM. ELAN address of Feigns in same IP telephony node. | Default route uses TLAN. |
| MGC (Created using Element Manager) | ELAN address of EM FQDN address of UCM Backup. | Default route uses TLAN. |
| VGMC (Created using Element Manager) | ELAN address of EM FQDN address of UCM Backup. | Default route uses TLAN. |

**Table 34: Static IP Route Configuration for Managed Services Configuration**

| Element Type For Linux elements, this is based on UCM role (primary, backup, member) and deployment manager packages | Destination(s) | Comments |
|---|---|---|
| UCM Primary, UCM Backup | ELAN addresses of all members of the security domain (CS, EM, SS, VGMC, MGC, UCM Primary/Backup) | Network routes are recommended. Default route uses TLAN. |
| HA CS (VxWorks) (Created using LD 117 commands) | All (0.0.0.0/0) | Only a single network interface therefore default route can be used, but must be configured. |
| Co-Res CS (Linux) | UCM Primary, UCM Backup, management stations, and ELAN addresses of MGCs, VGMCs, GR CSs, EM, SSs, SIPLs, TM, CallPilot, Contact Center, VPN Switch subnet, 3rd Party Systems. | If using the AML Link splitting feature on a co-resident SS, routing to applications using this interface may not be required. Default route uses TLAN. |
| EM (Created using Linux Base Manager) | UCM Primary, UCM Backup, management stations and ELAN addresses of Call Server & dependent elements (CS, MGC, VGMC, SS and SIPL), VPN Switch subnet. | Default route uses TLAN. |
| Signaling Server, SIPL (Created using Linux Base Manager) | FQDN address of UCM Primary & UCM backup. ELAN address of EM. ELAN address of VGMCs in same IP telephony node. | Default route uses TLAN. |
| MGC (Created using Element Manager) | ELAN address of EM FQDN address of UCM Backup. | Default route uses TLAN. |
| VGMC (Created using Element Manager) | ELAN address of EM FQDN address of UCM Backup. | Default route uses TLAN. |

# Server LAN design

The system servers and gateways can require up to four separate subnetworks. To differentiate the subnets and the corresponding network interface on each device, they are named:

- ELAN subnet
- TLAN subnet
- Nortel Server subnet
- Client subnet

Figure 41: Example: Enterprise IP Network on page 173 shows the logical elements of basic system connectivity in a CS 1000 network.

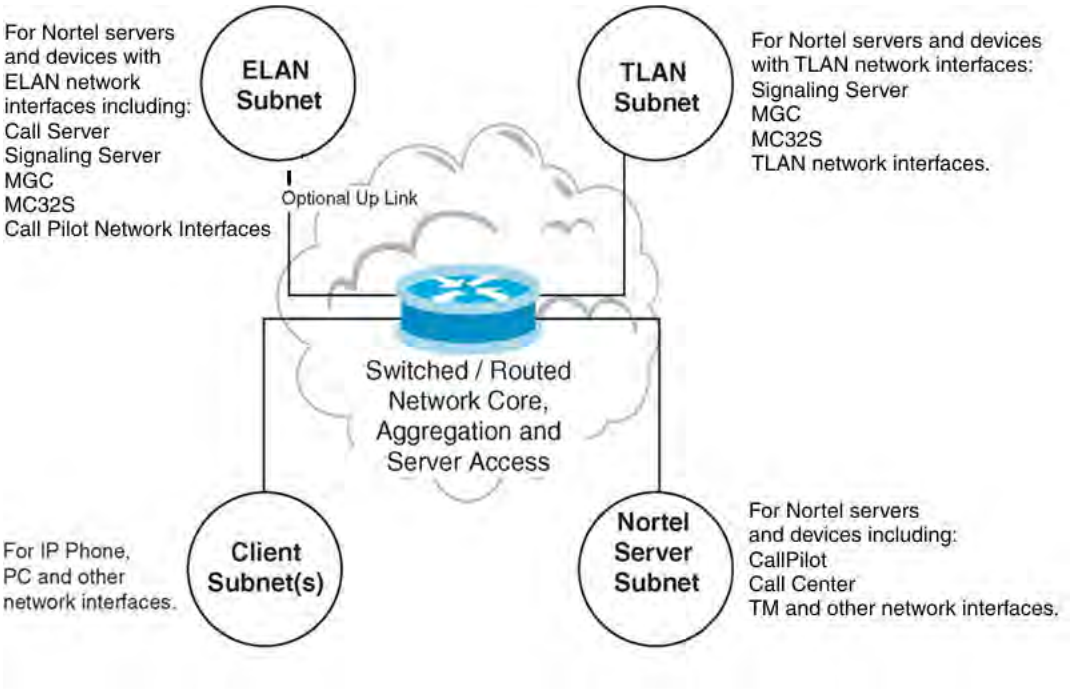


**Figure 41: Example: Enterprise IP Network**

Every device, with the exception of the Call Server, has an ELAN and a TLAN network interface. VoIP Desktop Clients on a QoS-managed IP network are usually separate subnets from the ELAN, TLAN, and Nortel server subnets.

## Server subnets

Figure 42: Layer 2 Ethernet connection model on page 174 shows the Ethernet connection model in a CS 1000 network.

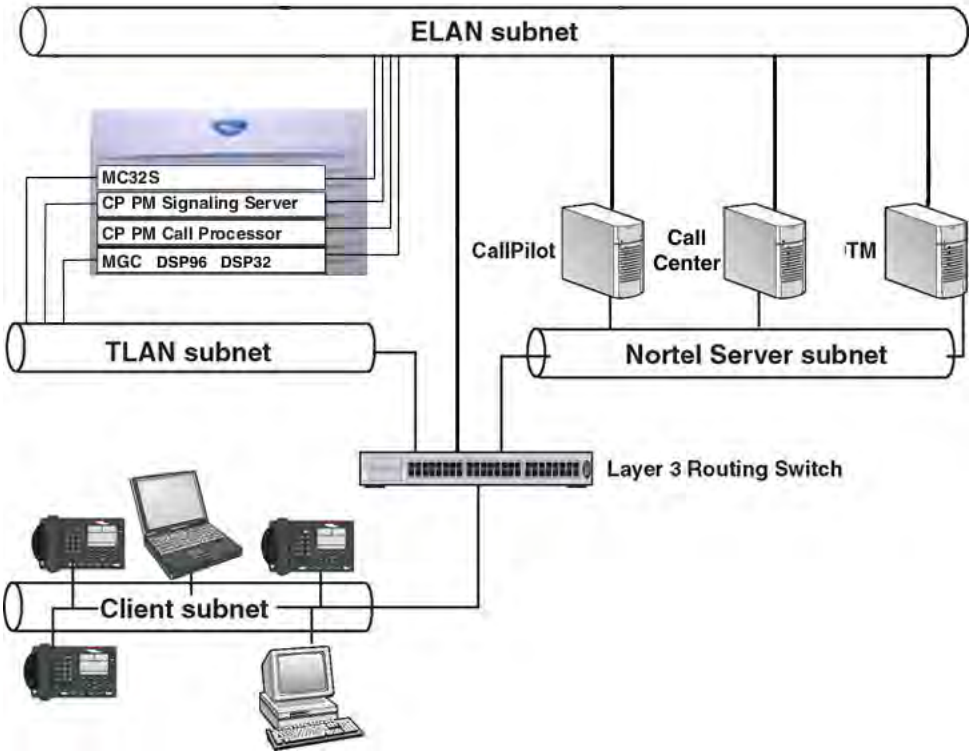


**Figure 42: Layer 2 Ethernet connection model**

## ELAN subnet

The ELAN subnet is an isolated 10BaseT subnet required for management traffic and intrasystem signaling traffic between the system Call Server and devices that require Call Server processing (for example, the Signaling Server, Media Gateway Cards, SSC cards, Voice Gateway Media Cards, CallPilot, and Symposium).

The ELAN subnet must create an isolated broadcast domain. Use of a Virtual LAN or a physically separate Layer 2 switch is acceptable as it reduces the risk of network outage due to broadcast storms or other extraneous network traffic.

Only Nortel servers with an ELAN network interface can connect to the ELAN subnet; do not connect other PCs or client. For example, connect the ELAN network interface from other applications, such as CallPilot and Symposium Call Center Server, to the ELAN subnet.

Configure Windows based servers with an ELAN network interface, and a second network interface that connects to another subnet (for example, SCCS, CallPilot servers). Do not transmit extraneous traffic, such as broadcasts or multicasts, onto the ELAN subnet.

Nortel recommends that you use a Layer 2 switch with broadcast and multicast rate limiting for the ELAN subnet to improve the robustness of all servers. Implement rate limiting for an isolated ELAN subnet, even if the Layer 2 switch is not connected to the rest of the network.

For information about designing a Communication Server 1000 server network for maximum redundancy, see Redundant LAN design on page 188.

The ELAN subnet also carries system management traffic. An uplink from the ELAN subnet to the Enterprise IP network becomes necessary if you use SNMP to manage a network of Communication Server 1000 or Meridian 1 systems. If you plan to connect the ELAN subnet to the Enterprise IP network, a Layer 3 switch or router capable of packet filtering must be used to separate the ELAN subnet from the Enterprise IP network. The Layer 3 switch must be configured to prevent random broadcast, multicast traffic from entering the ELAN subnet. The Layer 3 switch must also be configured with a packet filter to prevent unauthorized traffic from entering the ELAN subnet. If the ELAN subnet is connected to the Enterprise IP network without a packet filtering Layer 3 switch or router, the call handling ability of the system may be adversely affected.

### TLAN subnet

The TLAN subnet is a 100BaseT full duplex LAN that connects all Voice Gateway Media Cards and Signaling Servers within an IP telephony node. An IP telephony node is defined as a logical grouping of Voice Gateway Media Cards and Signaling Servers.

A device in a single IP telephony node cannot be a member of more than one subnet/VLAN. However, a subnet can have more than one IP telephony node as a member.

**Important:**

Nortel strongly recommends that you use a Layer 2 switch with broadcast and multicast rate limiting for the TLAN subnet.

Nortel further recommends that customers configure the TLAN subnet to carry only Communication Server 1000 specific traffic, and be separated from the rest of the Enterprise IP network by a Layer 3 switch. Deploy the IP Phones on the client side of the Enterprise IP network.

Optionally, the TLAN subnet can be configured as a restricted access subnet using a packet filtering device (for example, a firewall) to restrict traffic, based on source IP address or TCP/UDP port numbers, allowed to enter the TLAN subnet.

Nortel recommends that you use port prioritization for all TLAN connections. For detailed information on port prioritization, see QoS mechanism on page 40.

### Nortel Server subnet

The Nortel Server subnet is the least specialized of the four subnets described in this section. Nortel recommends that the Nortel Server subnet be used to connect the CLAN network interfaces on the CallPilot and Symposium servers as well as any other Nortel servers or applications associated with these systems.

**Important:**

Nortel strongly recommends that the Nortel Server subnet be separated from the rest of the Enterprise IP network by a Layer 3 switch.

Optionally, you can connect the CLAN network interfaces of the CallPilot, Symposium server to the dedicated Nortel Server subnet, or to any non-dedicated subnet (for example, shared with other servers) in the customer's Enterprise IP network.

**Important:**

Nortel strongly recommends the you use a Layer 2 switch for the Nortel server subnet.

The TLAN subnet and the Nortel Server subnet can be the same subnet.

## Communication Server 1000 Ethernet connections

Figure 43: MG 1000B detailed core system connections on page 176 through Figure 45: CS 1000M MGwith dual CP PII or CP PIV Call Server cards on page 177 shows Communication Server 1000 server and gateway network connectivity at Layer 1 and Layer 2.

The following figures show redundant Layer 2 switches that use virtual LANs to group the ELAN and TLAN subnets. For more information about Layer 2 and Layer 3 switch redundancy, see Redundant LAN design on page 188. In all cases, a single Layer 2 switch (or a single Layer 2 switch designated for the ELAN and TLAN subnets) can be used, but at the cost of system reliability.

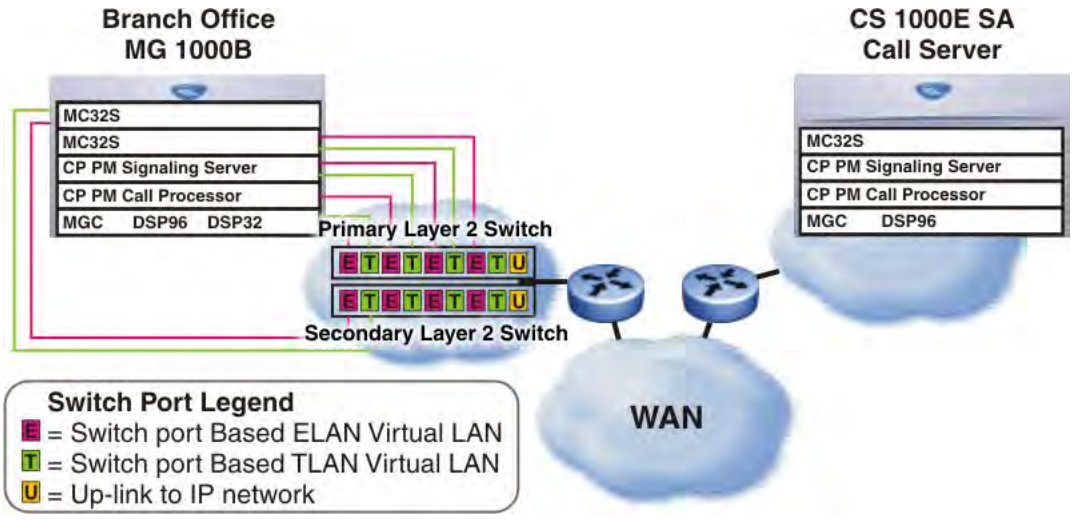


**Figure 43: MG 1000B detailed core system connections**

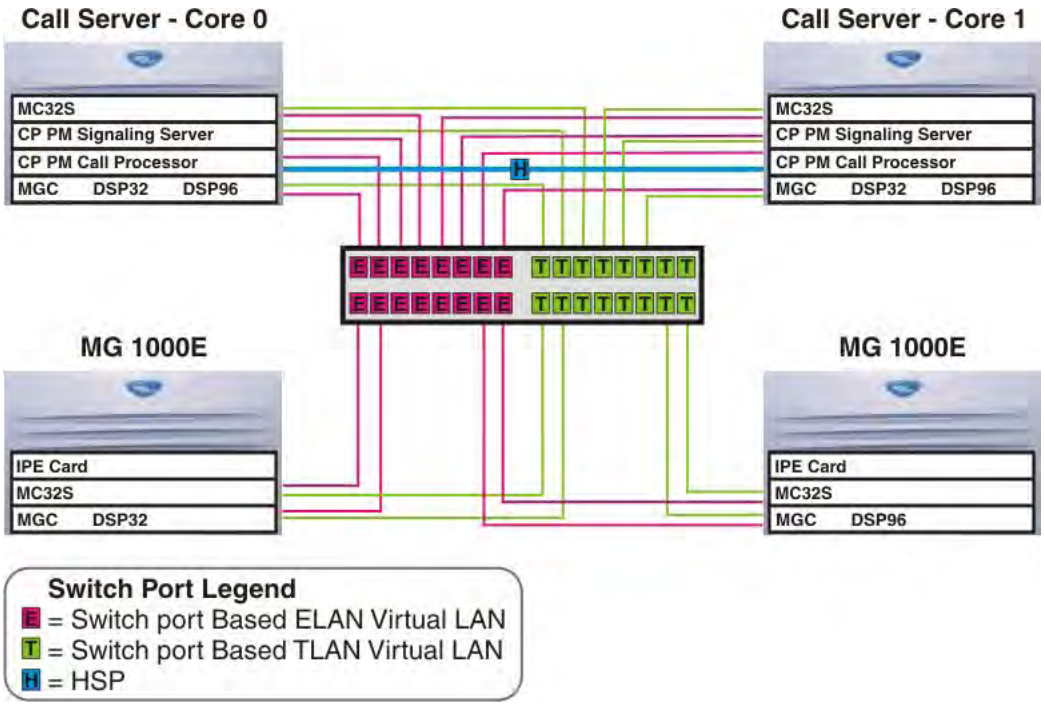


**Figure 44: Communication Server 1000E: Physically collocated Side 0 and Side 1**

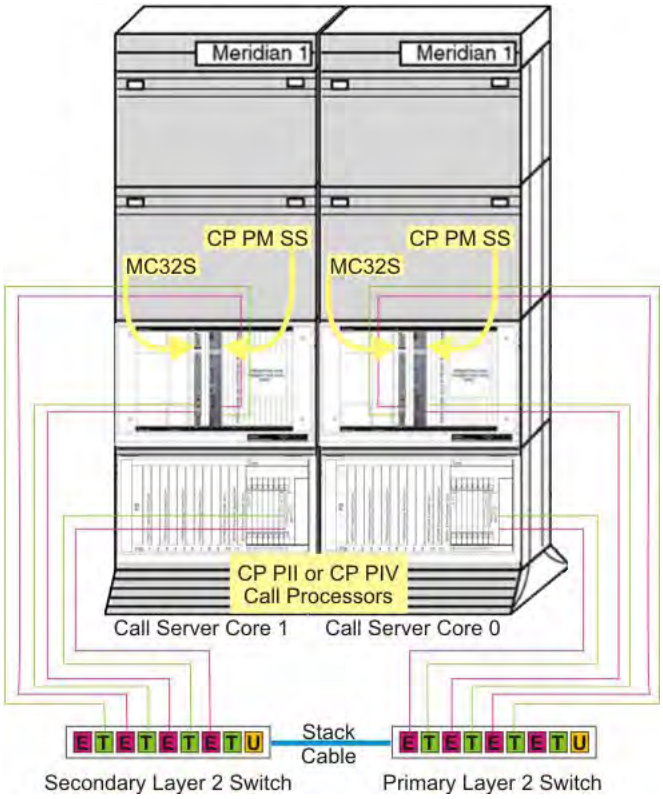


**Figure 45: CS 1000M MGwith dual CP PII or CP PIV Call Server cards**

## Ethernet requirements

Careful consideration must be given to the Layer 2 infrastructure that the system is connected to. This section describes issues that must be considered when you design the server LAN that connects a system to the IP network.

### General Layer 2 considerations

Passive Ethernet hubs are not supported. Use Layer 2 Ethernet switches for both the ELAN and TLAN subnets. Ideally, managed switches should be used.

The general requirements are as follows:

- no foreign broadcasts from other subnets
- no BootP relay agent requirement (only on the ELAN subnets router interface)
- the TLAN Ethernet cable between the ITG-P Line Card and the Layer 2 switch must be 50 meters or less
- disable the Spanning Tree protocol or enable port fast on the Layer 2 switch network interfaces connected to the ELAN and TLAN ports of the Meridian 1 and CS 1000M components.

### Communication Server 1000 network interfaces

The devices in the system have different network interface names depending on whether the devices are on the TLAN or ELAN subnets. Table 35: Network Interface Card Names on page 178 shows the network interface card names for the Voice Gateway Media Cards (Media Card 32-port card and ITG-P 24-port card), the Signaling Server, Small System Controller (SSC), and Call Processor Pentium (CPP).

**Table 35: Network Interface Card Names**

| Device type | TLAN/ELAN network interface | Network interface name | Configuration | Speed and duplex |
|---|---|---|---|---|
| Media Card | ELAN network interface | ixpMac1 | autonegotiate | 10BaseT Half Duplex |
| | TLAN network interface | ixpMac0 | autonegotiate | 100BaseT Full Duplex |
| ITG-P Line Card | ELAN network interface | InIsa0 | autonegotiate | 10BaseT Half Duplex |
| | TLAN network interface | InPci1 | autonegotiate | 100BaseT Full Duplex |
| Signaling Server | ELAN network interface | fei0 | autonegotiate | 100BaseT Full Duplex |
| | TLAN network interface | fei1 | autonegotiate | 100BaseT Full Duplex |

| Device type | TLAN/ELAN network interface | Network interface name | Configuration | Speed and duplex |
|---|---|---|---|---|
| SSC | ELAN network interface | qu0 | autonegotiate | 10BaseT Half Duplex |
| | TLAN network interface | not applicable | | |
| | IPDB network interface 1 | ipDB0 | autonegotiate | 100BaseT Full Duplex |
| | IPDB network interface 3 | ipDB2 | autonegotiate | 100BaseT Full Duplex |
| | IPDB network interface 2 | ipDB1 | autonegotiate | 100BaseT Full Duplex |
| | IPDB network interface 4 | ipDB3 | autonegotiate | 100BaseT Full Duplex |
| CP3 | ELAN network interface | ln0 | autonegotiate | 10Base T Half Duplex |
| CP4 | ELAN network interface | ln0 | autonegotiate | 10BaseT Half Duplex |
| CP P2 | ELAN network interface | fei0 | autonegotiate | 100BaseT Full Duplex |
| | TLAN network interface | not applicable | | |
| | HSP (high speed pipe for redundant CPUs) | fei1 | Hard coded | 100BaseT Full Duplex |
| CP P4 | ELAN network interface | gei0 | autonegotiate | 10/100/1000 BaseT Full Duplex |
| | HSP (high speed pipe for redundant CPUs) | gei1 | autonegotiate | 10/100/1000 BaseT Full Duplex |
| CP PM CS | ELAN network interface | fei0 | autonegotiate | 10/100 BT Full Duplex |
| | HSP (high speed pipe for redundant CPUs) | gei1 | autonegotiate | 10/100/1000 BT Full Duplex |
| CP PM SS | ELAN network interface | fei0 | autonegotiate | 10/100 BT Full Duplex |
| | TLAN network interface | fei1 | autonegotiate | 10/100 BT Full Duplex |

| Device type | TLAN/ELAN network interface | Network interface name | Configuration | Speed and duplex |
|---|---|---|---|---|
| MGC | ELAN network interface | eln0 | autonegotiate | 100BaseT Full Duplex |
| | TLAN network interface | eth0 | autonegotiate | 100BaseT Full Duplex |

## Broadcast and Multicast rate limiting

Rate limit all broadcast traffic in the ELAN and TLAN Layer 2 or Layer 3 switch to 150 broadcast packets per second (pps). Rate limit all multicast traffic in the ELAN and TLAN Layer 2 or Layer 3 switch to 150 broadcast pps. In some Layer 2 and Layer 3 switches it may be possible, and is recommended, to disable transmission of multicast packets entirely.

Apply the broadcast and multicast rate limiting at egress from the switch ports, or optionally configure all switch ports to rate limit ingress broadcast and multicast traffic. Rate limiting is in addition to the guidelines in Guidelines to configure a routable ELAN subnet on page 188.

## Network interface half: and full-duplex operation

The ELAN network interface on the Voice Gateway Media Card operates at half-duplex and is limited to 10BaseT operation due to filtering on the CS 1000M Cabinetand CS 1000M Chassisback planes.

The TLAN network interface on Voice Gateway Media Card operates at half- or full-duplex and can run at 10BaseT or 100BaseT.

Nortel recommends that any Layer 2 or Layer 3 switch ports connected to the ELAN or TLAN network interfaces be configure to auto-sense/autonegotiate for correct operation. Although full-duplex is preferred, it is not required. For example, for the IP Line application, half-duplex has ample bandwidth for a Voice Gateway Media Card with 24 busy channels, VAD disabled, and G.711 codec with 10 ms voice range.

Mismatches can occur if devices are hard configured for speed and duplex mode. Every device and port must be correctly configured to avoid duplex mismatch problems indicated by lost packets and CRC errors. The Voice Gateway Media Card cannot be hard coded for 100BaseT/ full-duplex operation, so the TLAN network interface operates in autonegotiate mode. Duplex mismatches and lost packets occur if the TLAN network interface is not configured properly.

## Spanning Tree options on Layer 2 switches

Nortel recommends that you disable the Spanning Tree option on the Layer 2 switch ports that connect to the TLAN and ELAN network interfaces on the CS 1000M system.

This option is enabled by default on most Layer 2 switches. If the option is left enabled, the subsequent Spanning Tree discovery algorithm initiated when a device connected to a port is reset, rebooted, or repowered, can interfere with the Master Election Process in the Communication Server 1000E system device. In most cases the Master Election Process recovers after a slight delay. However, Nortel recommends that the Spanning Tree option on these ports be disabled or the Port Fast option enabled.

### How to avoid system interruption

Use the following to avoid system interruption.

### Duplex mismatch

Duplex mismatches can occur in the LAN environment when one side is configured to autonegotiate and the other is hard configured. The autonegotiate side adapts to the fixed side settings, including speed. For duplex operations, the autonegotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

To hard configure all devices for speed/duplex, ensure every device and port is correctly configured to avoid duplex mismatch problems.

**⚠ Warning:**

Configure the Layer 2 or Layer 3 switch ports as autonegotiate.

If one side is manually configured and the other side is configured as autonegotiate, the following situation occurs:

The autonegotiate side sets itself to the speed of the manually configured side, but always sets itself to half-duplex. If the manually configured side is full-duplex, then a duplex mismatch occurs and voice quality is unsatisfactory.

**Important:**

Nortel strongly recommends that all Layer 2 ELAN and TLAN switch ports be configured to autonegotiate.

### I/O filter connector

The other TLAN network interface operation problem arises from the standard I/O filter connector in IPE modules on Meridian 1 Large Systems and CS 1000M Large Systems.

Use the following guidelines to avoid system interruption that stems from the standard I/O filter connector in IPE modules:

- Ensure that the standard IPE module I/O filter is replaced with the provided Voice Gateway Media Card/ITG-specific filter connector that removes filtering from pairs 23 and 24.
- Do not install the Voice Gateway Media Card/ITG-specific filter connector on top of the standard IPE module I/O filter connector.
- Replace the IPE module backplane I/O ribbon cable assemblies with those that have interchangeable I/O filter connectors.
- The CAT-5 Ethernet cable from the TLAN network interface to the Layer 2 switch port must meet the UTP Category 5 termination and impedance uniformity standards.
- The CAT-5 Ethernet cable from the TLAN network interface of the ITG Pentium card to the Layer 2 switch port must not exceed 50 meters in length.

The TLAN network interface can autonegotiate to 100BaseT full-duplex. For the TLAN network interface to operate correctly at 100BaseT full-duplex speeds, do the following:

- Install the Voice Gateway Media Card/ITG-specific filter connector correctly by replacing the standard IPE Module I/O filter connector.
- Order new IPE Module Backplane I/O ribbon cable assemblies that have interchangeable I/O filter connectors, if it becomes necessary to use one of the IPE Modules with molded on I/O filter connectors.
- Ensure that the UTP cabling is CAT-5 compliant.
- Always keep the CAT-5 Ethernet cable from the TLAN network interface to the Layer 2 switch port less than 50 meters for the ITG-Pentium 24-port trunk card.
- As an interim measure, connect to each ITG-Pentium 24-port trunk card and log on to the ITG shell. In the shell, use the commands **`tlanDuplexSet`** and **`tlanSpeedSet`** to configure the TLAN network interface to operate at half-duplex 10BaseT.

## IP address requirements

This section describes IP address requirements for each node, card, and IP Phone.

A node is a group of ITG-P Line Cards and Media Cards in a Meridian 1 or Communication Server 1000 system. Each card in a node has two IP addresses: one for the TLAN network interface and one for the Meridian 1 or Communication Server 1000 ELAN network interface. Each node has one Node IP address on the TLAN subnet dynamically assigned to the connection server on the node Master. The IP Phone uses the Node IP address during the registration process.

All Communication Server 1000 ELAN network interface IP addresses must be on the same subnet as the system Call Server ELAN network interface IP address.

### General requirements for node IP addressing

To configure a node, the following IP addresses must be assigned:

- One IP address for each TLAN network interface of every Voice Gateway Media Card and Signaling Server.
- One IP address for each ELAN network interface of every Voice Gateway Media Card and Signaling Server.
- One TLAN Node IP address. This alias IP address appears dynamically on the TLAN network interface of one card in the node, the Leader or node Master. This address is shared among all the cards.
- On Communication Server 1000 systems, one IP address for the Signaling Server ELAN network interface and Signaling Server TLAN network interface.

In addition to the IP addresses, the following network information must be provided:

- ELAN network interface subnet mask
- ELAN network interface default gateway IP address

- TLAN network interface subnet mask
- TLAN network interface default gateway IP address

**Note:**

Use separate ELAN and TLAN subnets with the Voice Gateway Media card. The user interface provides an option to use the same subnets, but you must use different subnets.

The default setting of separate ELAN and TLAN subnets protects the subnet from extraneous network traffic, including broadcast and multicast storms. It may also protect the Call Server from unauthorized access from the Enterprise network.

**Important:**

Nortel strongly recommends that you use separate dedicated ELAN and TLAN virtual LANs and subnet. They must be separated by a router/Layer 3 switch.

You must use a single ELAN and TLAN subnet, see ELAN and TLAN network interfaces on a single subnet on page 187.

### SS TLAN configuration requirements

This section describes the single server TLAN configuration requirements.

- If single SS is supposed to have 900 and more sets registered, its TLAN subnet mask should be checked first.
- If the TLAN subnet mask is 9 or less bits there are no limitations or special requirements.
- If the TLAN configuration is 10 and more bits subnet mask (10 bits subnet mask is 255.255.252.0) the IP sets IP addresses and subnet mask settings should be checked.

The maximal number of IP phones configured in the same subnet as SS TLAN is 900. If more sets are required they should be configured in different subnet or VLAN configuration can be used to avoid this limitation.

In this case the VLANs should be configured similar way:

- SS TLAN and only 900 sets IP addresses or MACs can be in the same VLAN.
- All other IP sets should be in different VLAN.

These instructions are needed to avoid ARP table overload on the SS since only 968 ARP entries can be added to ARP table.

**Note:**

All these limitations are only applicable for the SS which runs on VxWorks, not Linux.

### CP PM Call Server IP address requirements

The CP PM Call Server IP address is the IP address of the CP PM Call Server on the ELAN subnet. The CP PM Call Server requires one IP address for the ELAN network interface and a second IP address for the high speed pipe, when used in a High Availability configuration. The CP PM Call Server ELAN network interface IP address must correspond to the Active ELNK IP address configured in LD 117.

The Alternate Call Server ELAN network interface IP address must be in the same ELAN subnet as the Primary Call Server ELAN network interface IP address.

### Gateway Controller IP address requirements

The Gateway Controller requires

- one ELAN IP address when there are no DSP resources
- one ELAN IP address and two TLAN IP addresses when there is one DSP daughterboard
- one ELAN IP address and three TLAN IP addresses when there are two DSP daughterboards

The MGC card supports a maximum of two DSP daughterboards. The MG XPEC card and CP MG card contain non-removable DSP resources.

### Signaling Server IP address requirements

The Signaling Server requires:

- one IP address for the Signaling Server ELAN network interface
- one IP address for the Signaling Server TLAN network interface

The IP addresses are configured in the Signaling Server Install Tool menu. Follower Signaling Servers are configured using Communication Server 1000 Element Manager running on the Leader Signaling Server. For more information about the Signaling Server, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

### Network Routing Service IP address requirements

The Network Routing Server (NRS) software can be run on a Signaling Server in stand-alone mode with no other applications, or it can run in co-resident mode with other applications such as the Line TPS.

For a standalone NRS, only the TLAN network interface is required. A node IP address and a TLAN network interface IP address must be configured on the standalone NRS. Use of the ELAN network interface is not required. When asked to enter an ELAN IP address, assign a private IP address, for example, 10.10.0.1 with mask 255.255.255.0. Do not configure a Call Server IP address.

For a co-resident NRS, the Signaling Server IP address requirements apply:

- one IP address for the Signaling Server ELAN network interface
- one IP address for the Signaling Server TLAN network interface

The NRS IP address is the TLAN network interface IP address of the Signaling Server.

The ELAN and TLAN network interface IP addresses, and the NRS IP addresses, are configured from the Signaling Server Install Tool menu. Follower Signaling Servers are configured using Element Manager running on the Leader Signaling Server.

### Voice Gateway Media Card IP address requirements

Provide an IP address for both the ELAN and TLAN network interfaces. All cards must be connected to the same ELAN subnet, which is also the same subnet to which the system's Call Server is connected. All cards in a node must be connected to the same TLAN subnet.

The ELAN network interface MAC address corresponds to the Management MAC address, which is assigned during manufacturing and cannot be changed. Locate the faceplate sticker

on the Voice Gateway Media Card. The ELAN/Management MAC address is the MOTHERBOARD Ethernet address.

The Voice Gateway Media Card IP addresses are configured using Element Manager.

Use separate subnets for the IP Telephony node. Each Voice Gateway Media Card configuration requires a

- Management (ELAN network interface) IP address
- Voice (TLAN network interface) IP address
- Management MAC address
- Voice LAN gateway IP address

### ELAN and TLAN subnet configuration examples

The following ELAN and TLAN subnet restrictions apply:

- The Leader 0 and Leader 1 cards must coreside on a single TLAN subnet with the Node IP Address.
- Follower cards must reside on the same TLAN subnets.
- All devices must coreside on the same ELAN subnet as their respective Call Server and node Leader.

For dual subnet configuration, make sure the TLAN and ELAN subnets do not overlap.

### Example 1–Invalid configuration

The following configuration is not valid, as the TLAN and ELAN subnets overlap.

| **ELAN network interface:** | |
|---|---|
| IP address | 10.0.0.136 |
| Subnet mask | 255.255.255.128 |
| Default Gateway IP address | 10.0.0.129 |

| **TLAN network interface:** | |
|---|---|
| Node IP address | 10.0.0.56 |
| IP address | 10.0.0.57 |
| Subnet mask | 255.255.255.0 |
| Default Gateway IP address | 10.0.0.1 |

The range of IP addresses in the ELAN subnet – 10.0.0.129 to 10.0.0.255 – overlaps the range of IP addresses in the TLAN subnet – 10.0.0.1 to 10.0.0.255. This contravenes the IP addressing practices, as it is equally valid to route the IP packets over either interface. The resulting behavior from such a setup is undetermined.

The overlapping IP address scheme must be corrected.

### Example 2–Valid configuration

The following configuration is valid, as the ELAN and TLAN subnets do not overlap.

The IP addresses can be split as follows.

| ELAN network interface: | |
|---|---|
| IP address | 10.0.0.136 |
| Subnet mask | 255.255.255.128 |
| Default Gateway IP address | 10.0.0.129 |

| TLAN network interface: | |
|---|---|
| Node IP address | 10.0.0.56 |
| IP address | 10.0.0.57 |
| Subnet =mMask | 255.255.255.128 |
| Default Gateway IP address | 10.0.0.1 |

The TLAN subnet has a range of addresses from 10.0.0.1 to 10.0.0.127. The ELAN subnet is a separate subnet, with a range of addresses from 10.0.0.129 to 10.0.0.255. This configuration results in a smaller TLAN subnet, but it meets the requirement that subnets do not overlap.

### Selecting private or public IP addresses

There are a number of factors to consider when determining if the TLAN and ELAN subnets will use private (internal) IP addresses or public IP addresses.

### Private IP addresses

Private, or internal, IP addresses are IP addresses that are not routed over the Internet. They can be routed directly between separate intranets, provided that there are no duplicated subnets in the private IP addresses. Private IP addresses can be used to configure the TLAN and ELAN subnets, so that scarce public IP addresses are used efficiently.

Three blocks of IP addresses have been reserved for private intranets:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Some routers and firewalls provide a Network Address Translation (NAT) function that allows the customer to map a registered globally unique public IP address to a private IP address without renumbering an existing private IP address autonomous domain. NAT allows private IP addresses to be accessed selectively over the Internet.

### Public IP addresses

Public IP addresses can be used for the TLAN and ELAN subnets, but consume limited resources.

This has the same result as the private IP address solution, but the ELAN subnet is accessible from the IP network without NAT.

### ELAN and TLAN network interfaces on a single subnet

IP Trunk 3.0 (or later) supports the use of a single network interface (for example, the ELAN network interface).

Single subnet configuration implies the configuration and use of just one network interface, namely the ELAN network interface, over which all voice and management traffic is routed. Single subnet configuration can also mean configuring both the TLAN and ELAN network interfaces in the same subnet. Neither configuration is supported. The ELAN and TLAN network interfaces must be assigned IP addresses in different subnets.

Separate or dual subnet configuration implies configuration of both the TLAN and ELAN network interfaces. All management and intrasystem signaling traffic is routed out the ELAN network interface, while all telephony traffic is routed out the TLAN network interface.

**Important:**

Nortel recommends that you use separate subnets, the Network Activity LEDs provide useful status information regarding the state of the ELAN and TLAN network interfaces. When you use an ITG-Pentium 24-port trunk card in a single-subnet configuration, all traffic uses the ELAN network interface. This eliminates the use of the TLAN network interface.

Although not recommended, the single subnet configuration of voice and management could be used in the following situations:

- The combined voice and management traffic on the ELAN subnet is so low that there is no impact on packetized voice QoS performance.
- The customer is willing to tolerate occasional voice quality impairments caused by excessive management traffic.

### Multiple nodes on the same ELAN and TLAN subnets

There are several configurations where it is acceptable to put multiple nodes on the same dedicated ELAN and TLAN subnets (separate subnets):

- Several nodes that belong to the same customer and related to the same Communication Server 1000 Call Server can be configured to route calls with different codecs, depending on the digits dialed, or the Network Class of Service (NCOS) of the originating telephone. It can also be configured to limit the maximum number of IP Trunk calls to a particular destination node. The traffic engineering considerations on the TLAN subnet determine how many different nodes can be configured on the same LAN segment.
- Layer 2 (10BaseT or 100Base-TX) switching equipment or ATM infrastructure can support a Virtual LAN (VLAN) segment distributed across a campus or large corporate network. In this case, some or all of the ITG destination nodes can be on the same subnet.
- In test labs, training centers, and trade shows, it is common for destination nodes to be located on the same ELAN and TLAN subnets.

Do not place other IP devices, except those designated as acceptable by Nortel, on the ELAN or TLAN subnets.

## Guidelines to configure a routable ELAN subnet

Use the following guidelines when you configure a routable ELAN subnet on the Enterprise IP network.

1. External multicasts must not be transmitted on the ELAN subnet. Generally, multicast forwarding is disabled by default on a gateway router. Ensure that no multicast routing protocols are enabled on the ELAN subnet gateway router. Do not configure or allow the ELAN or TLAN subnet gateway router (the Layer 3 switch) to forward multicast traffic to the ELAN subnet.
2. External broadcasts must not be forwarded to the ELAN subnet. Ensure that the Layer 3 switch is configured so that it does not forward broadcast traffic from elsewhere on the network to the ELAN subnet. This includes disabling any features on the Layer 3 switch which forward broadcast packets to a subnet when the received packets destination IP address is the subnet broadcast IP address. This can also include disabling other broadcast forwarding mechanisms, such as UDP broadcast forwarding, DHCP forwarding, or NetBIOS forwarding.
3. An ELAN subnet gateway router must be capable of Packet Filtering in order to prevent unauthorized traffic from entering the ELAN subnet. Management traffic is sent from management systems to the Communication Server 1000 system. Management traffic includes FTP, Telnet, HTTP, SNMP, DBA, and rlogin servers. For the control and management of TCP and UDP port numbers for each component connected to the ELAN subnet, see Port number tables on page 321. Configure the packet filter to forward any traffic with the source IP address equal to management system IP address and a management service destination TCP or UDP port. The packet filter should then drop all other traffic.

# Redundant LAN design

A redundant network has one or more backup systems or elements available to processing and transmit in case of system or element failure.

## Single physical location

To begin planning for redundancy, classify equipment into primary and secondary group, as shown in Figure 46: Primary and secondary equipment groups on page 189.

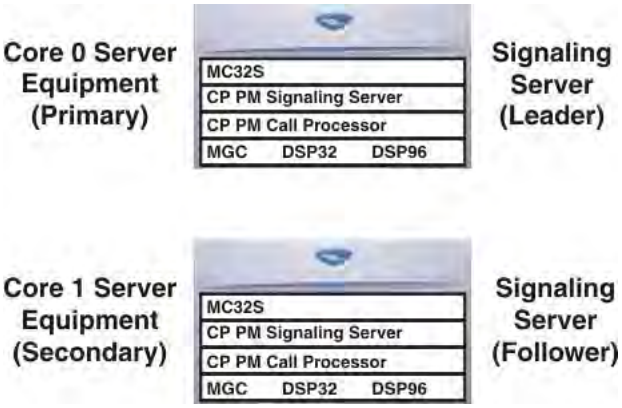


**Figure 46: Primary and secondary equipment groups**

To implement a redundant core network, follow these recommendations:

- Connect ELAN and TLAN network interfaces for the primary core components (Call Server, Leader Signaling Server, and media cards) to the primary Layer 2 switch.
- Connect ELAN and TLAN network interfaces for the secondary core components (Alternate Call Server, Follower Signaling Server, and media cards) to the secondary Layer 2 switch.
- Provide backup power for all essential components and networking devices.
- Use data equipment that supports port-based Virtual LANs (VLANs) and prioritization (IEEE 802.1Q standard).
- Install load sharing connections or install backup connections, using the OSPF or Spanning Tree Protocol (STP), to multiple Layer 3 switches. OSPF is the preferred protocol in this case.

  **⚠ Warning:**

  Spanning Tree Protocol convergence can cause Layer 2 switch ports to be disabled for up to 60 seconds. This can affect the entire system.

- If you use a highly available chassis-based system (for example, Passport 8100), designate one card as the primary Layer 2 switch and another card as the secondary Layer 2 switch. Group the ELAN and TLAN subnets with port-based VLANs.

  Use of a single highly available Nortel Passport 8600 switch can provide a five nines network.

Figure 47: Redundant core network: no VLAN on Layer 2 switch infrastructure on page 190 through to Figure 49: MG 1000E redundancy details on page 191 show a network architecture that divides the core components into primary and secondary devices. Each device is connected to its corresponding Layer 2 switch. Both the ELAN and TLAN network interfaces are connected to the respective Layer 2 switch. VLANs can be used to reduce the number of switches required to obtain a redundant core network.

Figure 47: Redundant core network: no VLAN on Layer 2 switch infrastructure on page 190 show a redundant core network that does not use VLANs on the Layer 2 switch infrastructure.

**Important:**

The primary and secondary TLAN network interfaces must be in the same subnet and broadcast domain.

The primary and secondary ELAN network interfaces must be in the same subnet and broadcast domain

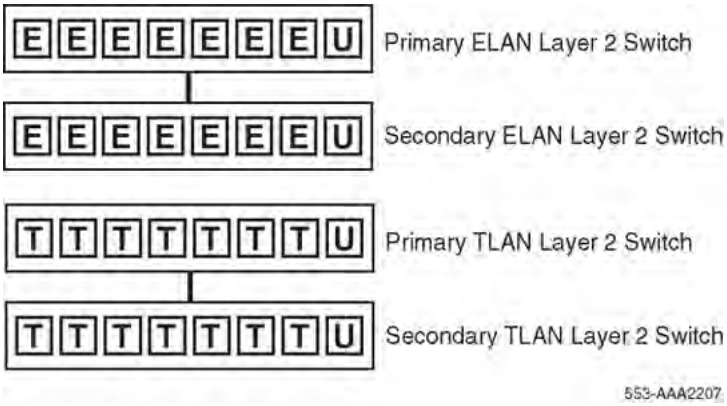


**Figure 47: Redundant core network: no VLAN on Layer 2 switch infrastructure**

Figure 48: Redundant core network: VLANs on the Layer 2 switch infrastructure on page 190 is an example of a redundant core network that does use VLANs on the Layer 2 switch infrastructure.

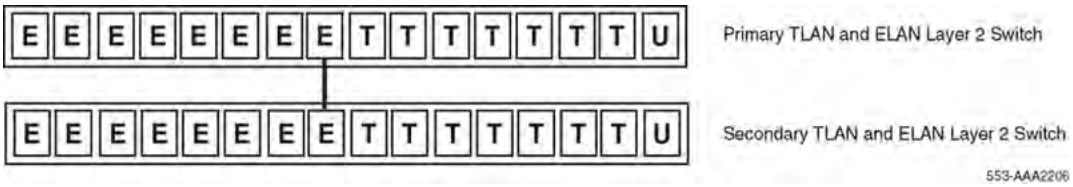


**Figure 48: Redundant core network: VLANs on the Layer 2 switch infrastructure**

**Important:**

You can use VLANs to avoid the use of two Layer 2 switches.

Figure 49: MG 1000E redundancy details on page 191 shows MG 1000E redundancy details. To obtain maximum redundancy:

- Connect alternate connecting media cards to primary and secondary Layer 2 switches.
- Connect the primary MG 1000E IPDB network interface to the primary Layer 2 switch.
- Connect the secondary IPDB network interface to the secondary Layer 2 switch.

**Note:**

It is possible to locate an MG 1000E ELAN on a different Layer 3 subnet to that of the Call Server provided that network parameters are included.

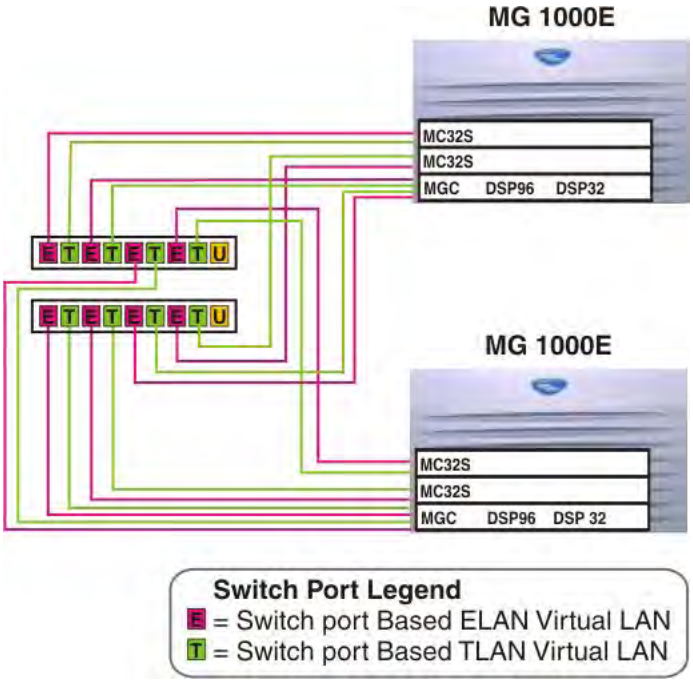


**Figure 49: MG 1000E redundancy details**

## Communication Server 1000E Campus redundancy

Figure 50: Campus redundancy: Layer 2 switch configuration on page 192 and Figure 51: Campus redundancy: Side 0 with VLANs on page 192 show campus redundancy for a Communication Server 1000E system. If you plan to use campus redundancy, follow these recommendations:

- To implement the campus redundant Layer 2 switch configuration, Virtual LANs are required on the Layer 2 switches.
- The Layer 2 switch ports that connect the HSP network interfaces must be in a completely isolated VLAN.
- Group the two gigabit fiber optic links using a multilink trunk protocol.

Enable Spanning Tree Protocol Fast Port on all switch ports and the multilink trunk or disable Spanning Tree Protocol on all switch ports.

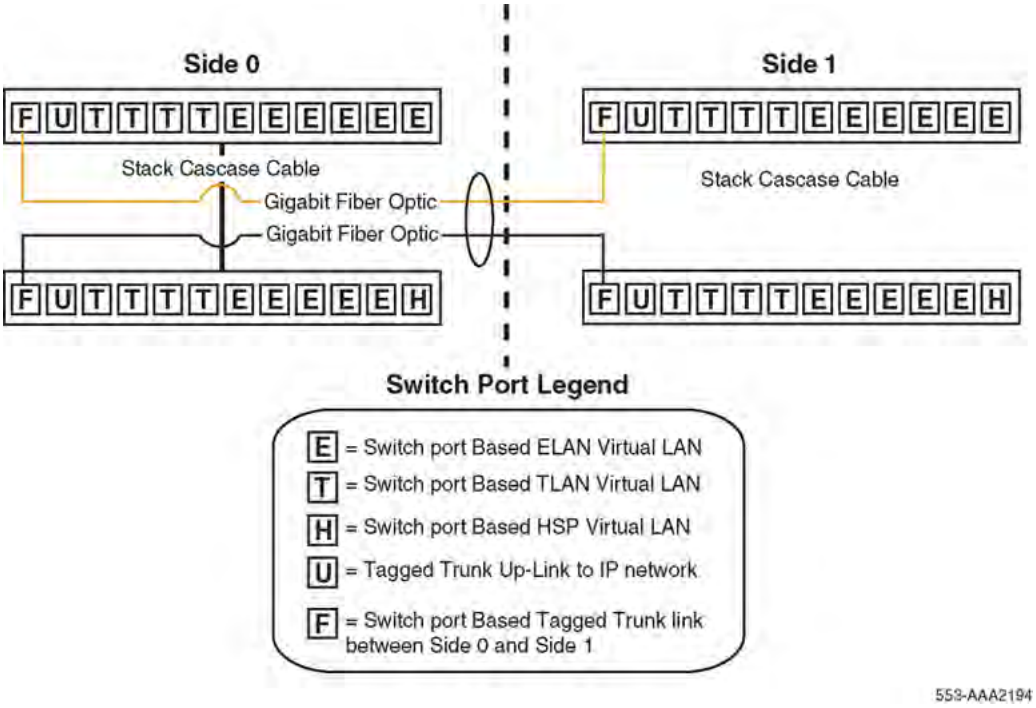


**Figure 50: Campus redundancy: Layer 2 switch configuration**

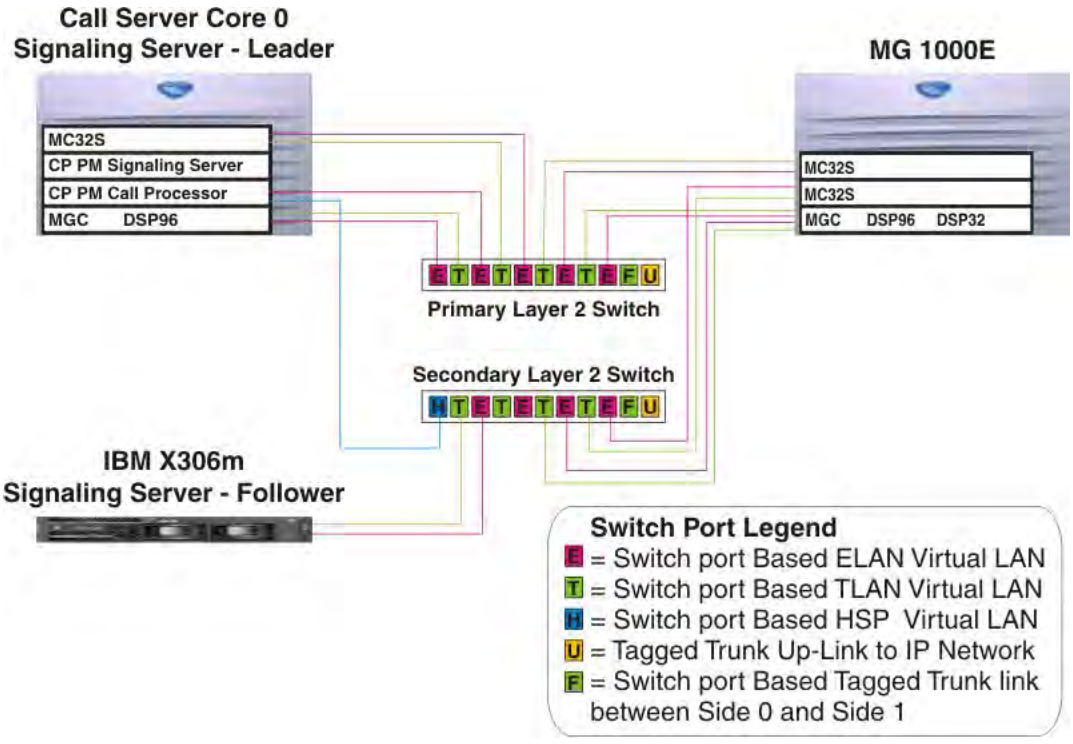


**Figure 51: Campus redundancy: Side 0 with VLANs**

**Important:**

In Figure 51: Campus redundancy: Side 0 with VLANs on page 192, Side 0 and Side 1 are considered to be identical.

For detailed information about campus redundancy, see *System Redundancy Fundamentals, NN43001-507*.

# Zone Based Dialing plan

The following components interact with this feature:

- CLID
- Features which depend on CLID
- DAPC
- Keymap download
- LNR
- ISDN (new ZBD IE)
- OCS
- Tone Table
- CallPilot
- Call Park
- Remote Call Forward
- BSF
- GR
- Pre-translation
- EM
- VNR
- Call Forward
- Call Transfer
- Conference
- PD/Corp directory
- ESA

## Feature dependencies and restrictions

The new Zone Based Dialing plan (ZBD) IE is created to send the ZBD specific data inside ISDN messages.

Use the zone based AC1/AC2/INTC/NATC parameters instead of the configuration in the route and customer data block for the zone based Dial Access Prefix on CLID (DAPC) feature. For incoming inter-site calls, access prefixes from numbering zone parameters are received and inserted to the beginning of CLID; DAPC is enabled on each telephone (CLS DAPA), for example, for an international call, AC1+INTC is inserted.

You must configure a seven-digit DN for a ZBD feature key and the site prefix must be configured from two- to four-digits.

The seven-digit DN is sent to TPS. Use the seven-digit DN to generate a user ID that implements features such as PD/RL/CL. The site prefix is cut off on the TPS side before sending the UNISTIM message to the telephone.

## LD 10, 11

LD 10 and 11 are modified to store numbering zones for telephones (IP, TDM, analog, UEXT, and PCA) in protected unit blocks.

## LD 12

LD 12 is modified to store numbering zones for an attendant in a protected unit block.

## LD 15

Prompts ZBD and DIALPLAN, are added to LD 15.

The ZBD prompt enables or disables the ZBD feature. It has a yes or no value.

Use the DIALPLAN prompt for DN/CLID processing. It includes PUB and PRV values. If the DIALPLAN prompt is configured to PUB, then the appropriate E164 CLID is displayed on a terminating telephone. If it is configured to PRV then a seven-digit DN/CLID is displayed.

## LD 20

LD 20 is modified to print out numbering zones for a telephone.

## LD 21

LD 21 is modified to print out the status of the ZBD feature, enabled or not. Also, the configured value for DIALPLAN is displayed in the ZBD prompt group.

## LD 22

LD 22 is modified to print out the status of the ZBD package.

## LD 43

ZBD databases are dumped into /u/db/ during EDD and are also backed up to the secondary device. ZBD databases are restored to /u/db/ during database restore.

## LD 81

LD 81 is modified to print out information and count configured sets for specified numbering zones.

## LD 83

LD 83 is modified to print out numbering zone for configured sets.

## LD 117

LD 117 is modified to add the following commands:

- configure/change/delete/print numbering zones
- configure/change/delete/print numbering zone parameters
- configure/change/delete/print ZFDP and ZDID entries
- change designator for numbering zones

## Feature impact on planning and engineering tasks

You must reconfigure telephones to a seven-digit DN, which consists of site prefix and short DN.

You must configure the network to guarantee an 80-millisecond (ms) round trip delay requirement for signaling between Communication Server 1000 and SMG.

# Vacant Number Routing feature

Enhancements are performed for a VNR call over IP because IP accessible users are typically a subset of the total users. If a VNR call over IP is rejected due to a specific cause, for example Cause x. If Cause x is one of the MCDN Alternate Routing (MALT) configurable causes provided in Element Manager (EM) and the user has selected Cause x to perform MALT, alternate routing is performed for the call at the Call Server. The feature impacts the treatment provided to the VNR call. The treatment is based on the previous and current rejection cause. The best treatment is provided so that the user gets the correct reason of rejection for the VNR call. MALT is performed for the existing six causes, and for any of the added ten provisional causes if the call clears from the IP network with a Do MALT indication.

This feature is an enhancement on the existing VNR feature thus you must enable the VNR feature package for the feature to work properly. For more information about VNR enhancements, see *IP Peer Networking Installation and Commissioning, NN43001-313*.

# Dialing plan

When a number is dialed, the 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.

After the call is sent over the IP network, the call is routed to the MG 1000B Core, which uses the Network Routing Service (NRS) to route the call. In a SIP network, the Redirect Server translates the address from a telephone number to a SIP URI, and authorizes the call. In an H.323 network, the H.323 Gatekeeper translates the address from a telephone number to an IP address, and authorizes the call.

Specific dialing plan configuration is required for IP Phones to properly select a main office or branch office that provides access to the PSTN for the originating IP Phone. A common configuration might be:

- Branch Users select the MG 1000B PSTN for local calls.
- Main office users select the main office PSTN for local calls.
- All users select either the main office or MG 1000B 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 Call Server. The NRS keeps track of each TNDN in the network so that it knows to which endpoint (Call Server or MG 1000B Core) to return when asked to resolve a TNDN address.

For more information, see *Dialing Plans Reference, NN43001-283*.

Nortel recommends that customers use Coordinated Dialing Plan (CDP) between the main office and its branch offices because it enables all users at the Main or Branch Office, to call each other using an extension number. CDP enables consistent dialing between the main office and MG 1000B IP telephones and devices. For more information about on-net configuration examples, see *Branch Office Installation and Commissioning, NN43001-314*.

## Off-net dialing plan

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

If routed over a Virtual Trunk, a request is sent to the NRS to determine the location of public E.164 numbers. The NRS 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 route cost to determine the least cost route.

The NRS replies with the address information for E.164 numbers and provides a list of alternative SIP or H.323 endpoints, sorted by cost. If a terminating endpoint resource is busy when a call attempt is made, the originating endpoint tries the next alternative. If no alternative is available over the IP network, the originating endpoint steps to the next entry on its route list, which could be a TIE or PSTN alternate route. For more information about off-net configuration examples, see *Branch Office Installation and Commissioning , NN43001-314*.

# Routing

The following describes routing of Branch Office calls.

## Branch user call to an MG 1000B 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 calls from an MG 1000B PSTN to an MG 1000B telephone (DID call)

If the DN is valid and can terminate, call termination at the Branch Office is treated differently for IP Phones and non-IP Phones, as follows:

- IP Phones — if the telephone is registered to the MG 1000B CP PM (Local Mode), the call is terminated locally. If the telephone is not registered to the MG 1000B CP PM (Normal Mode), the call is routed through a Virtual Trunk to the main office.
- Non-IP Phones — all are terminated locally (within the Branch Office).

If the DN is not valid, the number is considered vacant by the MG 1000B CP PM, and VNR is used to route the call to the NRS for resolution.

# SIP/H.323 zones

In a SIP/H.323 network, each NRS controls one SIP/H.323 zone. Each zone can consist of many SIP/H.323 endpoints. If a call terminates beyond the call originator zone, the Redirect Server or H.323 Gatekeeper of the called party zone provides the endpoint information to establish the connection.

You can divide a system into several zones. You can also divide a customer within a system into different zones. It is more common to assign one zone to one system and one customer.

# Distributed Media Gateway 1000E

A Media Gateway 1000E (MG 1000E) can be physically distributed within an Enterprise IP network. The gateway can be configured in a different subnet than the Call Server providing the following criteria are met:

- The Signaling Servers remain in the same ELAN subnet as the Call Server.
- Distributed Media Gateway 1000E does not support Media Card MC32.
- The TPS must be disabled for Media Cards (MC32S) in a different subnet.
- Packet loss on the Enterprise IP network must be less than 0.5% (0% packet loss is recommended).
- Round-trip delay between Call Server and MG 1000E must be less than 80 ms.
- Use of a QoS mechanism is highly recommended and assists in meeting packet loss and latency requirements.

Each ELAN subnet must be configured in a separate node and a call server can be configured to use multiple nodes. A node is a collection of signaling servers, media cards, or a combination of both. A node can be composed of a single media card or a single signaling server. A node must have one Leader; the rest of the node is configured as followers. Each subnet can have more than one node, but nodes cannot span subnets. The Leader uses the Bootstrap Protocol (BOOTP) to supply IP addresses to the followers in its node.

A media card or server configured as a follower, must be in the same ELAN broadcast domain as the Leader. If the follower is not in the same ELAN broadcast domain as the Leader, it must be configured in a different node. If the follower is the only member of the node, it must be configured as the Leader.

A follower broadcasts a BOOTP request over the ELAN to obtain available IP addresses. A Leader that has configured the MAC address of the follower in its BOOTP tables responds to the BOOTP request from the follower with the IP addresses. The follower stores the IP addresses and uses them to boot. The follower does not boot if the BOOTP request fails. If the BOOTP request fails and the follower has previously made contact with a Leader, it boots using the stored IP addresses from the last successful response.

The Gateway Controller and SSC, which control the cabinet that contains a media card, do not use BOOTP so they do not have the same restrictions as the media card. The SSC and Gateway Controller are not part of a node and cannot be used as a Leader.

# Survivable SIP Media Gateway Data Replication

Survivable SIP Media Gateways offer full survivability to the gateway and its associated endpoints because a copy of the primary system database exists on the survivability blade of the gateway. The system keeps the gateway copy up-to-date by automatically replicating data from the primary system to the gateway.

To ensure proper operation of the survivability feature the data network must meet the performance requirements for the successful replication of data from the primary system to the gateway across the data network. These performance requirements are:

- 300ms round trip delay, maximum
- Less than 1% packet loss

# DHCP configuration

This section provides general guidelines on how to configure a host with a Dynamic Host Configuration Protocol (DHCP) server to support Nortel IP Phones 200x and the IP Softphone 2050.

If you are not familiar with DHCP, Nortel recommends that you read Request for Comments (RFC) 2131 Dynamic Host Configuration Protocol, RFC 1533 DHCP Options and BOOTP Vendor Extensions, and the Help manual for the DHCP server on the host.

For a general overview about DHCP server technology, see DHCP supplemental information on page 391

## IP Phones

IP Phones 200x and the IP Softphone 2050 are VoIP telephones that function as a telephone to the Meridian 1 and Communication Server 1000 systems. The IP Phone encodes voice as binary data and packetizes the data for transmission over an IP network to the Voice Gateway Media Card or to another IP Phone.

The Nortel IP Phone can act as a DHCP client in one of two modes:

- partial DHCP mode
- full DHCP mode

All the configuration parameters for the IP Phonecan be entered manually. Each IP Phone requires network configuration parameters, Connect Server parameters, IP Telephony node ID, and Virtual TN. If there are several IP Phones to configure, manual configuration is time

consuming and prone to error. Using full or partial DHCP to automatically configure the IP Phones is more efficient and flexible and ensures that you use current information.

## Partial DHCP mode

When the IP Phone is configured to operate in partial DHCP mode, the DHCP server needs no special configuration to support IP Phones. The IP Phone receives the following network configuration parameters from the DHCP server:

- IP address configuration for the IP Phone
- subnet mask for the IP Phone IP address
- default gateway for the IP Phone LAN segment

**Important:**

In partial DHCP mode, the Connect Server parameters, (node ID and Virtual TN) must be entered manually.

## Full DHCP mode

In full DHCP mode, the DHCP server requires special configuration. The IP Phone obtains network configuration parameters and Connect Server configuration parameters from specially configured DHCP servers.

The following parameters are provided for the primary and secondary Connect Servers:

- Connect Server IP address — for IP Line 4.5, the Connect Server IP address is the IP Telephony node IP address.
- port number = 4100
- command value = 1; identifies the request to the Connect Server as originating from an IP Phone
- retry count = 10 (typically)

**Important:**

The IP Telephony node ID and Virtual TN must always be configured manually even in full DHCP mode.

## 802.1Q configuration of IP Phones

802.1Q VLAN support is configured using the display interface of the IP Phones during the initial configuration procedure of the IP Phone.

For 802.1Q configuration procedures of the IP Phones, see *IP Phones Fundamentals (NN43001-368)*.

# Configuring the DHCP server to support full DHCP mode

The DHCP capability of the IP Phone enables the telephone to receive network configuration parameters and specific Connect Server parameters. This section describes the IP Phone unique class identifier and requested network configuration and Connect Server parameters for automatic configuration.

## IP Phone class identifier

The IP Phone is designed with a unique class identifier that the DHCP server can use to identify the telephone. All Nortel IP Phones use the same text string: Nortel-i2004-A. The ASCII string is sent inside the Class Identifier option of the IP Phone DHCP messages.

The DHCP server also includes the text string in its responses to the IP Phone DHCP client to notify the IP Phone that the server is IP Phone aware, and that it is safe to accept the server offer. The string appears in the beginning of a list of specific Voice Gateway Media Card information that the IP Phone DHCP client requests.

When the DHCP server is configured to recognize the IP Phone as a special class, the DHCP server can treat the IP Phone differently than other DHCP clients. DHCP host configuration parameters can then be grouped by class to supply only information relevant to the IP Phone DHCP client, such as the Connect Server parameters. The administrator can also design the network according to the client class; if necessary, making maintenance easier.

Depending on the capabilities and limitations of the DHCP server used, and the design of the network, some advanced functions are not available.

## Requested network configuration parameters

Using full DHCP mode, an IP Phone-aware DHCP server can automatically configure Nortel IP Phones by requesting a list of Connect Server configuration parameters. The IP Phone uses DHCP to request and receive the information.

IP Phones that operate in partial DHCP mode can receive an IP address from any DHCP server. In full DHCP mode, the server must be configured to respond to the request for the vendor specific encapsulated options.

Table 36: IP Phone network configuration parameters on page 203 lists the network configuration parameters requested by the IP Phone in the Parameter Request List option (Option Code 55) in the DHCPDISCOVER and DHCPREQUEST messages. The DHCPOFFER and the DHCPACK reply messages from the DHCP server must contain the options in Table 36: IP Phone network configuration parameters on page 203.

**Table 36: IP Phone network configuration parameters**

| Parameters requested by IP Phone (Option Code 55) | DHCP server response: Option Code |
|---|---|
| Subnet mask — the client IP subnet mask | 1 |
| Router/gateways — the IP address of the client's default gateway (not required in DHCPOFFER in IP PhoneFirmware 1.25 and later for compatibility with Novell DHCP server) | 3 |
| Lease time — implementation varies according to DHCP server | 51 |
| Renewal time — implementation varies according to DHCP server | 58 |
| Rebinding interval — implementation varies according to DHCP server | 59 |
| IP Line site specific or vendor specific encapsulated/site options. | 43, 128, 144, 157, 191, 251 |

The first five parameters in Table 36: IP Phone network configuration parameters on page 203 are standard DHCP options and have predefined option codes. The last parameter is for Voice Gateway Media Card information, which does not have a standard DHCP option. The server administrator must define a vendor encapsulated and/or site specific option to transport this information to the IP Phone.

This nonstandard information includes the unique string that identifies the IP Phone and the Connect Server parameters for the primary and secondary servers. The IP Phone must receive the Connect Server parameters to connect to the IP Telephony node.

The administrator must use one of the site specific or vendor encapsulated option codes to implement the Voice Gateway Media Card information. This user defined option can then be sent as it is, or encapsulated in a Vendor Encapsulated option with Option Code 43. The method used depends on the DHCP server capabilities and the options are already in use by other vendors.

The IP Phone rejects any DHCPOFFER and DHCPACK messages that do not contain the following options:

- a router option — IP Phone requires a default gateway (router)
- a subnet mask option
- a vendor specific or site specific option

**Important:**

The vendor specific Option Code is 43. A Windows NT DHCP Server (up to SR4) supports only 16 octets of data for the vendor specific option, which is insufficient to support the minimum length of the IP Phone specific string. If you use a Windows NT DHCP Server, select the Site Specific option to accommodate the IP Phone specific string.

The site specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for site specific use by the DHCP RFCs.

## Format for IP Phone DHCP Class Identifier option

All Nortel IP Phones fill in the Class ID option of the DHCPDISCOVER and DHCPREQUEST messages with the null-terminated, ASCII encoded string Nortel-i2004-A, where A identifies the version number of the information format of the IP Phone.

The Class Identifier Nortel-i2004-A must be unique in the DHCP server domain.

## Format for IP Phone DHCP encapsulated Vendor Specific Option

The Nortel specific, encapsulated Vendor Specific Option for IP Phones 200x and the IP Softphone 2050 must be encapsulated in a DHCP vendor specific option (see RFC 1533) and returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the IP Phone to accept these messages as valid. The IP Phone extracts the relevant information from this option and uses it to configure the Connect Server IP address, the port number (4100), a command value (1), and the retry count for the primary and secondary Connect Servers.

Either this encapsulated Vendor Specific Option or a similarly encoded site specific option must be sent. The DHCP server must be configured to send one or the other but not both. The choice of using the vendor specific or the site specific option is provided to enable Windows NT DHCP servers to support the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option; and, as a result, Windows NT implementations must use the Site Specific version.

The format of the encapsulated Vendor Specific option is Type, Length, and Data.

### Type (1 octet):

There are five types:

- 0x80 (Site Specific option 128)
- 0x90 (Site Specific option 144)
- 0x9d (Site Specific option 157)
- 0xbf (Site Specific option 191)
- 0xfb (Site Specific option 251)

The choice of five types enables the IP Phone to work one or more values already in use by a different vendor. Select one value for the Type byte.

### Length (1 octet)

The Length value is variable. Count only the number of octets in the data field (see the following section).

### Data (variable number of octets)

The Data field contains an ASCII encoded character string as follows:

Nortel-i20xx-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr.

This string can be NULL terminated, although the NULL is not required for parsing.

The parameters for the data field are described in Table 37: Data field parameters on page 205 and in the list following the table.

**Table 37: Data field parameters**

| Parameter | Description |
|---|---|
| Nortel-i2004-A | Uniquely identifies the Nortel option, and is a response from a server that can provide the correct configuration information to the IP Phones 200x and the IP Softphone 2050. |
| iii.jjj.kkk.lll:ppppp | Identifies IP address and port number for the server (ASCII encoded decimal) |
| aaa | Identifies action for server (ASCII encoded decimal, range 0–255) |
| rrr | Identifies the retry count for server (ASCII encoded decimal, range 0–255) |
| comma (,) | ASCII "," separates fields. |
| colon (:) | ASCII ":" separates the IP address of the bootstrap server node IP address from the Transport Layer port number. |
| semicolon (;) | ASCII ";" separates the Primary from Secondary bootstrap server information. The bootstrap server is the Active Leader of the IP Telephony node. |
| period (.) | ASCII "." signals end of structure. |

- "aaa" and "rrr" are ASCII encoded decimal numbers with a range of 0 – 255. They identify the Action Code and Retry Count, respectively, for the associated TPS server. They are stored as one octet (0x00 – 0xFF) in the IP Phone. These fields must be no more than three digits long.
- Two Connect Servers and an optional external application server (XAS) can be specified in the DHCP string:
  - The first Connect Server is always considered primary.
  - The second Connect Server is always considered secondary.
  - An optional XAS can be appended to the Connect Servers.
- The string enables the configuration of information for two Connect Servers. One Connect Server exists for each IP node. In the typical system configuration of a single IP node, only the primary Connect Server is required. In this case, the primary Connect Server string must end with a period (.) instead of a semicolon (;). For example:

  Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr.

  If the secondary Connect Server portion of the string is specified, then the string information is typically the same as the primary Connect Server information. For example:

Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr.

When the Enhanced Redundancy for IP Line Nodes feature is used, two different Connect Server strings can be configured, separated with a semi-colon (;). This enables the telephone to register to two different nodes. For more information about the Enhanced Redundancy for IP Line Nodes feature, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

- Action code values include:
  - 0 — reserved
  - 1 — UNIStim Hello (currently this type is the only valid choice)
  - 2 to 254 — reserved
  - 255 — reserved
- The ASCII encoded decimal numbers iii.jjj.kkk.lll represent the IP address of the server. They do not need to be three digits long because the (. ) and (: ) delimiters guarantee parsing. For example, 001, 01, and 1 would be parsed correctly and interpreted as value 0x01 internal to the IP Phone. These fields must be no longer than three digits.
- The port number in ASCII encoded decimal is ppppp.. It does not need to be five digits long as the colon (:) and comma (,) delimiters guarantee parsing. For example, 05001, 5001, 1, and 00001 would be parsed correctly and accepted as correct. The valid range is 0 to 65535 (stored internally in the IP Phone as hexadecimal in a range of 0 to 0xFFFF). This field must be no longer than five digits.
- In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. Specifically, a leading zero does not change the interpretation of the value to be OCTAL-encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.
- When you use the Full DHCP option on the IP Phone 2004, the IP address of an XAS can be provided. To do this, append the XAS IP address and port to the Nortel DHCP option currently used to specify the first and second server IP address, ports, and retry and action codes. For Graphical XAS, the action code (aaa) and retry count (rrr) must be appended. For Text XAS, it is not necessary to append these values.

  The format of the exchange application server's IP address and port is:

  iii.jjj.kkk.lll:ppppp,aaa,rrr

  The XAS port action code (aaa) byte values are:
  - 1=Graphical XAS
  - 0=Text XAS

  The port field is processed if Graphical XAS is selected, but ignored for Text XAS (the fixed text port is used). XAS always uses port 5000.

  **Note:**

  If the XAS port action code (aaa) byte value is 0 (Text XAS), then the port action code and retry count fields are not required. If the XAS port action code (aaa) byte value is 1 (Graphical XAS), then the port action code and retry count fields are not optional and must be included in the configuration string.

For example, the format of the option used to specify Connect Server 1, Connect Server 2, and the exchange application server (XAS), where the XAS port action code (aaa) byte value is 1 (Graphical XAS) is:

Nortel-i20xx:A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr.

If the XAS port action code (aaa) byte value is 0 (Text XAS), the format of the option used to specify Connect Server 1, Connect Server 2, and the exchange application server (XAS) is:

Nortel-i20xx-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp

## Configuration string examples

Table 38: Configuration string for one Connect Server on page 207 to Table 43: Configuration string for two Connect Servers and an XAS (Graphical) on page 208 shows configuration strings with one or more Connect Servers and exchange application servers. The following conventions are used:

- The Nortel Class Identifier is separated from the servers by a comma (,).
- The servers are separated by semicolons (;).
- The IP address and port numbers are separated by a colon (:).
- The string is terminated with a period (.).

**Table 38: Configuration string for one Connect Server**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr. | |
|---|---|
| Nortel Class Identifier Field | Primary Connect Server |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr |

**Table 39: Configuration string for two Connect Servers**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr. | | |
|---|---|---|
| Nortel Class Identifier Field | Primary Connect Server | Secondary Connect Server |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr |

**Table 40: Configuration string for one Connect Server and an XAS (Text)**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp | | | |
|---|---|---|---|
| Nortel Class Identifier Field | Primary Connect Server | Placeholder Secondary Connect Server | XAS |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp |

| |
|---|
| Three IP addresses must be specified when using one Connect Server and XAS. If only two IP addresses are specified, the IP Phone assumes the second IP address is for the second Connect Server and does not recognize the XAS. Therefore, a placeholder IP address must be inserted for the second Connect Server in this situation. The placeholder IP address ensures that the XAS IP address appears as the third address in the string (where the IP Phone expects to find it). Nortel recommends simply repeating the IP address of the first Connect Server for the second Connect Server, to create the placeholder IP address. |

**Table 41: Configuration string for one Connect Server and an XAS (Graphical)**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr. | | | |
|---|---|---|---|
| Nortel Class Identifier Field | Primary Connect Server | Placeholder Secondary Connect Server | XAS |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr |
| Three IP addresses must be specified when using one Connect Server and XAS. If only two IP addresses are specified, the IP Phone assumes the second IP address is for the second Connect Server and does not recognize the XAS. Therefore, a placeholder IP address must be inserted for the second Connect Server in this situation. The placeholder IP address ensures that the XAS IP address appears as the third address in the string (where the IP Phone expects to find it). Nortel recommends that you repeat the IP address of the first Connect Server for the second Connect Server, to create the placeholder IP address. | | | |

**Table 42: Configuration string for two Connect Servers and an XAS (Text)**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp | | | |
|---|---|---|---|
| Nortel Class Identifier Field | Primary Connect Server | Secondary Connect Server | XAS |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp |

**Table 43: Configuration string for two Connect Servers and an XAS (Graphical)**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr. | | | |
|---|---|---|---|
| Nortel Class Identifier Field | Primary Connect Server | Secondary Connect Server | XAS |
| Nortel-i2004-A | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr | iii.jjj.kkk.lll:ppppp,aaa,rrr |

## Format for IP Phone DHCP Site Specific option

This section describes the Nortel specific, Site Specific option for the IP Phones 200x, and the IP Softphone 2050. This option uses the reserved for Site Specific use DHCP options (128 to

254) (see RFC 1541 and RFC 1533), and must be returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the IP Phone to accept these messages as valid.

The IP Phone retrieves the relevant information and uses it to configure the IP address for the primary TPS and optional secondary TPS. Either this site specific option must be present or a similarly encoded Vendor Specific option must be sent. That is, configure the DHCP server to send one or the other but not both. The choice of using either Vendor Specific or site specific options enables Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the vendor specific option and as a result, Windows NT implementations must use the Site Specific version.

The format of the option is Type, Length, and Data. The format is the same as that of the encapsulated vendor specific option (see Format for IP Phone DHCP encapsulated Vendor Specific Option on page 204).

# The VoIP network operation

The system can be managed using Communication Server 1000 Element Manager.

## Element Manager

Element Manager is a simple and user friendly, Web based interface that supports a broad range of system management tasks, that include:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, and D-channels)
- maintenance commands, system status inquiries, and backup and restore functions
- software download, patch download, and patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single access point to parameters traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease of use and access speed.
- The hide or show information option enables administrators to see information that relates directly to the task at hand.

- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer preselected defaults, lists, check boxes, and range values to simplify response selection.

The Element Manager Web server resides on the Signaling Server and can be accessed directly through a Web browser.

For more information about Element Manager, see *Element Manager System Reference – Administration, NN43001-632*.

## Network monitoring

The network design process continues after implementation of the VoIP network and commissioning of voice services over the network. If you make network changes to VoIP traffic, general intranet traffic patterns, network policies, network topology, user expectations, and networking technology can render a design obsolete or noncompliant with QoS objectives. Review the design periodically against prevailing and trended network conditions and traffic patterns, at least once every two to three weeks initially, and then on a quarterly basis.

It is assumed that the customer's organization already has processes in place to monitor, analyze, and redesign both the Meridian Customer Defined Network (MCDN) and the corporate intranet, so that both networks continue to conform to internal QoS standards. When operating VoIP services, the customer organization must incorporate additional monitoring and planning processes, such as:

- Collect, analyze, and trend VoIP traffic patterns.
- Monitor and trend one-way delay and packet loss.
- Monitor Operational Measurements.
- Perform changes in VoIP network and intranet when planning thresholds are reached.

By implementing these new processes, the VoIP network can be managed to meet desired QoS objectives.

## Determine VoIP QoS objectives

State the design objective of the VoIP network to determine the standard for evaluating compliance to meet user needs. When the VoIP network is first installed, the design objective expectations have been determined based on the work done, see Evaluating network performance on page 125.

Initially determine the QoS objective for each destination pair to ensure the mean+s of one-way delay and packet loss is below the threshold value for maintaining calls between those two sites at the required QoS level. The graphs in Figure 29: QoS levels with G.729A/AB

codec on page 130 and Figure 30: QoS level with G.711 codec on page 131 help determine what threshold levels are appropriate.

The following table describes examples of VoIP QoS objectives.

**Table 44: VoIP QoS objectives**

| Site Pair | IP Trunk 3.0 (or later) QoS objective | Fallback threshold setting |
|---|---|---|
| Santa Clara/ Richardson | Mean (one-way delay) + s (one-way delay) < 120 ms Mean (packet loss) + s (packet loss) < 0.3% | Excellent |
| Santa Clara/ Ottawa | Mean (one-way delay) + s (one-way delay) < 120 ms Mean (packet loss) + s (packet loss) < 1.1% | Excellent |

In subsequent design cycles, review and refine the QoS objective based on data collected from intranet QoS monitoring.

Determine the planning threshold based on the QoS objectives. The thresholds are used to trigger network implementation decisions when the prevailing QoS is within range of the targeted values thus allowing time for follow through of implementation processes. Configure the planning thresholds 5% to 15% below the QoS objectives, based on the implementation lag time.

## Intranet QoS monitoring

To monitor one-way delay and packet loss statistics, install a delay and route monitoring tool, such as ping and Traceroute, on the TLAN of each IP Trunk 3.0 (or later) site. Each delay monitoring tool runs continuously, injecting probe packets to each ITG site every minute. The amount of load generated by the tool is not considered significant. At the end of the month, the hours with the highest one-way delay are noted; for those hours, the packet loss and standard deviation statistics can be computed.

At the end of the month, analyze the QoS information for each site, Table 45: QoS monitoring on page 211 provides a sample.

**Table 45: QoS monitoring**

| Site pair | One-way delay Mean+s (ms) | | Packet loss Mean +s (%) | | QoS | | |
|---|---|---|---|---|---|---|---|
| | Last period | Current period | Last period | Current period | Last period | Current period | Object: ive |
| Santa Clara/ Richardson | 135 | 166 | 1 | 2 | Excellent | Good | Excellent |

| Site pair | One-way delay Mean+s (ms) | | Packet loss Mean +s (%) | | QoS | | |
|---|---|---|---|---|---|---|---|
| | Last period | Current period | Last period | Current period | Last period | Current period | Object: ive |
| Santa Clara/ Ottawa | 210 | 155 | 3 | 1 | Good | Excellent | Excellent |

Declines in QoS can be observed through the comparison of QoS between the last period and current period. If a route does not meet the QoS objective, take immediate action to improve route performance.

For information about how to obtain other specialized delay and route monitoring tool, see Network performance measurement tools on page 124.

## ITG Operational Measurements

The Voice Gateway Media Card collects Operational Measurements (OM) from the IP Phones and DSP channels and saves the information to a log file every 60 minutes. The Operational Measurements include:

- IP Phone Registration Attempted Count
- IP Phone Registration Confirmed Count
- IP Phone Unregistration Count
- IP Phone Audio Stream Set Up Count
- IP Phone Average Jitter (ms)
- IP Phone Maximum Jitter (ms)
- IP Phone Packets Lost/Late (%)
- IP Phone Total Voice Time (minutes and seconds)
- Gateway Channel Audio Stream Set Up Count
- Gateway Channel Average Jitter (ms)
- Gateway Channel Maximum Jitter (ms)
- Gateway Channel Packets Lost/Late (%)
- Gateway Channel Total Voice Time (minutes and seconds)

## OM report description

The OM log file is a comma separated (.csv) file stored on a server. A new file is created for each month of the year in which OM data is collected. It can be read directly, or imported to a spreadsheet application for post processing and report generation. Collect these OM reports

and store them for analysis. At the end of each month, identify the hours with the highest packet lost/late statistics and generate standard deviation statistics. Compare the data to target network QoS objectives.

Declining QoS can be observed by comparing QoS between periods. A consistently inferior measurement of QoS compared to the objective triggers an alarm. The customer must take steps to strengthen the performance of the route. The card creates a new log file each day and files automatically delete after seven days.

## User feedback

Qualitative feedback from users helps to confirm if the theoretical QoS settings match what end users perceive. The feedback can come from a Help Desk facility and must include information, such as time of day, origination and destination points, and a description of service degradation.

The fallback threshold algorithm requires a fixed IP Trunk 3.0 (or later) system delay of 93 ms, which is based on default IP Trunk 3.0 (or later) settings and its delay monitoring probe packets. The fallback mechanism does not adjust when IP Trunk 3.0 (or later) parameters are modified from their default values. Users can perceive a lower quality of service than the QoS levels at the fallback thresholds in the following situations:

- Delay variation in the intranet is significant. If the standard deviation of one-way delay is comparable with the voice playout maximum delay, it means that there is a population of packets that arrive too late to be used by the IP Trunk 3.0 (or later) node in the playout process.
- The jitter buffer is increased. In this case, the actual one-way delay is greater than that estimated by the delay probe.
- The codec is G.711A or G.711U. The voice packets formed by these codecs are larger (120 to 280 bytes) than the delay probe packets (60 bytes), which results in a greater delay experienced per hop. If there are low bandwidth links in the path, the one-way delay is noticeably higher in average and variation.

## QoS monitoring and reporting tools

Use QoS monitoring and reporting tools in the post installation, day-to-day activities of maintaining an acceptable QoS level for the VoIP network. Passive tools are used to monitor and report on real-time VoIP traffic metrics gathered from network devices that already collect and gather RMON information.

To adequately assess the data network on an ongoing basis, other intrusive tools are used to generate synthetic VoIP traffic. The intrusive tools are similar to those used to perform presales network assessments.

Nortel recommends that customers use a mechanism that provides notification of QoS policy breaches through e-mail, alarm, or page. The ability of these tools to generate timely reports

on QoS is also important. The QoS data is copied from holding registers into a Management Information Base (MIB) at each recording interval; therefore, the customer must periodically secure the data before it is refreshed at the next interval.

### Available tools

Some examples of QoS monitoring and reporting tools include:

- NetIQ Chariot
- RMON
- MultiRouter Traffic graphing tool
- SNMP NMS traffic reports

For more detailed information about specific QoS assessment, monitoring and reporting tools available, contact your Nortel sales representative.

## Network Diagnostic Utilities

Network diagnostic utilities are accessible on IP Phones to isolate voice quality problems. The diagnostic utilities can be run from the menu driven interface of the IP Phone itself. For details about running the diagnostic utilities on the IP Phone, see *IP Phones Fundamentals, NN43001-368*.

The diagnostic utilities are available at the OAM prompt of the Signaling Server Command Line Interface (CLI). Table 46: Network diagnostic CLI commands on page 216 describes the network diagnostic CLI commands, and indicates if they are available in Element Manager.

## Ping and traceroute

The system administrator can execute a ping or traceroute command from a specific endpoint with any arbitrary destination, typically another endpoint or Signaling Server. The CLI commands are:

- **`rPing`** — requests the IP Phone to ping a specified IP address.
- **`rPingStop`** — requests the IP Phone to stop pinging a specified IP address.
- **`rTraceRoute`** — requests the IP Phone to trace route a specified IP address.
- **`rTraceRouteStop`** — requests the IP Phone to stop tracing the route a specified IP address.

## IP Networking statistics

The system administrator can view information about the packets sent, packets received, broadcast packets received, multicast packets received, incoming packets discarded, and outgoing packets discarded. Use the CLI command **`eStatShow`** to display Ethernet statistics for a specified IP Phone.

## Ethernet statistics

The system administrator can view Ethernet statistics (for example, number of collisions, VLAN ID, speed, and duplex) for the IP Phone on a particular endpoint. The exact statistics depend on what is available from the IP Phone for the specific endpoint.

## RUDP statistics

The system administrator can view RUDP statistics (for example, number of messages sent, received, retries, resets, and uptime) for the IP Phones. Use the CLI command **`RUDPStatShow`** to display RUDP statistics.

## Real-Time Transport Protocol statistics

The system administrator can view RTP/RTCP QoS metrics (for example, packet loss, jitter, and R-value) while a call is in progress. The CLI commands are:

- **`RTPTraceShow`** — displays RTP/RTCP statistics for an IP endpoint (tcid if the endpoint is a Voice Gateway Media Card). This command can be active across all calls, and can show statistics for multiple intervals.
- **`RTPTraceStop`** — requests issuing IP endpoint to stop RTPTraceShow.
- **`RTPStatShow`** — displays RTP/RTCP statistics.

## DHCP

The system administrator can view DHCP settings (for example, IP address, S1, S2, and S4 addresses) for each IP Phone. Use the CLI command **`isetInfoShow`** to display standard DHCP configuration information, firmware version, hardware identification, and server information of an IP Phone.

**Table 46: Network diagnostic CLI commands**

| Command | Description | Available in Element Manager |
|---|---|---|
| rPing <TN \| IP> <dest><count> | Request IP Phone to ping an IP address, where:<br><TN \| IP> = TN or IP address of IP Phone issuing Ping <dest> = destination IP address <count> = number of successful ping responses the pinging IP Phone should receive. If this count is not specified, it is fixed to 4.<br>Example:<br>`oam> rping 47.11.215.153, 47.11.216.218, 5`<br>`56 bytes packets received from IP 47.11.216.218.`<br>`5 packets transmitted, 5 packets received, 0 packets`<br>`lost`<br>`minimum round trip time in ms: 0.1ms`<br>`average round trip time in ms: 0.2 ms`<br>`maximum round trip time in ms: 0.4ms` | Yes |
| rPingStop <TN \| IP> | Request for IP Phone to stop ping. | No |
| rTraceRoute <TN \| IP> <dest><count> | Request that specifies IP Phone to trace the route of a destination IP address. Where:<br><TN \| IP> = TN or IP address of IP Phone issuing rTraceRoute <dest> = the destination IP address <count> = maximum number of hops<br>Example:<br>`oam> rTraceRoute 47.11.215.153, 47.11.174.10, 6`<br>`1 -- 47.11.181.3 1.079ms 0.768ms 0.744ms`<br>`2 -- 47.11.174.10 2.681ms 2.654ms 2.690ms`<br>`3 -- * * *`<br>`4 -- * * *`<br>`5 -- * * *`<br>`6 -- last packet` | Yes |
| rTraceRouteStop <TN \| IP> | Request for IP Phone to stop route trace. | No |
| RUDPStatShow <TN \| IP> [, <clear>] | Display information received from an IP endpoint. Displayed information includes number of messages sent, number of messages received, and number of retries. If specified, the statistics are cleared before display. Where:<br><TN \| IP> = TN or IP address of an IP Phone <clear> = Clear counts of messages sent, messages received, and number of retries, where: 0 = Does not clear the statistics (default) 1 = Clears the statistics and displays zero counts | No |

| Command | Description | Available in Element Manager |
|---|---|---|
| | Example: do not clear statistics<br>`oam> RUDPStatShow 47.11.215.153`<br>`Messages sent: 309`<br>`Messages received: 321`<br>`Number of retries: 10`<br>`Uptime of current TPS registration: 2 hour 24 minutes 35 seconds`<br>Example: clear statistics<br>`oam> RUDPStatShow 47.11.215.153, 1`<br>`Messages sent: 0`<br>`Messages received: 0`<br>`Number of retries: 0`<br>`Uptime of current TPS registration: 2 hour 24 minutes 35 seconds` | |
| eStatShow <TN \| IP> [, <clear>] | Display Ethernet information received from an IP endpoint. If specified, statistics are cleared before they are displayed. Displayed information includes:<br>• interface speed and duplex mode<br>• autonegotiate protocol received/not received<br>• VLAN ID and priority<br>• packet collisions (peg count)<br>• CRC errors (peg count)<br>• framing errors (peg count)<br>Where:<br><TN \| IP> = TN or IP address of an IP endpoint.<br><clear> = Clears counts of packet collisions, CRC errors, and framing errors, where: 0 = Does not clear the statistics (default) 1 = Clears the statistics and displays zero counts.<br>Example: do not clear statistics<br>`oam> eStatShow 47.11.215.153`<br>`100 base T full duplex`<br>`Auto negotiate protocol received`<br>`VLAN ID: 88`<br>`Priority: 1`<br>`Packet collisions: 100`<br>`CRC errors: 30`<br>`Framing Errors:1`<br>Example: clear statistics<br>`oam> eStatShow 47.11.215.153, 1`<br>`100 base T full duplex`<br>`Auto negotiate protocol received`<br>`VLAN ID: 88` | No |

| Command | Description | Available in Element Manager |
|---|---|---|
| | Priority: 1<br>Packet collisions: 0<br>CRC errors: 0<br>Framing Errors: 0 | |
| isetInfoShow <TN \| IP> | Display standard DHCP configuration information, IP Phone firmware version, hardware identification, and server information of an IP Phone. Where: <TN \| IP> = TN or IP address of the IP Phone. Example:<br>oam> isetInfoShow 47.11.215.153<br>FW Version: 0602B50<br>HWID: 18006038DD1ADB6600<br>MAC: 006038DD1ADB<br>VLAN ID: 124<br>Priority: 6<br>Set IP: 47.103.225.125<br>Subnet Mask: 255.255.255.0<br>Set Gateway: 47.103.225.1<br>LTPS IP: 47.103.247.224<br>Node IP: 47.103.247.224<br>Node ID: 4420<br>S1 Node IP: 47.103.247.229<br>Port: 4100<br>Action: 1<br>S2 Node IP: 47.103.247.229<br>Port: 4100<br>Action: 1<br>S5 Node IP: 47.103.247.229<br>Port: 4100<br>XAS: Net6 | Yes |
| RTPStatShow <TN \| IP> | Display QoS polling information. Where: <TN \| IP> = TN or IP address of the IP Phone. Example:<br>The output lines in this example are truncated to fit in the available space; each line of output is actually prefixed by the following: RTPStatShow Report (RTCP-XR) from Set (164.164.8.20)<br>oam> RTPStatShow 164.164.8.20<br>Far End IP address: 164.164.8.21<br>Far End Port: 5200<br>Local Packet Sent: 2978<br>Local Packet Received: 2535<br>Local Packet Received out of order: 0<br>Local Pkt Loss: 14%<br>Local Average Jitter: 0ms<br>Local Latency: 9ms<br>Local Listening R: 63<br>Vocoder Type: 0<br>Local Avg Net Loss Rate: 14.79%<br>Local Avg Discard Rate: 0.00%<br>Local Avg Burst Density: 17.11% | Yes |

| Command | Description | Available in Element Manager |
|---|---|---|
| | Local Avg Burst Length: 2070ms<br>Local Gap Density: 10.34%<br>Local Gap Length: 1080ms<br>Local Avg End System Delay: 15ms<br>Local Avg Noise Level: 0dBm<br>Local Avg Signal Power: 0dBm<br>Local Round Trip Time Avg: 19ms<br>Local Round Trip Time Avg High: 19ms<br>Remote Listening R: 0<br>Remote Avg Net Loss Rate: 0%<br>Remote Avg Discard Rate: 0%<br>Remote Avg Burst Density: 0%<br>Remote Avg Burst Length: 0ms<br>Remote Gap Density: 0%<br>Remote Gap Length: 0ms<br>Remote Avg End System Delay: 0ms<br>Remote Avg Noise Level: 0dBm<br>Remote Avg Signal Power: 0dBm<br>Remote Round Trip Time Avg: 0ms<br>Remote Round Trip Time Avg High: 0ms<br>Remote Packet Loss: 0%<br>Remote Average Jitter: 0ms<br>Remote Latency: 0ms | |
| RTPTraceShow <TN \| IP> [, <polling period>] | Display RTP/RTCP statistics for an IP endpoint. This command can be active across all calls. Where:<br>• <TN IP> = TN or IP address of the endpoint (tcid if the endpoint is a Voice Gateway Media Card)<br>• <polling period> = Number of polling periods to be displayed. If not specified, default is 10 polling periods.<br>Example:<br>The output lines in this example are truncated to fit in the available space; each line of output is actually prefixed by the following: RTPTraceShow Report from Set (164.164.8.20)<br>oam> RTPTraceShow 164.164.8.20<br>Far End IP address: 164.164.8.21<br>Far End Port: 5200<br>Far End IP address: 164.164.8.21<br>Far End Port: 5200<br>Local Packet Sent: 2978<br>Local Packet Received: 2535<br>Local Packet Received out of order: 0<br>Local Pkt Loss: 14%<br>Local Average Jitter: 0ms<br>Local Latency: 9ms<br>Local Listening R: 63<br>Vocoder Type: 0<br>Local Avg Net Loss Rate: 14.79%<br>Local Avg Discard Rate: 0.00%<br>Local Avg Burst Density: 17.11% | No |

| Command | Description | Available in Element Manager |
|---|---|---|
| | Local Avg Burst Length: 2070ms<br>Local Gap Density: 10.34%<br>Local Gap Length: 1080ms<br>Local Avg End System Delay: 15ms<br>Local Avg Noise Level: 0dBm<br>Local Avg Signal Power: 0dBm<br>Local Round Trip Time Avg: 19ms<br>Local Round Trip Time Avg High: 19ms<br>Remote Listening R: 0<br>Remote Avg Net Loss Rate: 0%<br>Remote Avg Discard Rate: 0%<br>Remote Avg Burst Density: 0%<br>Remote Avg Burst Length: 0ms<br>Remote Gap Density: 0%<br>Remote Gap Length: 0ms<br>Remote Avg End System Delay: 0ms<br>Remote Avg Noise Level: 0dBm<br>Remote Avg Signal Power: 0dBm<br>Remote Round Trip Time Avg: 0ms<br>Remote Round Trip Time Avg High: 0ms<br>Remote Packet Loss: 0%<br>Remote Average Jitter: 0ms Remote Latency: 0ms | |
| RTPTraceStop | Request issuing IP endpoint to stop RTPTraceShow. | No |

For information about network diagnostic utilities, see *IP Phones Fundamentals, NN43001-368* and *Signaling Server IP Line Applications Fundamentals, NN43001-125* .

## Voice quality monitoring

The PVQM feature monitors voice quality by measuring the following:

- Latency: length of time for information to travel through the network, in seconds
- Jitter: variability in latency, in seconds
- Packet Loss: number of packets lost during transmission, in percentage
- R:Value: measurement of listening R-Value using ITU E-Model. R-Value maps to Mean Opinion Score (MOS).

The sampled metrics are compared to user configured thresholds to determine system performance. When sampled metrics exceed configured thresholds, statistics are generated on the system.

For details about configuring metric thresholds, see Configure voice quality metric thresholds on page 223.

Statistics for each metric are collected on the Signaling Server or Voice Gateway Media Card to create a traffic report. The traffic report classifies metric threshold violation peg counts as Warning or Unacceptable.

Each summarized traffic report is added to the IP Phone zone Traffic Report 16 (TFS016), which in turn summarizes voice quality over the reporting period on a zone-by-zone basis. IP Phone zone Traffic Report 16 (TFS016) provides the system administrator with an overall view of voice quality on the system. For information about IP Phone zone Traffic Report 16 (TFS016), see *Traffic Measurement Formats and Output Reference, NN43001-750*.

An SNMP alarm is generated when a voice quality metric threshold exceeds Warning or Unacceptable status. For details about controlling the number of SNMP alarms generated, see Configure and print zone alarm notification levels on page 223.

## IP Phones voice quality monitoring

The following diagram shows voice quality monitoring for IP Phones within the VoIP system.

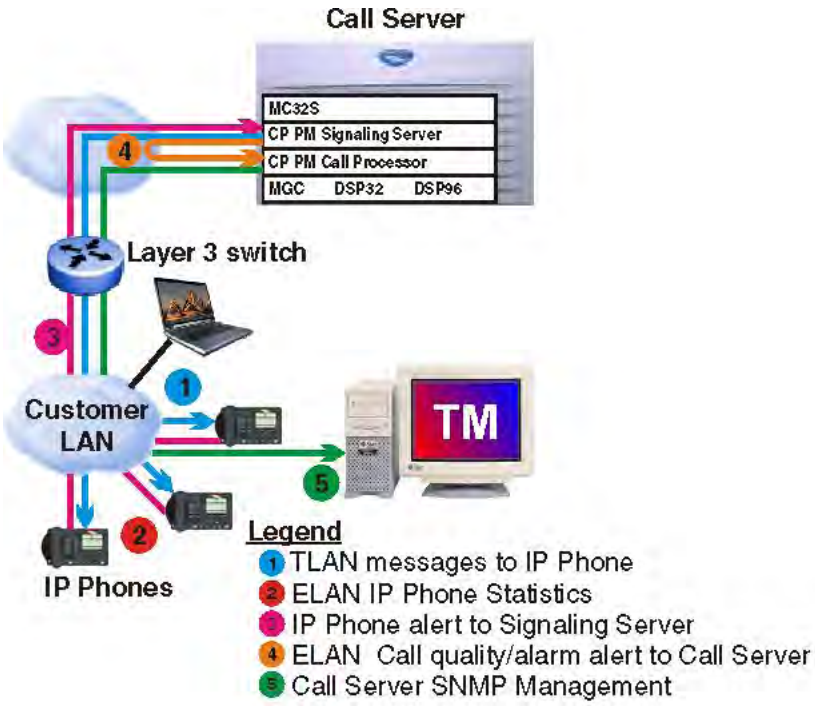


**Figure 52: IP Phones voice quality monitoring**

The following actions occur when you monitor voice quality for IP Phones:

1. The Signaling Server sends preset threshold values to the IP Phone.
2. Statistics are collected and compared on the IP Phone.
3. When a threshold is exceeded, the IP Phone sends an alert to the Signaling Server or Voice Gateway Media Card, which generates an initial SNMP alarm.

For voice quality metric alarms that reach the Unacceptable level, the path (tracer) of the voice media is written to the log file on the Signaling Server or Voice Gateway Media Card for diagnostic purposes.

4. Call quality information and alarm alert is forwarded to the Call Server.
5. The Call Server generates a second SNMP alarm.

## Voice quality alarms

Table 47: Call Server alarms: Call-by-call on page 222 identifies metrics, threshold levels, alarming severity, and QoS alarms.

**Table 47: Call Server alarms: Call-by-call**

| Metric | Threshold level | Severity | Alarms |
|---|---|---|---|
| Call Server alarms: Call-by-call | | | |
| Latency, Jitter, Packet Loss, R-Value | Warning | Info | QoS0001 - QoS0005 (excluding QoS0004) |
| Latency, Jitter, Packet Loss, R-Value | Unacceptable | Minor | QoS0007 - QoS0010 |
| Call Server alarms: Aggregated by zone | | | |
| Latency, Jitter, Packet Loss, R-Value | Warning | Minor | QoS0012 - QoS0015 |
| Latency, Jitter, Packet Loss, R-Value | Unacceptable | Critical | QoS0017 - QoS0020 |
| Signaling Server (LTPS) alarms | | | |
| Latency, Jitter, Packet Loss, R-Value | Warning | Warning | QoS0022, QoS0024, QoS0026, QoS0028 |
| Latency, Jitter, Packet Loss, R-Value | Unacceptable | Minor | QoS0030, QoS0032, QoS0034, QoS0036 |
| Latency, Jitter, Packet Loss, R-Value | Clear | Clear | QoS0023, QoS0027, QoS0029, QoS0031, QoS0033, QoS0035, QoS0037 |

For information about QoS alarms, see *Software Input Output Reference — System Messages, NN43001-712*.

## Configure voice quality metric thresholds

The system administrator can configure and print voice quality metric thresholds on a per call or zone basis. Use the following commands in LD 117:

- **CHG CQWTH** — Change voice quality Warning thresholds on a per call basis.
- **CHG CQUTH** — Change voice quality Unacceptable thresholds on a per call basis.
- **CHG ZQWTH** — Change voice quality Warning thresholds on a zone basis.
- **CHG ZQUTH** — Change voice quality Unacceptable thresholds on a zone basis.
- **PRT QSTHS** — Display all voice quality thresholds.
- **PRT AQoS** — Display QoS records for zones.
- **PRT ZQoS** — Display QoS records for zones.

For detailed information about the previous commands, see *Software Input Output — Maintenance, NN43001-711*.

## Configure voice quality sampling (polling)

Use the **CHG SQoS** command in LD 117 to configure the sampling (polling) period, zone alarm:rate collection window, and the minimum number of samples to collect during the window.

For detailed information about the previous commands, see *Software Input Output — Maintenance, NN43001-711* .

## Configure and print zone alarm notification levels

Systems that process a large number of calls potentially generate a significant number of SNMP alarms. Controlling the number of alarms by configuring zone alarm notification levels helps isolate voice quality problems and reduce network traffic.

Voice quality threshold alarms are examined for their severity relative to the alarm notification level settings. If the voice quality threshold alarm severity exceeds the configured notification level, it generates an SNMP alarm; otherwise, the alarm is suppressed.

Voice quality threshold alarm notification levels can be configured on a zone-by-zone basis so that some bandwidth zones can be monitored for all alarms and other zones will report only serious voice quality problems. Alarm notification levels are defined in Table 48: Voice quality threshold alarm notification levels on page 224.

**Table 48: Voice quality threshold alarm notification levels**

| Level | Description | Alarms |
|---|---|---|
| 0 | All voice quality alarms are suppressed | None |
| 1 | Allow zone based Unacceptable alarms | QoS0017, QoS0018, QoS0019, QoS0020 |
| 2 | Allow all of the above PLUS zone based Warning alarms | All of the above PLUS, QoS0012, QoS0013, QoS0014, QoS0015 |
| 3 | Allow all of the above PLUS per call Unacceptable alarms | All of the above PLUS, QoS0007, QoS0008, QoS0009, QoS0010, QoS0030, QoS0031, QoS0032, QoS0033, QoS0034, QoS0035, QoS0036, QoS0037 |
| 4 | Allow all of the above PLUS per call Warning alarms | All of the above PLUS, QoS0001, QoS0002, QoS0003, QoS0005, QoS0018, QoS0019, QoS0022, QoS0023, QoS0024, QoS0025, QoS0026, QoS0027, QoS0028, QoS0029 |

QoS0036 and QoS0037 are not currently reported.

The system administrator controls the number of alarms generated by the system using the **CHG ZQNL** alarm notification level configuration commands. The system administrator can print alarm notification levels using the **PRT ZQNL** command. Both commands are in LD 117.

For detailed information about these commands, see *Software Input Output — Maintenance, NN43001-711*.

## Heterogeneous environments

In an environment with a mixture of Nortel equipment and third-party equipment, voice quality monitoring, detection, and alarming is performed only on IP endpoints that have voice quality monitoring capabilities.

For information on IP endpoints and their voice quality capabilities in the system, see Table 49: IP endpoint and voice quality capabilities on page 225.

**Table 49: IP endpoint and voice quality capabilities**

| Endpoint type | Voice quality monitoring operation |
|---|---|
| IP Phones without PVQM package 401 | Detects jitter, packet loss, and latency (when the far end is RTCP compliant) threshold violations.<br>Threshold violations are detected asynchronously by the IP Phone. |
| IP Phones with PVQM package 401 | Detects jitter, packet loss, and latency (when the far end is RTCP compliant) and R-Value threshold violations.<br>Threshold violations are detected asynchronously by the IP Phone. |
| IP Softphone 2050 | Detects jitter, packet loss, and latency (when the far end is RTCP compliant) threshold violations.<br>Threshold violations are detected by polling. |
| Communication Server 1000 and Meridian 1 systems with Voice Gateway Media Cards running IP Line 4.0 (and later) | Detects jitter and packet loss threshold violations.<br>Threshold violations are detected by polling. |
| Third party Gateway | Not supported |

# Network Management

## SNMP Network Management Systems

Simple Network Management Protocol (SNMP) based Network Management Systems (NMS) monitor Real-Time networks from end-to-end. NMS ensures that problems on a network running Real-Time traffic are solved quickly to maintain high quality service.

SNMP NMS software can be configured to perform the following actions:

- map the network
- monitor network operation through polling of network devices
- centralize alarm management through SNMP traps
- notify network administrators of problems

The CS 1000 system can integrate into an NMS to provide a complete view of the converged voice and data network. Problems can be isolated quickly when looking at the entire network.

Nortel also provides a complete line of Enterprise Network management software with the Enterprise Network Management Solutions product line. An SNMP interface is available in the

traffic reporting system so that any third party system can have a standards based interface into the system traffic reports. For more information, see *Communication Server 1000 Fault Management — SNMP, NN43001-719*.

## Policy Management

Policy Management simplifies network QoS configuration by managing network QoS policies from a central location.

Details, such as Layer 2, Layer 3, Layer 4, and trust configurations can be implemented for the entire network from a central location. A variety of policy managers are usually available from the network equipment vendor.

The Common Open Policy Services (COPS) protocol is used to transmit standard policies to the network devices.

For more details on Nortel ENMS Policy Services, contact your Nortel representative.

## CS 1000 network inventory and configuration

Record the current CS 1000 design and log all additions, moves, and changes that occur in the CS 1000 network. The following information must be recorded:

- CS 1000 site information
  - location
  - dialing plan
  - IP addressing
- Provisioning of CS 1000 nodes
  - number of cards and ports
- CS 1000 node and card parameters
  - fallback threshold level
  - codec image
  - voice and fax payload
  - voice and fax playout delay
  - audio gain, echo canceller tail delay size, Silence Suppression threshold
  - software version

# Chapter 6: Configuration

This chapter contains information about configuring a converged data and voice network.

## Navigation


- Configuring Quality of Service in Element Manager on page 228
- Bandwidth Management on page 229
- Configuring Dialing Plan on page 236
- Zone Based Dialing plan on page 30
- Meridian Customer Defined Network Alternate Routing and Vacant Number Routing on page 252
- Codec configuration on page 252
- Adaptive Network Bandwidth Management configuration on page 253
- Provisioning for Tandem Bandwidth Management on page 254
- Bandwidth Management support for Network Wide Virtual Office on page 259
- Alternate Call Routing on page 264
- Zone configuration on page 281
- SIP Line service on page 317

# Communications Server 1000 configuration for network requirements

You can configure Communication Server 1000 to meet varying network requirements, with the following three basic configurations:

- A Small configuration, which is suitable for single system installations and a single ELAN subnet interconnecting all of the Communication Server 1000 dependent elements.
- A Normal configuration, which is suitable for larger installations and deploys multiple ELAN subnets or multiple Communication Server 1000 systems within the same UCM Security Domain.
- A Managed Services configuration, which is suitable for installations where complete isolation between the ELAN or Signaling and Management Network, and the various Enterprise Networks are required.

# Small configuration

The Small configuration is intended for small systems which consist of a single Call Server with a single ELAN subnet linking all of the Communication Server 1000 elements, including the UCM Primary Security Server. Routing is not required between the ELAN subnet and the TLAN/Enterprise Network. The characteristics of systems using this configuration are:

# Configuring Quality of Service in Element Manager

The following procedure describes how to configure Quality of Service in Element Manager.

1. In the Element Manager navigation tree, click **IP Telephony, Nodes: Servers, Media Cards, Configuration**.

   The Node Configuration window appears.

2. In the Node Configuration window, click **Edit** next to the node to configure.

   The Edit window appears.

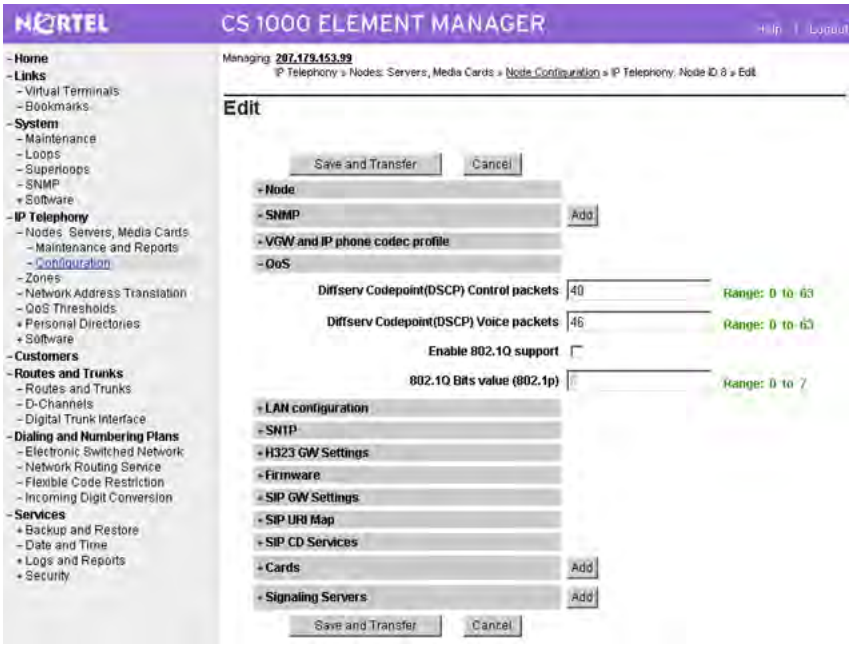


**Figure 53: QoS in Element Manager**

3. Click **QoS**.
4. From the Input Value section, the following values must be configured: Select Diffserv Codepoint(DSCP) Control packets= 40: Class Selector 5 (CS5). The range is 0 to 63. This configures the priority of the signaling messaging. Select Diffserv Codepoint(DSCP) Voice packets = 46: Control DSCP: Expedited Forwarding (EF). The range is 0 to 63. The Differentiated Service (DiffServ) CodePoint (DSCP) determines the priorities of the management and voice packets in the IP Line network. The values are stored in IP telephony CONFIG.INI file. The values used in the IP packets are respectively 160 (40*4) and 184 (46*4). Click **Enable 802.1Q support** check box. Enter 802.1Q Bits value (802.1p) (Range 0 to 7).
5. Enter the IP Phone priority in the **802.1Q Bits value (802.1p)** text box.
6. Click Save and Transfer.

# Bandwidth Management

The following sections describe how to configure Bandwidth Management in a Communication Server 1000 network.

## Configuration rules

The following list contains the configuration rules for Bandwidth Management.

- Each Call Server in the network must be configured with a unique VPNI, with the exception that branch office (MG 1000B and SRG) Call Servers must be configured with the same VPNI as that of the main office Call Server with which they register.
- Different networks usually use different VPNI numbers
- Nortel recommends that all endpoints on a Call Server (IP Phones and Voice Gateway Media Cards) be configured with the same zone number.
- Virtual Trunks must be configured with a different zone number than the endpoints.

## Configuring Bandwidth Management

Perform the following steps to configure Bandwidth Management on the Call Server.

1. Define a VPNI number in LD 15.
2. Configure the Bandwidth Management parameters for each zone on the Call Server using either Element Manager or LD 117.

   For more information about Adaptive Network Bandwidth Management configuration parameters and Configuration using LD 117, see Adaptive Network Bandwidth Management configuration on page 253.
3. Configure Call Server zones to use for endpoints (telephone and gateways).

   For more information about zones, see Zones on page 28.

   - Intrazone Preferred Strategy = Best Quality (BQ)
   - Intrazone Bandwidth = default (1 000 000 kbit/s)
   - Interzone Preferred Strategy = Best Bandwidth (BB)
   - Interzone Bandwidth = maximum bandwidth usage allowed between peer Call Servers
4. Configure Call Server zones to use for Virtual Trunks.

   - Intrazone Mandatory Strategy = Best Quality (BQ)
   - Intrazone Bandwidth = default (1000000)
   - Interzone Mandatory Strategy = Best Quality (BQ)
   - Interzone Bandwidth = default (1000000)
5. Configure the IP Phone, DSP, and Virtual Trunk data with the corresponding zone numbers.

For example, an IP Phone 2004 telephone in zone 8 `LD 11 REQ NEW TYPE 2004P1, 2004P2 ... ZONE 8`

For more information regarding Media Gateway channel zone configuration, see *Communication Server 1000E Installation and Commissioning, N43041-310*. For more information on configuring trunk zones, see*IP Peer Networking Installation and Commissioning, NN43001-313*.

# Maintenance commands

Maintenance commands can be run in Element Manager or LD 117. The prt intrazone and prt interzone commands are available in Element Manager from the Zones page.

### Printing intrazone and interzone statistics for a zone

1. In the Element Manager navigation tree, select IP Networks, Zones. The Zones window appears.
2. Click Maintenance Commands for Zones (LD 117). The Maintenance Commands for Zones pane opens, which lists the configured zones.

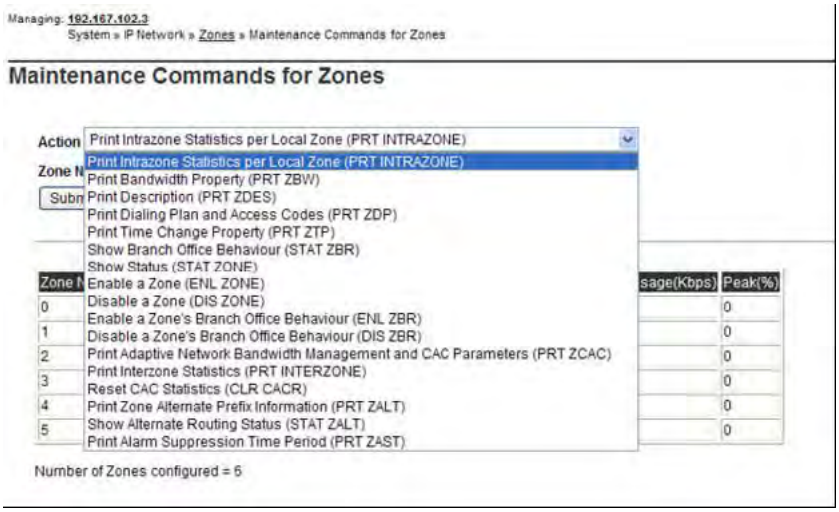


**Figure 54: Configured Zones list**

3. Perform one of the following:

   • To display intrazone statistics:

      i. Select Print Interzone Statistics (PRT INTERZONE) from the Action list.

      ii. Select a zone from the Zone Number list, by doing of the following:

         - Select ALL to print statistics for all zones.

         - Select a specific zone number to display statistics for a specific zone.

- To display interzone statistics:
  - Select Print Intrazone Statistics per Local Zone (PRT INTRAZONE) from the Action list.
  - Select a specific zone number to display statistics for a specific zone.

4. Click Submit.

   The Maintenance Commands for Zones pane appears, which displays the statistics for the specified zone or zones. A blank field indicates the statistic is either not available or not applicable to that zone.

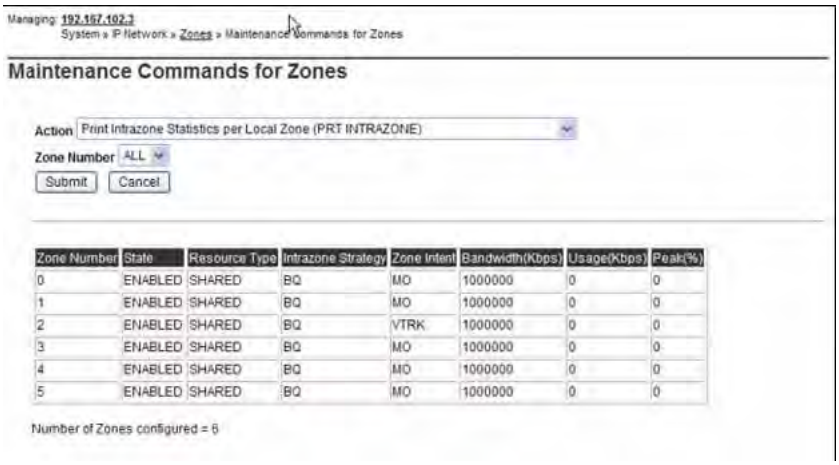


**Figure 55: Interzone statistics example**

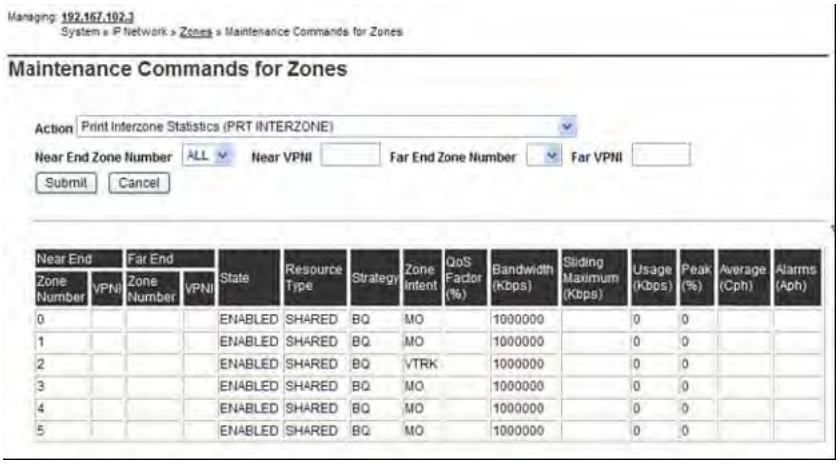


**Figure 56: Intrazone statistics example**

## Configuring a Bandwidth Management zone

You can configure a new Bandwidth Management zone using LD 117 and the NEW ZONE command. An existing zone can be modified using the CHG ZONE command.

Use the command NEW RANGE_OF_ZONES to create a range of new zones, or the command OUT RANGE_OF_ZONES to remove a range of zones.

Use the command IMPORT ZONEFILE to read a CSV file and create new zones listed in the file, or apply updates contained in the CSV file for zones that already exist. You can use the command GEN ZONEFILE to generate a CSV file that contains information for all configured zones on the Call Server.

You can use the command PRT ZPAGE to print zone information for a number of zones.

**Table 50: LD 117 – Configure Bandwidth Management zone**

| Command | Description |
|---|---|
| NEW \| CHG ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>] | Configure a new zone (NEW) or change (CHG) an existing zone, where:<br>• zoneNumber = 0–8000<br>**Caution:**<br>Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.<br>• intraZoneBandwidth = Available intrazone bandwidth (Kbit/s); Nortel recommends this value be configured to the maximum value.<br>• intraZoneStrategy = BQ (Best Quality) or BB (Best Bandwidth); Nortel recommends this value be configured to BQ.<br>• interZoneBandwidth =<br>- For Call Server zone = Maximum bandwidth usage (in Kbit/s) allowed between peer Call Servers<br>- For Virtual Trunk zones = 1000000 (Kbit/s)<br>• interZoneStrategy = BQ (Best Quality) or BB (Best Bandwidth); Nortel recommends this value be configured to BB to conserve interzone bandwidth.<br>• zoneIntent = type of zone, where:<br>- MO = Main Office (Call Server) zone<br>- BMG = Branch Media Gateway (for branch office zones)<br>- VTRK = Virtual Trunk zone<br>• zoneResourceType = resource intrazone preferred strategy, where:<br>- shared = shared DSP channels (default) |

| Command | Description |
|---|---|
| | - private = private DSP channels<br>For more information about Private/Shared Zone configuration, see*Signaling Server IP Line Applications Fundamentals, NN43001-125*. |
| DIS ZONE <zoneNumber> | Disable a zone. When a zone is disabled, no new calls are established inside, from, or toward this zone. |
| ENL ZONE <zoneNumber> | Enable a zone. |
| GEN ZONEFILE <fileName> | Generate a CSV file that contains information for all configured zones on the Call Server. You can use the <fileName> parameter to specify a file name and file path for the CSV file. If you do not specify a file name and file path, a file named zone.csv is created and stored in the /u/db directory. After you execute this command the location of the file is displayed.<br>**Note:**<br>The maximum length of the path/file name is 255 characters |
| IMPORT ZONEFILE <fileName> | Read a CSV file and create new zones listed in the file, or apply updates contained in the CSV file for zones that already exist. If you do not specify a file name and file path, an attempt is made to use the zone.csv file stored in the /u/db directory; otherwise the command will use the file name and file path that you specify. The output for this command is the number of zones successfully added or changed.<br>**Note:**<br>The maximum length of the path/file name is 255 characters |
| NEW RANGE_OF_ZONES <zoneStartNumber> <zoneAmount> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType> | Create new bandwidth zones.<br>This command creates a range of new bandwidth zones starting from <zoneStartNumber>. The number of existing bandwidth zones must be less than 8001. If the number of existing bandwidth zones is greater than or equal to 8001, no bandwidth zones are created.<br>Where:<br>• zoneStartNumber = Zone number [0–8000]<br>**Caution:**<br>Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call |

| Command | Description |
|---|---|
| | processing issues occur if you use bandwidth zone numbers greater than 255.<br>• zoneAmount = Number of zones that must be created [1-8001]<br>• intraZoneBandwidth = Intrazone available bandwidth (0 to 0.1MBps)<br>• intraZoneStrategy = Intrazone preferred strategy (Best Quality (BQ) or Best Bandwidth (BB))<br>• interZoneBandwidth = Interzone available bandwidth (0 to 0.1MBps)<br>• interZoneStrategy = Interzone preferred strategy (BQ or BB)<br>• zoneIntent = MO (default), BMG, or VTRK<br>• zoneResourceType = shared or private |
| OUT RANGE_OF_ZONES <zoneStartNumber> <zoneAmount> | Remove a range of existing bandwidth zones.<br>This command deletes a range of existing bandwidth zones, starting from <zoneStartNumber>. If there are no bandwidth zones with a zone number greater than <zoneStartNumber>, then no bandwidth zones are deleted.<br>Where:<br>• zoneStartNumber = Zone number [0–8000]<br>• zoneAmount = Number of zones that must be deleted [1-8001] |
| OUT ZONE <zoneNumber> | Remove a zone. |

**Important:**

Do not use the PRT ZONE command. It has been replaced by the PRT INTRAZONE and PRT INTERZONE commands.

**Table 51: LD 117 – Print zone statistics**

| Command | Description |
|---|---|
| PRT INTRAZONE <zone> | Print intrazone statistics for the identified zones, where:<br>• zone = ALL or 0–8000<br>The following output appears:<br>• Zone<br>• Type = PRIVATE/SHARED<br>• Strategy = BB/BQ |

| Command | Description |
|---|---|
| | • zoneIntent = MO/VTRK/BMG<br>• Bandwidth = number of Kbit/s<br>• Usage = number of Kbit/s<br>• Peak = % |
| PRT INTERZONE <nearZone> <nearVPN> <farZone> <farVPN> | Print interzone statistics for the specific VPNI zone; where:<br>• nearZone = ALL or 0–8000<br>The following output appears:<br>• Zone number = 0–8000<br>• Zone VPNI = 1–16283<br>• Type= PRIVATE/SHARED<br>• Strategy = BB/BQ<br>• ZoneIntent = MO/VTRK |
| PRT ZPAGE [<zone number> <zonesPerPage>] | Prints zone information for <zonesPerPage> zones starting from zone number <zoneNumber>. Data is printed for the following categories:<br>• zone number<br>• intrazone bandwidth<br>• intrazone strategy<br>• interzone bandwidth<br>• interzone strategy<br>• resource type<br>• zone intent<br>• description |

# Configuring Dialing Plan

Use the following procedures to configure the dialing plan for the main and branch offices and the NRS database. See Prerequisites to configure the dialing plan on page 106 before proceeding with configuration.

### Configuring the main office

1. Configure the ZACB property for the branch office zone.

**Table 52: LD 117 – Define the Zone Access Code 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 MG 1000B PSTN. |

The ZACB and ZDP 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. SRG user calls are treated exactly the same as those for main office users.

- CHG ACB <zone> ALL

  In this configuration, calls dialed with AC1 and calls dialed with AC2 undergo zone based digit manipulation. All SRG user calls can then be routed to the SRG PSTN.

  For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If an SRG user dials 1 87654321, ZDP is inserted in the dialed digits to form a digit string of 1 101 87654321. If an SRG 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 SRG user calls dialed with AC1 can then be routed to the SRG PSTN.

  For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If an SRG user dials 1 87654321, ZDP is inserted in the dialed digits to form a digit string of 2 101 87654321. If an SRG 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 SRG user calls dialed with AC2 can then be routed to the SRG PSTN.

  For example, assume that AC1 = 1, AC2 = 2, and ZDP = 101. If an SRG user dials 1 87654321, zone based digit manipulation does not occur and the digit string remains unchanged. If an SRG user dials 2 87654321, ZDP is inserted in the dialed digits to form a digit string of 2 101 87654321.

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.

The Access Code dialed by the user is used internally by the Call Server. It is not sent as part of the outpulsed digits (to the NRS or to the trunks).

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 ZDP property for the branch office zone in the main office.

**Table 53: LD 117 – Define the Zone Digit Prefix property digit manipulation**

| 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 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 Call Server and the network NRS to distinguish the SRG user calls from the main office user calls, and route them accordingly. The digit manipulation occurs before any digit processing in the main office Call Server or NRS.

**Important:**

If DialingCode1, DialingCode2, or DialingCode3 are already present in the dialed digits, then they will not be reinserted.

Nortel recommends that the ZDP attribute for each branch office zone be configured to a unique nondialable 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 and the NRS (H.323 Gatekeeper/SIP Redirect Server), 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 Call Server (step 4) routes the call to the NRS 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 NRS. The NRS recognizes 101 at the front of the digit string and routes the call to the destination SRG. At the branch office, the ESN Special Number is configured to remove 101 from the digit string and route the call based on the digits 87654321.

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 Call Server routes the call to the NRS 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 NRS. The NRS recognizes 101 at the front of the digit string and routes the call to the destination SRG. At the branch office, the ESN Special Number is configured 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 NRS. A Digit Manipulation Index (DMI) is associated with the RLI to allow manipulation of the digits to be outpulsed. For this application, at the main office, the DMI is used to update the call type of the off-net calls to the Special Number (SPN) to make sure the number stays in the Private/ Special Number domain.

4. Configure the DMI in LD 86 with the DGT feature.

   **Table 54: LD 86 – Configure the Digit Manipulation Index at the main office**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15. |
| FEAT | DGT | Digit manipulation data block |
| DMI | 1-1999 | Digit Manipulation Index numbers The maximum number of Digit Manipulation tables is defined at the MXDM prompt in LD 86. |
| DEL | (0)-19 | Number of leading digits to be deleted, usually 0 at the main office. |
| INST | x...x | Insert. Up to 31 leading digits can the main office. Default is none. |
| ISPN | (YES) NO | IP Special Number For off-net calls For on-net calls |
| CTYP | SPN LOC | Call type to be used by the call. This call type must be recognized by the NRS and far-end switch. This is critical for correct CLID behavior. If ISPN=NO, the CLID is based on this field. If ISPN=YES, the CLID is based on the call type before digit manipulation. For off- |

| Prompt | Response | Description |
|---|---|---|
| | | net calls (ISPN=YES) For on-net calls (ISPN=NO) |

5. Configure the RLI in LD 86 with the RLB feature.

**Table 55: LD 86 – Configure the Route List Index**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15. |
| FEAT | RLB | Route List data block |
| RLI | 0-127 0-255 0-1999 | Route List Index to be accessed CDP and BARS NARS FNP |
| ENTR | 0-63 X | Entry number for NARS/BARS Route List Precede with x to remove |
| LTER | NO | Local Termination entry |
| ROUT | 0-511 0-127 | Route number of the Virtual Trunk as provisioned in LD 16. Range for Large Systems Range for MG 1000B |
| ... | | |
| DMI | 1-1999 | Digit Manipulation Index number as defined in LD 86, FEAT = DGT |

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 ISPN YES CTYP NATL REQ NEW CUST 0 FEAT RLB RLI 10 ENTR 0 LTER NO ROUT 10 ... DMI ...`

6. Configure ESN Special Number and Digit Manipulation.

**Table 56: LD 90 – Configure ESN Special Number and Digit Manipulation**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15. |
| FEAT | NET | Network translation tables |
| 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 |

| Prompt | Response | Description |
|---|---|---|
| | | 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 | 0-1999 | Route List Index configured in LD 86 |
| - CLTP | LOCL NATL INTL | Type of call that is defined by the special number. Local PSTN National PSTN International PSTN |

After configuring the zone based digit manipulation and specialized route, 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.

For off:net calls the following should be considered.

- If all calls that have undergone zone based digit manipulation are to be routed by the NRS, one SPN must be provisioned for each call type to route calls to the NRS based on the ZDP.
- If some calls are to be routed by the NRS, and others by the main office Call Server, multiple SPN 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 SPN (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 SPN must be configured for each branch office. Similarly if two dialed digits are included in the SPN (ZDP + two dialed digits), a maximum of 100 SPN must be configured for each branch office. For each additional dialed digit included in the SPN, the maximum number of SPN that must be provisioned for each branch office is increased by a factor of ten.

If a single Access Code that undergoes zone based digit manipulation is used for both on-net and off-net calls, then separate DMI and SPN must be provisioned to correctly route these calls. The SPN must correctly identify the routing to be used, and its CLTP field must configure the call type correctly. A DMI, associated with this SPN, is used to make sure the number stays in the Private/Special Number domain.

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 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 b. The RLI routes the call to the NRS with the correct type of number.
- CLTP — Enter the type of call defined by this Special Number: local (LOCL), national (NATL), or international (INTL).
- 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.

  **Important:**

  RLI and DMI values do not have to be the same, but for clarity, it may be useful to configure 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 CLTP NATL … SPN
1015 FLEN 10 (7 digits for long-distance + 3 digits for ZDP) … RLI 30
CLTP LOCL … SPN 1016 FLEN 10 (7 digits for long-distance + 3 digits
for ZDP) RLI 30 CLTP LOCL ...
```

After configuring main office routing to the NRS, the NRS database must be provisioned to identify the desired endpoint for the calls. This procedure configures the NRS database with the inserted digits specified by the zone based digit manipulation configuration.

Instead of configuring the NRS database, you can configure a route in the main office to directly route the call.

## Configuring the NRS database

1. In NRS, click the **Configuration** tab.
2. Click **set Standby DB view** to work in the standby (inactive) database.
3. Select **Routing entries** from the navigation side of the **Network Routing Service** window.

   The **Routing Entries** window appears.




**Figure 57: NRS Routing Entries window**

4. Choose the appropriate Service Domain, L1 Domain, and L0 Domain from the corresponding drop down menus.
5. Click **Look up** to open a window with a lookup path for gateway endpoints.
6. Click **Search** to display a list of gateway endpoints and click on the endpoint at the branch office.




| # | ID [ Click to select ] | Support Protocol(s) | Description | # of routing entries | # of default routes |
|---|---|---|---|---|---|
| 1 | srqGWsite1 | RAS H.323 | This is a Gatew . . . | 2 | 0 |
| 2 | srqGWsite2 | RAS H.323 | This is a SRG G . . . | 0 | 0 |

**Figure 58: NRS Look up path for gateway endpoints**

A list of routing entries corresponding to that endpoint appears.

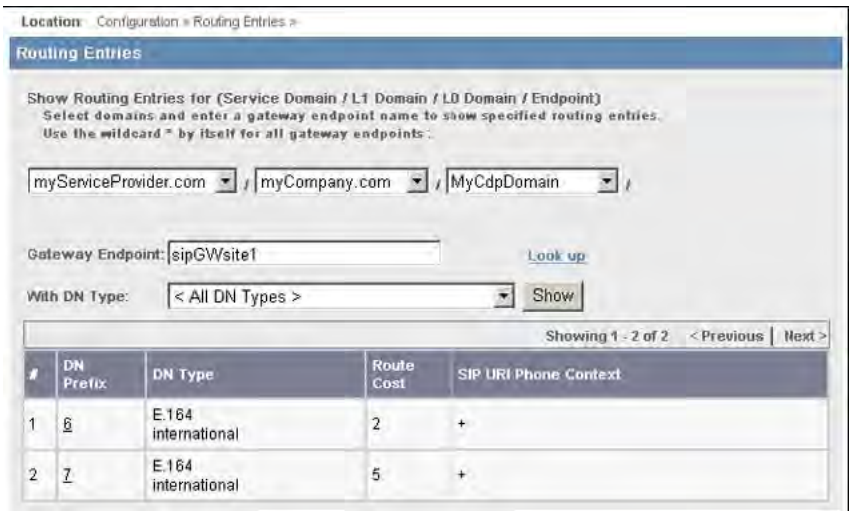


**Figure 59: NRS Routing Entries window for selected endpoint**

7. Click **Add** in the **Routing Entries** window to add a routing entry.

   The Add Routing Entry window appears.

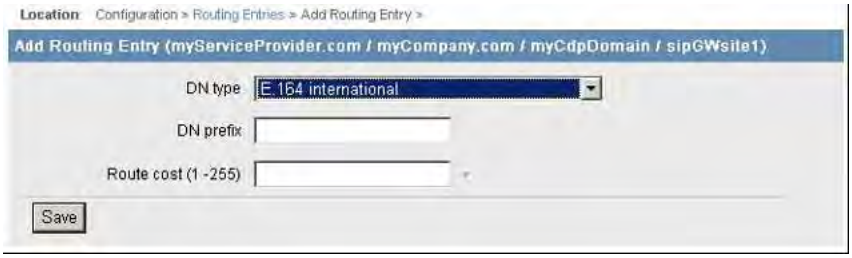


**Figure 60: Add Routing Entry**

8. Configure the numbering plan entries for the branch office. This is usually configured 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.

   The type of number configured in the NRS should be configured to match the type of number as configured in the main office.

   If some calls are to be routed differently from others, it is possible to provision the multiple Numbering Plan Entries in the NRS 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 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 NRS.

## 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. The DMI is also used to convert the call type back correctly according to the incoming SPN pattern.

2. Configure the DMI in LD 86 with the DGT feature.

   **Table 57: LD 86 – Configure the Digit Manipulation Index at the branch office**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15 |
| FEAT | DGT | Digit manipulation data block |
| DMI | 1–1999 | Digit Manipulation index numbers |
| 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. |
| ISPN | NO | IP Special Number |
| INST | x...x INTL NPA NXX LOC SPN | Insert. UP to 32 leading digits can be inserted. Call type used by the call. The far-end switch must recognize this call type. International National UDP Local PSTN Special Number |

3. Configure the RLI in LD 86 with the RLB feature.

   **Table 58: LD 86 – Configure Route List Index**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15. |
| FEAT | RLB | Route List data block |
| RLI | 0–127 0–255 0–1999 | Route List Index to be accessed CDP and BARS NARS FNP |
| ENTR | 0–63 X | Entry number for NARS/BARS Route List Precede with x to remove |

| Prompt | Response | Description |
|---|---|---|
| LTER | NO | Local Termination entry |
| ROUT | 0–511 0–127 | Route number of the Virtual Trunk as provisioned in LD 16. Range for Large Systems Range for MG 1000B |
| ... | | |
| DMI | 1–1999 | Digit Manipulation Index number as defined in LD 86, FEAT = DGT |

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 (Configure to
remove Zone Digit Prefix (ZDP) added in the main office) INST
CTYP LOC (Configure according to associated SPN pattern) REQ
NEW CUST 0 FEAT RLB RLI 18 ENTR 0 LTER NO ROUT 18 ... DMI
18 ...
```

4. Configure ESN Special Number and Digit Manipulation.

**Table 59: LD 90 – Configure ESN Special Number and Digit Manipulation**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| CUST | xx | Customer number as defined in LD 15. |
| FEAT | NET | Network translation tables |
| TRAN | AC1 | Translator – Access Code 1 (NARS/BARS) Because the call is incoming to the branch office, AC1 is triggered if INAC = YES in the Route Data Block for the Virtual Trunk in LD 16 and the INTL call type is associated with AC1 in NET_DATA of the Customer Data Block in LD 15. |
| TYPE | SPN | Special code translation data block |
| | 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 | 0-1999 | Route List Index configured in LD 86 |

After configuring the specialized route for calls that have been routed to the branch office by the NRS, the route must be associated with the ESN Special Number.

The branch office receives 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.

**Important:**

The DMI configured in LD 86 in step 1 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
```

## Configuring the branch office dialing plan using 1000 Element Manager

In Element Manager, configure the branch office–specific zone dialing plan and access codes.

1. In the Element Manager navigation tree, select **IP Network, Zones**.

   The Zones window appears.

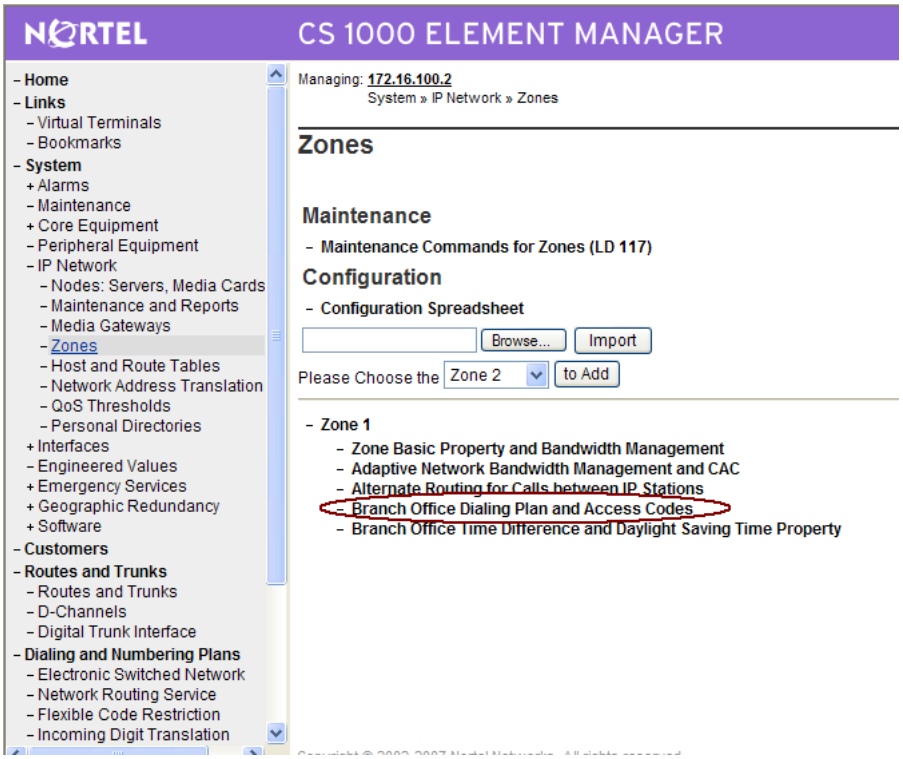


**Figure 61: Zones window**

2. In the Zones window in Element Manager, select the **Branch Office Dialing Plan and Access Codes** option, and enter the necessary information.

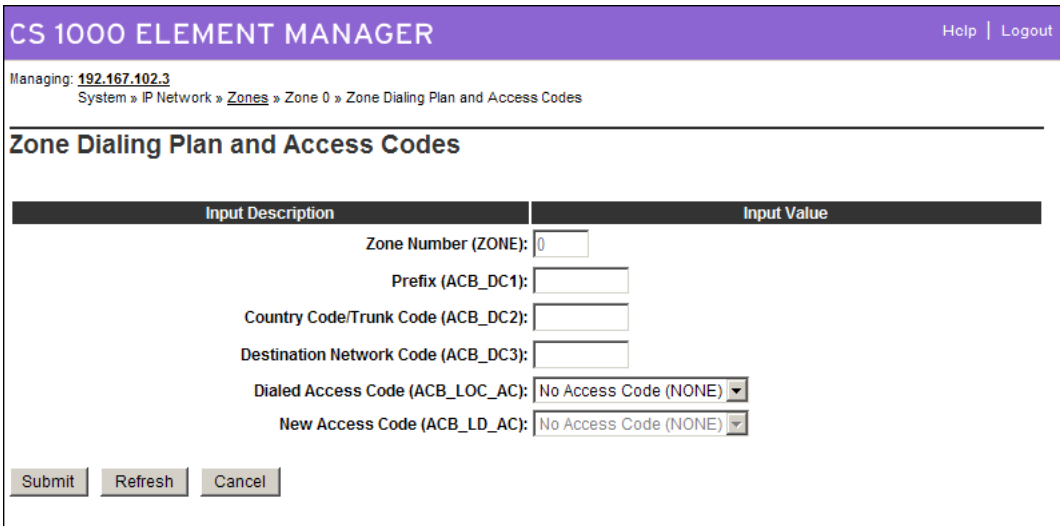


**Figure 62: Zone dialing Plan and Access Codes**

## Testing PSTN access using an SRG or MG 1000B IP Phone

Use the following procedure to test that PSTN access is working correctly.

1. From an SRG or MG 1000B IP Phone in Local Mode:
    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 an SRG or MG 1000B IP Phone in Normal Mode:
    a. Make a local PSTN call.
    b. Make a long distance call.

   The calls must be routed according to the main office ESN configuration.

## Troubleshooting

For calls that tandem over the Virtual Trunk to the branch office and go out to the PSTN trunks in the branch office, the following configuration problems can occur:

- The call receives 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 NRS might not be properly configured. If the NRS rejects the call, a diagnostic message is displayed on the 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 NRS 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#}).

For more information about troubleshooting, see *Branch Office Installation and Commissioning , NN43001-314*.

# Zone Based Dialing

To configure zone based parameters, the Zone Based Dialing plan option is activated using LD 15. After it is configured to **YES**, the `DIALPLAN` prompt is shown to select public or private on-net dial plan.

## LD 15

Use the prompt, `DIALPLAN` , in LD 15 to select public or private. If it configured to **PUB**, then appropriate E.164 `CLID` is displayed on a terminating telephone.

**Table 60: New prompts for LD 15**

| Prompt | Response | Comment |
|---|---|---|
| REQ: | CHG | Change the existing data block |
| TYPE: | FTR_DATA | Customer features and options |
| ... | | |
| VO_CUR_ZONE_TD | (NO) YES | |
| ZBD | (NO) YES | ZBD option |
| - DIAL_PLAN | PUB or PRV | Type of dialing plan for DN and CLID display |

Configure the numbering zones for telephones in LD 10, 11, and 12.

**Important:**
You can only assign numbering zones to a telephone when it is configured in LD 117.

In the following examples, assume that two sites exist; Belleville with Direct Inward Dialing (DID) numbers, 1 613 967 4xxx and Amsterdam, 31 20 630 3xxx.

## Configuring numbering zone and numbering zone based parameters

The following configuration tasks are for LD 117.

**Table 61: Configuration tasks for LD 117**

| Configuration task | Command | Input parameters | Output |
|---|---|---|---|
| Add numbering zone | NEW NUMZONE | (numbering zone number: mandatory) (parameters list – optional) | none |
| Change numbering zone parameters | CHG NUMZONE | (numbering zone number: mandatory) (parameters list – mandatory) | none |
| Remove numbering zone | OUT NUMZONE | (numbering zone number: mandatory) | none |

| Configuration task | Command | Input parameters | Output |
|---|---|---|---|
| Printout numbering zone parameters | PRT NUMZONE | (numbering zone number: optional) (range: optional) | none |

The following table displays a sample numbering zone printout.

**Table 62: Sample printout values for the PRT NUMZONE command**

| Zone | PREF | CC | NPA | AC1 | AC2 | NATC | INTC | DAC | TTBL | FLAGS |
|---|---|---|---|---|---|---|---|---|---|---|
| 0-1023 | 00-9999 | 0-9999 | 0-9999 | 0-99 | 0-99 | 0-9999 | 0-9999 | (0)-1 | (0)-32 | (0x0)-0xff |

The following list provides a description of the commands, as shown in the previous table.

- PREF: site prefix
- CC: country code
- NPA: area code, used for dialing through ZFDP
- AC1: trunk access code 1
- AC2: trunk access code 2
- NATC: national dial code
- INTC: international dial code
- DAC: the flag to delete an NPA from CLID for a local subscriber call. It also show you dial NPA for a NXX/REG2 call. If DAC is 0 then AC + NPA + NXX + DN should be dialed. If DAC is 1 then AC + NXX + DN should be dialed.
- TTBL: tone table
- FLAGS: zone specific ZBD flags (you do not need to use it for the current time; it will be used for future enhancements)

In situations where ZBD parameters are not provided, hard coded default values are used.

In situations where a zone number is not provided, the full list of ZBD zones are printed out.

Modify a prefix for zone based pretranslation using the following command and syntax: **CHG ZPARM** [numbering zone number] **PREF** [Prefix].

Add a numbering zone designator using the following command and syntax: **CHG NZDES** [numbering zone] [designator]. The designator parameter consists of a maximum of 96 characters.

**Important:**
NUMZONE 0 always exists in the system. It cannot be deleted.

You cannot configure two different numbering zones with the same PREF.

# Meridian Customer Defined Network Alternate Routing and Vacant Number Routing

Existing configurations for Meridian Customer Defined Network Alternate Routing (MALT) and Vacant Number Routing (VNR) are required for the feature to work properly.

## Meridian Customer Defined Network Alternate Routing configuration

MALT is performed based on SBOC configurations done in the RLB for VNR RLI. If you configure SBOC to RRA, then Rerouting is accomplished in the current node for all the MALT cause values. If you configure SBOC to RRO, then rerouting is accomplished at the originating node. If you configure SBOC to NRR, then MALT is not to be. Configure the MALT prompt with the number of alternate routes that are tried for the respective RLI. Configure SBOC on the last entry as a value other than RRA/RRO; make it NRR (no reroute).

## Vacant Number Routing configuration

VNR must be configured to yes in LD 15. NET_DATA and the RLI selected for VNR calls are given. The prerequisite for configuring VNR, FNP, must be configured to yes. For more information on VNR configuration, see *IP Peer Networking Installation and Commissioning, NN43001-313*.

# Codec configuration

The following sections describes how to configure codecs and in Communication Server 1000.

## G.729 VAD negotiation via SIP

When configuring the G.729 codec, the setting Voice Activity Detection (VAD), impacts largely on bandwidth usage.

Use G.729 Annex B for VAD. When SIP negotiations for media capability occur, a device explicitly states Annex B capability, or it implies VAD support by not stating support.

If you configure the IP Peer configuration as Communication Server 1000 G.729 VAD = No, and configure the other Nortel or Third Party SIP device as G.729 VAD = Yes (or do not state Annex B capability in the SIP messaging), a speech path issue could occur. To correct this, configure the Communication Server 1000 G.729 VAD = Yes.

## Configuring codecs

For information about configuring voice gateway profile data, which includes configuring codecs, see Signaling Server IP Line Applications Fundamentals (NN43001-125).

# Adaptive Network Bandwidth Management configuration

This section contains information on configuration rules and advanced notes for Adaptive Network Bandwidth Management. For information on configuring Adaptive Network Bandwidth Management, see Configuring Adaptive Network Bandwidth Management and CAC on page 283

## Configuration rules

The following list contains the configuration rules for Adaptive Network Bandwidth Management.

- Adaptive Bandwidth Management only applies to INTERZONE calls (not INTRAZONE calls).
- All branch offices (MG 1000B or SRG) associated with a particular main office must have the same VPNI as the main office Call Server.
- All IP Phones (other than the IP Softphone 2050) and DSP endpoints on a Call Server must be configured for the same zone.
- The IP Softphone 2050 used remotely must be configured for zone 0.
- Branch office systems (MG 1000B or SRG) should tandem all calls through the main office Call Server to allow bandwidth monitoring and control. The media path is direct between the branch office and any point in the network.

- Trunk Route Optimization (TRO) must be disabled between the main office Call Server and the MG 1000B Core or SRG. The media path is direct between the branch office and any point in the network.
- Adaptive Network Bandwidth Management parameters are configured on the main office only and must not be configured at the branch offices.

**⚠ Caution:**

Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.

# Advanced configuration notes

The following information describes advanced configuration for Adaptive Network Bandwidth Management.

- The default values for Cpl, Cj, Cd, Cr, and CQos can be increased to increase the response time for Sliding Maximum changes. However, increasing the default values can cause the Sliding Maximum to temporarily decrease to a lower value then necessary, resulting in the needless blocking of interzone calls.
- Increasing the value of ZQRT will increase the speed at which the Sliding Maximum increases. The same effect can be achieved by decreasing ZQRTI. However, changing these values can cause the sliding maximum to oscillate until the network degradation is removed.
- To change the notification level (ZQNL) of the Call Server so it can react to the QoS alarms, use LD 117 to change this level. For more information about alarm notification levels, see Configure and print zone alarm notification levels on page 223.

## Element Manager configuration

Element Manager can be used to enable and configure the feature.

A zone must exist before it can be configured for Adaptive Network Bandwidth Management. For more information about configuring Adaptive Network Bandwidth Management and how to create and configure basic properties of the zone, see Adaptive Network Bandwidth Management and CAC on page 282.

# Provisioning for Tandem Bandwidth Management

The following steps summarize how to provision for Tandem Bandwidth Management.

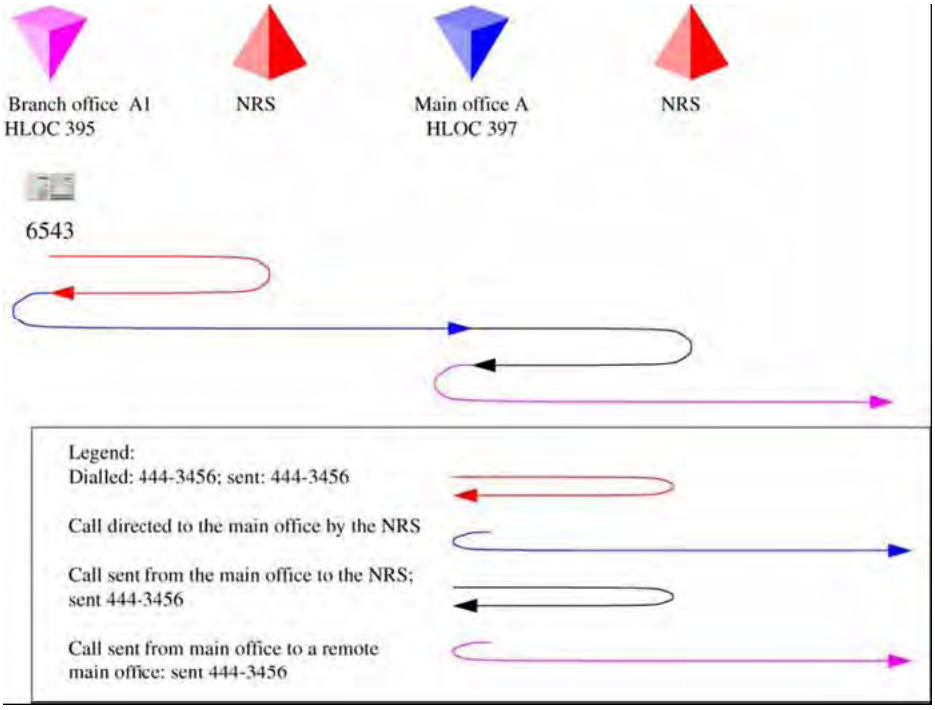


**Figure 63: Network configuration provisioning example**

1. Enter the main office Gateway endpoint identifier in the Tandem Endpoint field for each branch office gateway configured on the NRS.

   This provides tandeming for outbound calls from a branch office through its main office.

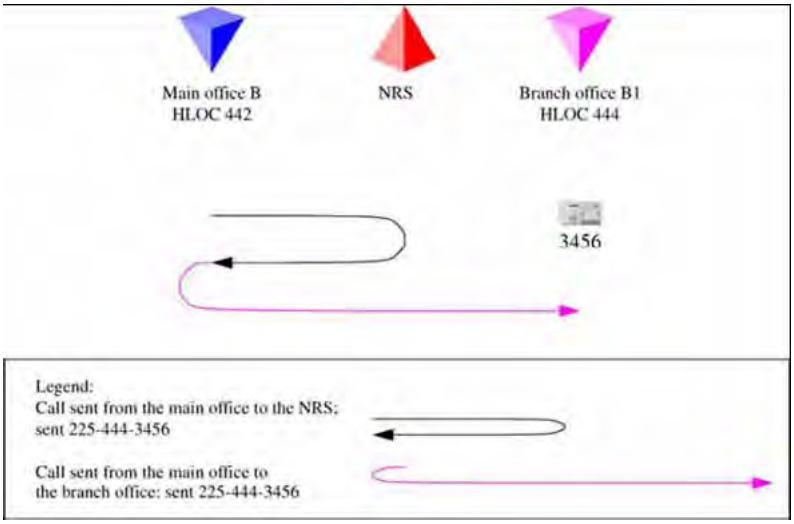


**Figure 64: Tandem endpoint configuration in Element Manager**

2. Plan the gateway routing prefixes, if not already done. At least one prefix is needed for each branch office. Any branch office that has a prefix for ESN 911 calls does not require another.

   These prefixes are SPN (Special Number) entries when using ESN 911.

3. Provision the NRS to send all calls to an LOC without a gateway routing prefix to the main office of that LOC or to the main office which provides service for the branch office using the LOC.

   In the example, the NRS is provisioned with 841 (for main office B) and 842 (for main office A).

4. Provision the NRS to send all calls to a LOC with a gateway routing prefix to the branch office directly.

   Using the gateway routing prefix and the Type of Number of SPN, the entries can be differentiated from the normal LOCs easily.

   In the example, the NRS is provisioned with 741-841 at branch office B and 742-842 for branch office A.

5. Provision the main office with the DGT table DMIs to insert the prefixes and configure the Type of Number.

6. Create RLB RLI entries to use these DMIs for the VTRK routes. One RLI per branch office is the minimum requirement. Note that calls from remote systems typically have the HLOC prefix.

**Table 63: Main office B DMI and RLI provisioning (for calls in branch office B)**

| Create a DMI | Create an RLI |
|---|---|
| LD 86 | LD 86 |

| Create a DMI | Create an RLI |
|---|---|
| REQ new | REQ new |
| CUST 0 | CUST 0 |
| FEAT dgt | FEAT flb |
| DMI 50 | RLI 50 |
| DEL 0 | ENTR 0 |
| ISPN no | LTER no |
| INST 741841 | ROUT 71 |
| CTYP loc | DMI 50 |

7. Provision the main office with CDP DSCs (mapped by the RLI into Location Codes) sufficient to uniquely identify all of its branch offices (using extended location codes, if required)

   Use the RLI index defined for each branch office as the RLI value of the LOC definition. This is the route to the branch office.

   **Table 64: Main office B LOC provisioning for LOC 741 841**

| Create a CDP mapped to the LOC: |
|---|
| LD 87 |
| REQ new |
| CUST 0 |
| FEAT CDP |
| TYPE DSC |
| DSC 4030 |
| FLEN 4 |
| RLI 50 |

8. Provision the main office and branch office with a home location code (HLOC) or multiple codes to terminate all calls that should terminate on this system.

   **Table 65: Main office and branch office HLOC provisioning: Main office B and branch office B**

| Create a DMI | Create an HLOC |
|---|---|
| LD 86 | LD 90 |
| REQ new | REQ new |
| CUST 0 | CUST 0 |
| FEAT dgt | FEAT net |

| Create a DMI | Create an HLOC |
|---|---|
| DMI 61 | TRAN ac1 |
| DEL 3 | TYPE hloc |
| ISPN no | HLOC 841 |
| | DMI 61 |

9. Provision the main office to send all other LOCs to the IP network without prefixes. These are going to a remote main office.

**Table 66: Main office B LOC provisioning for LOC to remote main office system: main office A is LOC 842**

| Create an RLI | Create a LOC |
|---|---|
| LD 86 | LD 90 |
| REQ new | REQ new |
| CUST 0 | CUST 0 |
| FEAT rlb | FEAT net |
| RLI 51 | TRAN ac1 |
| ENTR 0 | TYPE loc |
| LTER no | LOC 842 |
| ROUT 75 | FLEN 7 |
| | RLI 71 |

10. Provision the branch office with a terminating RLI with a DMI to delete the LOC prefixes.

**Table 67: Branch office terminating RLI provisioning**

| Create a DMI | Create an HLOC |
|---|---|
| LD 86 | LD 90 |
| REQ new | REQ new |
| CUST 0 | CUST 0 |
| FEAT dgt | FEAT net |
| DMI 61 | TRAN ac1 |
| DEL 6 | TYPE hloc |
| ISPN no | HLOC 741 |
| | DMI 61 |

# Bandwidth Management support for Network Wide Virtual Office

A Current Zone field for IP Phones is used to distinguish between the Bandwidth zone number configured for the IP Phone and the current nonconfigurable zone number, but is changed dynamically by Virtual Office feature operation. The Current Zone field is used in the bandwidth calculation routines instead of the Configured Zone field to have correct bandwidth calculation in case of Network Wide Virtual Office call scenarios.

The administrator can check the value of the Current Zone for IP Phones that use the LD 20, PRT command. This value is not configurable so no changes are made in LD 11.

## Prerequisites

The following configuration is used:

- Bandwidth zones are allocated on a Network-wide basis.
- All zones in the network are configured on all the Call Servers.
- All Call Servers within the network have the identical copy of the zone table and each individual zone policy.
- Main Office and Branch Office need to have the same VPNI setting to ensure correct bandwidth management control by the Main Office. Also, they must have the same VPNI setting across call servers so as to support bandwidth management for Network Wide Virtual Office (NWVO). Two systems within the same LAN requires the same VPNI setting to ensure INTRAZONE call treatment.
- Call Servers that belong to different networks have different VPNI numbers. Each network has its own individual VPNI numbers.
- Divide a network into several VPNIs if it consists of more than 255 locations. Use a zone number in the range 1 to 8000 because zone 0 does not support Alternate Call Routing and Adaptive Bandwidth Management.
- The identical copy of the zone table within the network should be configured manually unless a synchronization mechanism is introduced.

## Operating parameters

The following list describes the operating parameters to support a Network Wide Virtual Office.

- Only IP Phones with the IP Client cookies feature enabled are supported
- The correct Bandwidth Management calculation for a Virtual Office (VO) IP Phone is possible only within the home customer network (when all the systems are configured with the same VPNI number).
- The maximum number of Bandwidth Zones that can be configured on the Call Servers within the home customer network is limited to 8000 (1 to 8000).
- Interaction with previous releases is not supported. Therefore, the correct bandwidth calculation is not provided if a remote VO login is performed from a Communication Server 1000 with a software release that is earlier than Communication Server 1000 Release 5.0. In this case, the earlier release bandwidth calculation method is used.
- If two or more Call Servers have the same VPNI and Bandwidth zone configured, the usage in this zone can not be synchronized between these Call Servers.
- The feature supports only one customer. If more than one customer is configured, the customer with the lowest customer number is supported.

## Feature Packaging

The Bandwidth Management support for Network Wide Virtual Office feature requires the following two packages on the system:

- Virtual Office (VO) package 382
- Virtual Office Enhancement (VOE) package 387

## Feature Implementation

Use the following tables to implement this feature.

**Table 68: LD 15 – Define VPNI number in Customer Data Block**

| Prompt | Response | Description |
|---|---|---|
| REQ | new/chg | Add new or change existing data. |
| TYPE | NET_DATA | Networking. |
| -VPNI | 1-16283 | Virtual private network identifier. |

**Table 69: LD 117 – Define Zone data**

| Command | Description |
|---|---|
| NEW ZONE <zoneNumber> <intraZoneBandwidth> <intraZoneStratgey> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType> | Define a new Zone with parameters. All parameters must be entered:<br>• zoneNumber from 0-8000.<br>• intraZoneBandwidth from 0-0.1 Mbit/s.<br>• intraZoneStrategy is the intrazone preferred strategy where BQ is Best Quality and BB is Best Bandwidth.<br>• interZoneBandwidth from 0-0.1 Mbit/s.<br>• InterZoneStrategy is the interzone preferred strategy where BQ is Best Quality and BB is Best Bandwidth.<br>• zoneIntent is the type of zone, where MO is Main Office zone, BMG is Branch Media Gateway zone, and VTRK is Virtual Trunk zone.<br>• zoneResourceType is resource Intrazone preferred strategy, where shared is shared DSP channels and private is private DSP channels. |

**Table 70: LD 11 – Configure IP Phones**

| Prompt | Response | Description |
|---|---|---|
| REQ | new/chg | New or change request. |
| TYPE | a...a | Telephone type. Type question mark (?) for a list of possible responses. |
| TN | l s c u c u | Terminal number for Large System and Communication Server 1000E system, where l = loop, s = shelf, c = card, u = unit. Terminal number for Small System and Media Gateway 1000B, where c = card and u = unit. |
| CUST | xx | Customer number, as defined in LD 15. |
| BUID | <user_id> | Dialable DN, Main Office User ID. Enter X to delete. |
| MOTN | l s c u | Main Office TN for Large System and Communication Server 1000E system, where l = loop, s = shelf, c = card, and u = unit. Main Office TN for Small System and Media Gateway 1000B 1000T, where c = card and u = unit. |

| Prompt | Response | Description |
|---|---|---|
| ZONE | <number> | Zone Number to which the IP Phone belongs. |
| CLS | VOLA VOUA | Virtual Office Logon Allowed (VOLA) and Virtual Office User Allowed (VOUA) Allow/deny Virtual Office operation from this TN. Allow/deny Virtual Office login to this TN using other phone (destination of Virtual Office login). |

In the following two tables, use LD 15 to choose zone (current or configured) for Zone based digit manipulation.

**Table 71: LD 15 – Zone based digit manipulation (choose zone for current or configured)**

| Prompt | Response | Description |
|---|---|---|
| REQ | chg | Change existing data block. |
| TYPE | FTR_DATA | Features and options. |
| CUST | xx | Customer number. |
| VO_CUR_ZONE_ZDM | YES/NO (default) | Disable or enable using Current zone for Zone based digit manipulation. |

**Table 72: LD 15 – Time and Date (choose zone for current or configured – default value)**

| Prompt | Response | Description |
|---|---|---|
| REQ | chg | Change existing data block. |
| TYPE | FTR_DATA | Features and options. |
| CUST | xx | Customer number. |
| VO_CUR_ZONE_ZDM | YES/NO (default) | Disable or enable using Current zone for Zone based digit manipulation. |

# Feature Interactions

The following feature interactions exist.

## Zone based Digit Manipulation

The Customer Data Block (CDB) prompt is used to configure the Zone (Current or Configured) for the Zone: based Digit Manipulation feature. It allows Virtual Office (VO) users to use either

local PSTN connections of the CS were they are physically located (Current Zone), or remote PSTN connections to the CS were their VO TNs are configured (Configured Zone) depending on customer preferences

### Time and Date

The Time and Date prompt is added to the Customer Data Block (CDB) to configure the Zone (Current or Configured) for the Time and Date feature. It allows the Virtual Office (VO) user to have the local time and date appear on the IP Phone.

### Off-Hook Alarm Security

The Off-Hook Alarm Security feature uses information about the Current Zone field rather than the Configured Zone field for operation.

## Operating parameters

This section describes the operating parameters to support Alternate Call Routing (ACR).

Applies to all Communication Server 1000 systems.

Applies to station-to-station, interzone calls. The call can be between IP Phones or a TDM telephone at the main office and an IP Phone at the branch office.

Configurable for main office and branch office zones, not virtual trunk zones.

The operation of the ACR for the Network Bandwidth Management feature depends on the proper configuration of the Network Bandwidth Management feature. If Network Bandwidth Management encounters insufficient bandwidth for an interzone call, the ACR for Network Bandwidth Management feature attempts to reroute the call through the PSTN or TIE/MCDN route, if ACR is configured for the originating zone. It is possible to configure this feature to reroute all calls to MCDN or PSTN routes and still maintain the main office and branch office architecture.

Configure the Voice Gateway Bandwidth zone and the IP Phone Bandwidth zone with the same number on each Call Server.

For alternately routed calls that originate at the branch office, the network administrator must decide whether to program the main office to use conventional PSTN or TIE/MCDN routes that physically terminate at the branch office or to use conventional trunks at the main office. Outpulsed digits on the PSTN trunks must be in the format required by the Central Office serving the chosen system. For example, if the two systems are served by the same Central Office, PSTN calls can use the trunks at the main office. However, if the two systems are located

at a great distance from each other, it may make sense to program the main office to use trunks at the branch office for alternately routed calls.

If there is a location with multiple NXX codes for DID users, it is possible to translate and outpulse calls properly as long as each NXX has a unique DN range. NonDID users can be reached through the attendant console, by deleting the ALTPrefix and the DN dialed and inserting the digits in the Listed Directory Number (LDN).

When calls are rerouted to use the PSTN instead of the station-to-station IP network, there may be a loss of feature functionality normally available for station-to-station calls. Features that are not available over the PSTN are not available to the user.

This feature does not apply to virtual trunk calls. Virtual Trunk calls already have this feature and can be alternately routed using traditional methods (such as NARS), which are outside the scope of this feature.

ACR for Network Bandwidth Management does not apply to users who are registered in local mode to the branch office.

Calls that are in an ACD queue cannot be alternately routed by this feature. These calls remain in the ACD queue until an ACD agent and sufficient bandwidth are available.

Music on Hold is not affected by this feature.

A QoS0038 message prints when insufficient bandwidth is detected between two zones. A QoS0039 message prints when the ACR for Network Bandwidth Management feature is invoked.

If a user at a branch office attempts to make a conference call, ACR for Network Bandwidth Management is not invoked.

# Alternate Call Routing

When a user dials a station-to-station call between two different zones (the calling and called telephones are not located in the same geographic area) and the bandwidth limit has been reached, the Alternate Call Routing (ACR) feature is invoked.

There are many choices of alternate routes for overflow calls. Network administrators who do not want calls to be blocked, but have a limited amount of bandwidth available, overflow calls to conventional trunks (Public Switched Telephone Network [PSTN] or TIE/Meridian Customer Defined Network [MCDN]). This feature allows calls to be routed by overflowing them, trading off the capital cost of WAN bandwidth against the incremental cost of overflowed calls.

When there is insufficient bandwidth for a station-to-station call, the ACR feature uses a trunk for a call that would not normally use a trunk. The following network diagram illustrates an example of a dialed call that experiences low bandwidth or unacceptable QoS conditions and is routed to an alternate MCDN route.

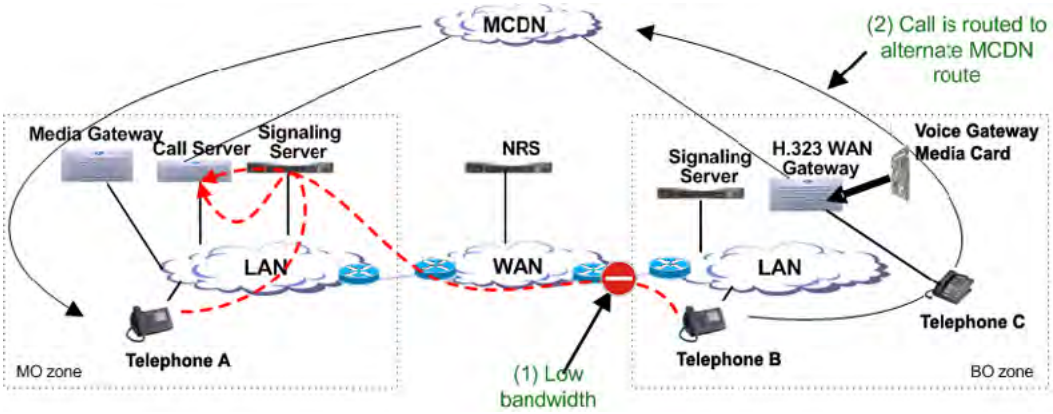


**Figure 65: Example of Alternate Call Routing**

Nortel recommends that ACR be used with Direct Inward Dial (DID) numbers, to allow calls that are rerouted over the PSTN to ring the intended telephone directly. It is possible to use this feature without DID such that when the call gets rerouted over the PSTN it reaches an attendant console or a specific telephone.

Prior to the introduction of the ACR feature, there was no alternate routing mechanism for the following station-to-station calls:

- branch office calls to or from the main office
- branch office calls to or from another branch office controlled by the same main office

This feature enables alternate routing to occur for branch office users registered to the main office, when they place interzone and station-to-station calls to the main office stations or branch office stations.

The ACR for the Network Bandwidth Management feature can be triggered by operation of either of the following features:

- Network Bandwidth Management
- Adaptive Network Bandwidth Management

The ACR for the Network Bandwidth Management feature can be configured to operate in one of the following ways:

- Insufficient bandwidth: Alternately routes station-to-station IP network calls that encounter lack of bandwidth or poor QoS in the originating or terminating zone as the calls are being established.
- All Calls: Alternately routes station-to-station IP network calls, regardless of available bandwidth.

Configure Insufficient bandwidth or All Calls as one of the modes of operation on a zone basis.

## Insufficient bandwidth

In situations where there is insufficient bandwidth to establish a call between two sites, the call is routed over the PSTN using the local PRI trunk or gateway and is then routed to the PRI

trunk or gateway nearest to the other site. The terminating end point answers the call and a voice path is established between the two end points over the PSTN.

For an inter site calls, the usual NARS step-back-on-congestion mechanism engages if the call fails to connect due to insufficient bandwidth. The next entry in the route list, if configured to do so, routes the call over the PSTN.

For calls within the same call server where there is insufficient bandwidth, the call cannot be rerouted using the usual step-back-on-congestion mechanism. An alternate route is configured for each zone with a ZALT prefix defined in LD 117 for routing the call.

## Unregistered resources

Alternate Call Routing (ACR) for unregistered resources is used to reroute calls if the terminating resource, such as a telephone or DSP, is unregistered locally but is likely to be registered elsewhere in the network, for example, an SMG in survivable mode. The alternate route can be a PSTN resource or any other available network.

The Flexible Orbiting Prevention Timer (FOPT) is configured to prevent an infinite loop from occurring in the network. The FOPT defaults to six-seconds and blocks subsequent call redirections from occurring on that resource within the same six-second period. When ACR is blocked by Orbit Prevention, the “no answer” call processing treatment configured for that resource such as Hunt or Call Forward No Answer (CFNA) is applied.

For example, in a situation where both locations are in survivable mode and a call is made to an IP Phone that appears unregistered on the local SMG, the prefix is extracted from the ZALT table and is appended to the dialed digits. The SMG reattempts to route the call using a routing entity, such as the PSTN, to the SMG where the destination IP Phone is likely to be registered. If the IP Phone is not registered on the target SMG and is redirected back to the local SMG within the FOPT timer period, Orbit Protection blocks this and any other redirections regardless of the origin, and the “no answer” call processing treatment is applied. For more information about example call flows, see *Dialing Plans Reference, NN43001-283*.

Each zone on which ACR is enabled must have a ZALT prefix defined to route calls. The Alternate Prefix (ALTPrefix) is configured in LD 117 using the Zone Alternate Route (ZALT) command. ACR for unregistered resources is enabled or disabled in LD 117 by configuring Unreg ACR to Yes or No. FOPT is configured in LD 15 using the TIM_DATA command. The FOPT input parameter must be even numbers from 0 and 30.

**Important:**

Call Forward (CFW) and ACR for unregistered resources share the Orbit Prevention feature. ACR for unregistered resources provides the same alternate routing function as ACR for Network Bandwidth Management, see Insufficient bandwidth on page 265. ACR for unregistered resources also applies in a High Scalability scenario. For more information, see *Communication Server 1000E Planning and Engineering -- High Scalability Solutions, NN43041-221*.

## LD 117

Configure the ZALT prefix in LD 117, as shown below.

CHG ZALT <zone> <ALTPrefix> [<All calls>] [<Unreg ACR>]

- zone: is the property to change
- ALTPrefix: is a digit string of up to seven digits that is appended as a prefix to the dialed number. ALTPrefix is used for calls that cannot be routed through the WAN due to insufficient bandwidth, poor QoS, or the terminating resource is unregistered.
- All calls: is configured to Yes or No to allow or deny alternate routing for the all call subfeature. The parameter is optional and configured to No by default.
- Unreg ACR: is configured to Yes or No to enable alternate routing for the unregistered resources subfeature. The parameter is optional and configured to No by default.

## Dialing plan

There are many ways that calls are dialed in a network. A station-to-station call is dialed using the following.

- Directory Number (DN)
- Coordinated Dialing Plan DN (starting with a Local Steering Code or Distant Steering Code)
- Uniform Dialing Plan DN (starting with a Location Code or Home Location Code)
- Transferable DN (TNDN) or Group Dialing Plan DN

Main offices and branch offices must be able to translate the calls, after the ALTPrefix is inserted, using CDP or VNR. Take into account the format of the calls with an ALTPrefix inserted prior to the rest of the digits.

Before deciding whether to program the steering codes as Distant Steering Codes (DSC) or Trunk Steering Codes (TSC), take into account that the system counts the digits in calls that start with a DSC.

Without Flexible Numbering Plan (FNP), DSC calls must have the same number of digits as specified in LD 86 ESN (the NCDP prompt). With FNP, fewer digits are acceptable, if the FLEN prompt is programmed correctly.

The maximum length of a CDP DN is seven digits (if DNXP is not equipped), and ten digits, if DNXP is equipped. For more information, see*Dialing Plans Reference, NN43001-283*.

Calls preceded by the ALTPrefix can be handled by the Vacant Number Routing (VNR) feature. Use Flexible Numbering Plan (FNP) software for this type of routing.

# Feature interactions

The following feature interactions exist.

## Automatic redirection of IP trunk calls

For the Communication Server 1000 Release 5.5 Alternate Routing for Network Bandwidth Management feature, the SRG does not support an automatic redirection of IP trunk calls through the PSTN when such calls are blocked by the Communication Server 1000 due to bandwidth availability.

## Call Redirections

The ACR for the Network Bandwidth Management feature works with Call Transfer, Call Forward All Calls, and Conference. Redirection operates as if the user dialed the ALTPrefix manually.

## Controlled Directory Number

Calls to Controlled Directory Numbers (CDN) are not supported for Alternate Call Routing; the feature is for station to station calls.

## Multiple Appearance Directory Number

Alternate Call Routing (ACR) for the Network Bandwidth Management feature checks for zone number only against the first member of the MADN group. The assumption is that you configure all members of the MADN group in the same zone. If you configure MADNs across multiple zones, then not all members of the MADN group can answer a call that uses ACR.

## Network Bandwidth Management

The ACR for the Network Bandwidth Management feature does not detect insufficient bandwidth. It reacts to insufficient bandwidth detected by the Network Bandwidth Management and Adaptive Network Bandwidth Management features.

## Network Class of Service

The calling telephone must have an Network Class of Service (NCOS) assigned that allows the call to use the alternate route.

### Network Routing Service (NRS)

Both the main office and branch office must be registered on the Nortel NRS for tandem routing to work for main office to branch office tandeming.

### Trunk Route Optimization (TRO)

Disable Trunk Route Optimization between the branch office (or SRG) and the main office to allow the tandeming required for the feature to work.

### UEXT TNs

The ACR for unregistered resources feature applies to all .ETHERSET subtypes with the exception of UEXT TNs, for example, Mobil-X and SIPL as the UEXT TNs always appear unregistered in normal operation. WiFi and IP 2050 phones can appear unregistered on a routine basis so the ACR feature is configurable on a bandwidth zone basis.

### Virtual Office

It is not possible to determine the real Bandwidth Zone of a telephone logged in as a Virtual Office telephone.

## Feature packaging

The ACR for Network Bandwidth Management feature requires the software package Coordinated Dialing Plan (CDP) package 59 and the optional package Flexible Numbering Plan (FNP) package 160.

## ALTPrefix

When the ACR for Network Bandwidth Management feature is invoked, the dialed number is modified with a prefix (called the ALTPrefix) inserted at the beginning of the digit string. The ALTPrefix can have a maximum of seven digits.

The system handles the call with the ALTPrefix inserted as if the user had dialed the digits.

The ALTPrefix applies to the zone in which the call originates. There is one ALTPrefix for each zone that requires alternate routing.

All Call Servers must be able to translate the ALTPrefixes for all zones that require ACR for Network Bandwidth Management.

# Alternate Call Routing for Network Bandwidth Management scenarios

The following section describes how Alternate Call Routing (ACR) works.

## Call from branch office telephone in Normal Mode

The following examples present the steps that occur in ACR scenarios from a branch office telephone in normal mode.

1. The interzone station-to-station call is attempted. There is insufficient bandwidth available to make the call.
2. The main office inserts the ALTPrefix associated with the originator's zone (the branch office in this case) before the dialed digits.
3. The main office uses Coordinated Dialing Plan (CDP) or Vacant Number Routing (VNR) to route the call to a virtual trunk.
4. A request is made to the NRS to determine the endpoint. The NRS returns the branch office address as the endpoint.
5. The call is routed on the virtual trunk to the branch office.
6. The branch office treats the ALTPrefix as a steering code. The branch office determines the Route List Index (RLI) and uses a Digit Manipulation Index (DMI) to change the dialed number into a PSTN/MCDN formatted number.
7. The call is routed over the PSTN/MCDN trunks to the telephone at the main office or other branch office.

## Prerequisites for a call between a Branch Office and a main office telephone

At the main office, configure the following:

- Use one of the dialing plan software packages to process the call, such as CDP or NARS.
- Provision an ALTPrefix for the BO2 zone.
- Provision the ALTPrefix as a Steering Code at the main office. Build a Route List Index (RLI) so these calls go to the virtual trunk or configure the Vacant Number Routing feature to do the same.

At the branch office:

Provision the ALTPrefix as a steering code. Build a Route List Index and DMI associated with this steering code that alternately routes these calls to the PSTN with the correct digits.

At the NRS:

Create a CDP entry for the ALTPrefix in the branch office gateway.

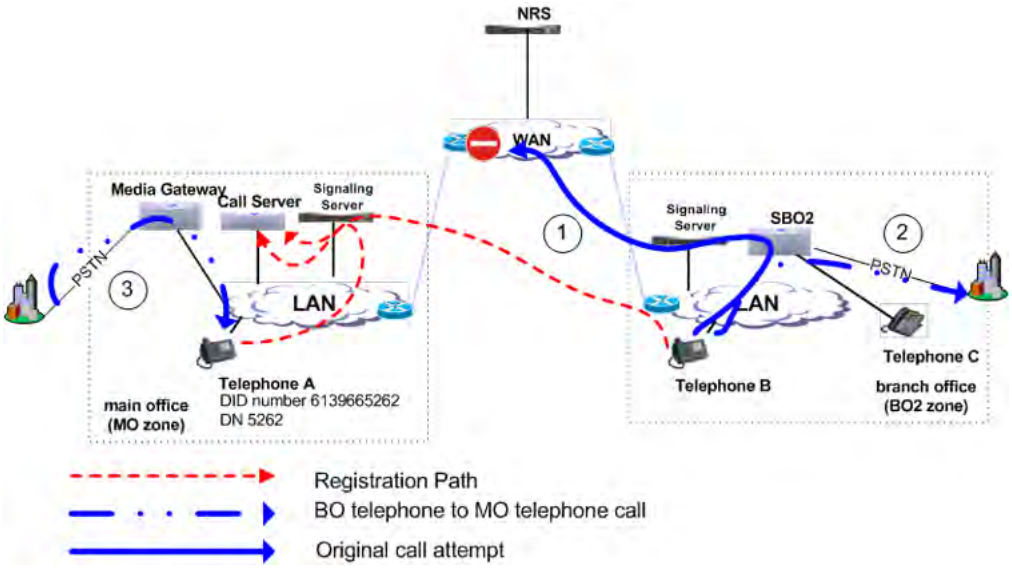


**Figure 66: Call from a branch office telephone in normal mode to a main office telephone**

1. The user for Telephone B in the BO2 zone dials Telephone A in the MO zone (DN 5262). See action labeled 1 in the previous diagram.
2. The main office Call Server determines there is insufficient bandwidth between the two zones.
3. The Call Server inserts the ALTPrefix configured for the BO2 zone prior to the telephone number of Telephone A, dialed by the user.

   For example, if the ALTPrefix assigned is 222, the dialed number becomes 2225262.
4. The call is routed to the virtual trunk by CDP or VNR. The virtual trunk sends a request to the NRS for address resolution. The digit string sent to the NRS contains the ALTPrefix. The NRS returns the IP address of the Branch Office endpoint to the virtual trunk.
5. The virtual trunk places the call to the Branch Office.
6. The Branch Office receives the call and recognizes the first part of the number as a Steering Code. The call is steered to an RLI. The DMI manipulates the number into a PSTN number and the Branch Office outpulses the digits to the Central Office (CO) serving the Branch Office. (This may be the same CO as the one serving the main office.) If the alternate route has MCDN trunks in the BO2 zone, the call is outpulsed on one of these trunks, after the Branch Office uses Digit Manipulation.

See action labeled 2 in Figure 66: Call from a branch office telephone in normal mode to a main office telephone on page 271.

For example, The digit string 2225 is programmed as a Distant Steering Code (DSC) at the Branch Office. Calls starting with this DSC are handled by an RLI with PSTN trunks as an entry. If the Public format number for the destination telephone is a DID number, then the Digit Manipulation Index associated with the PSTN route must:

- delete 3 digits (remove the ALTPrefix 222)
- insert 1613966 (to compose the DID number of the destination telephone, which is 15063486020)

This example is illustrated in Figure 67: Digits dialed and outpulsed between Branch Office and main office on page 273.

7. The call comes into Telephone A from the PSTN or MCDN trunks in the main office zone. See action labeled 3 in Figure 66: Call from a branch office telephone in normal mode to a main office telephone on page 271.

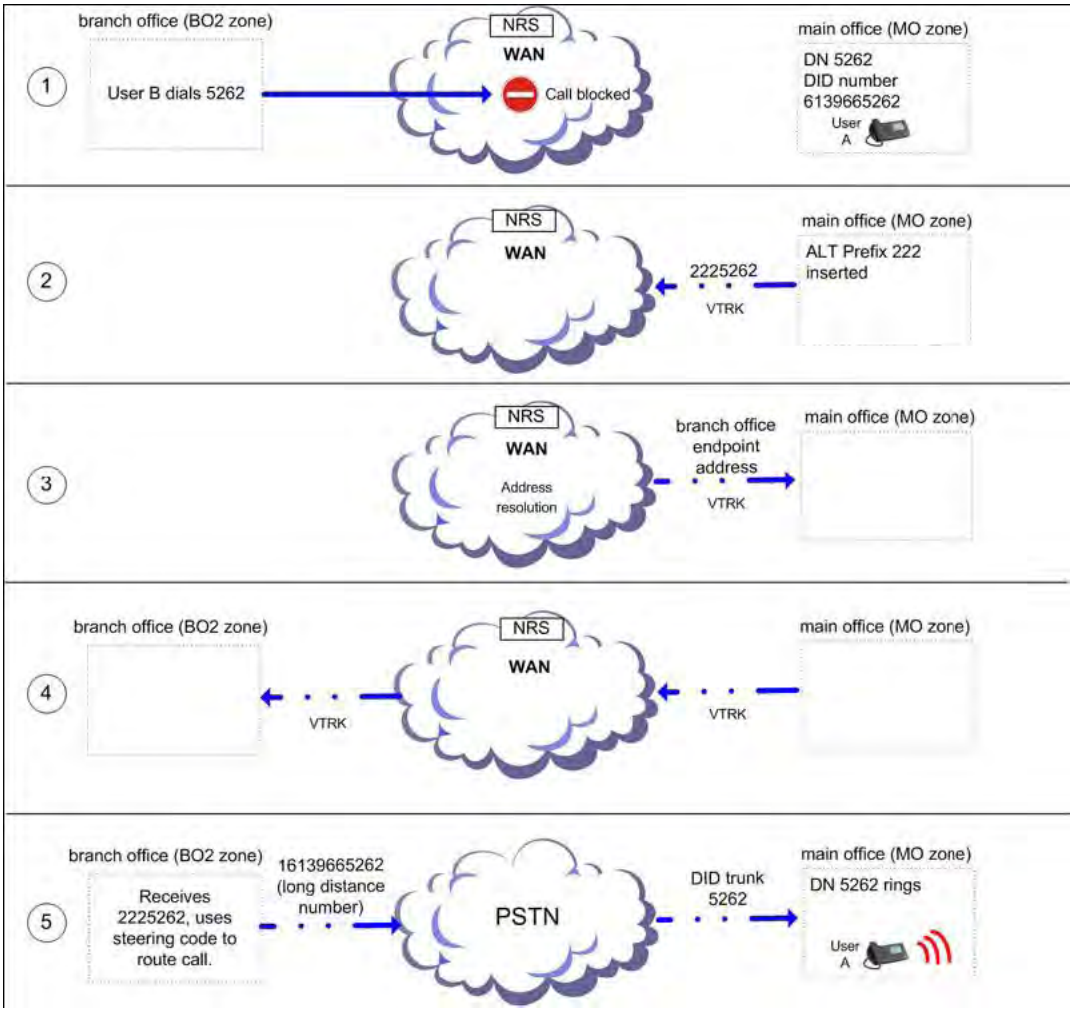


**Figure 67: Digits dialed and outpulsed between Branch Office and main office**

## Call from main office to Branch Office telephone

The following examples present the steps that occur in ACR scenarios from the main office telephone to a branch office telephone.

1. The interzone station-to-station call is attempted. There is insufficient bandwidth available to make the call.
2. The main office inserts the ALTPrefix associated with the originator's zone (the main office in this case) before the dialed digits.
3. The main office uses CDP and recognizes the ALTPrefix as a steering code.
4. The main office determines the RLI and uses a DMI to change the dialed number into a PSTN/MCDN formatted number.
5. The call is routed over the PSTN/MCDN to the telephone at the branch office.

With the ALTPrefix digits inserted, the resulting number must be one that CDP or VNR software can process as a steering code.

The main office manipulates the digits in the call into a number appropriate for routing from the SRG on PSTN/MCDN trunks.

The steering code allows the call to be translated and referenced to a RLI from which the system chooses the alternate route. The digit manipulation capability of CDP allows digits (such as the ALTPrefix) to be deleted, and it can also insert digits so the resulting number is appropriate for the alternate route choice selected (PSTN or MCDN). For example, you can manipulate the digits for PSTN routes so that DID destinations are dialable.

### Prerequisites for a call between a main office and a Branch Office telephone

At the main office configuring the following:

- Use one of the dialing plan software packages to process the call, such as CDP or NARS.
- Provision an ALTPrefix for the BO2 zone.
- Provision the ALTPrefix as a Steering Code. Build a Route List Index (RLI) so these calls go to the virtual trunk or configure the Vacant Number Routing feature to do the same.
- Provision the ALTPrefix as a Steering Code. Build a Route List Index (RLI) and Digit Manipulation Index (DMI) associated with this steering code that can alternately route calls to the PSTN.
- Configure a DMI to outpulse the correct digits to the Branch Office telephone. See

At the Branch Office:

No provisioning required.

At the NRS:

No provisioning required.

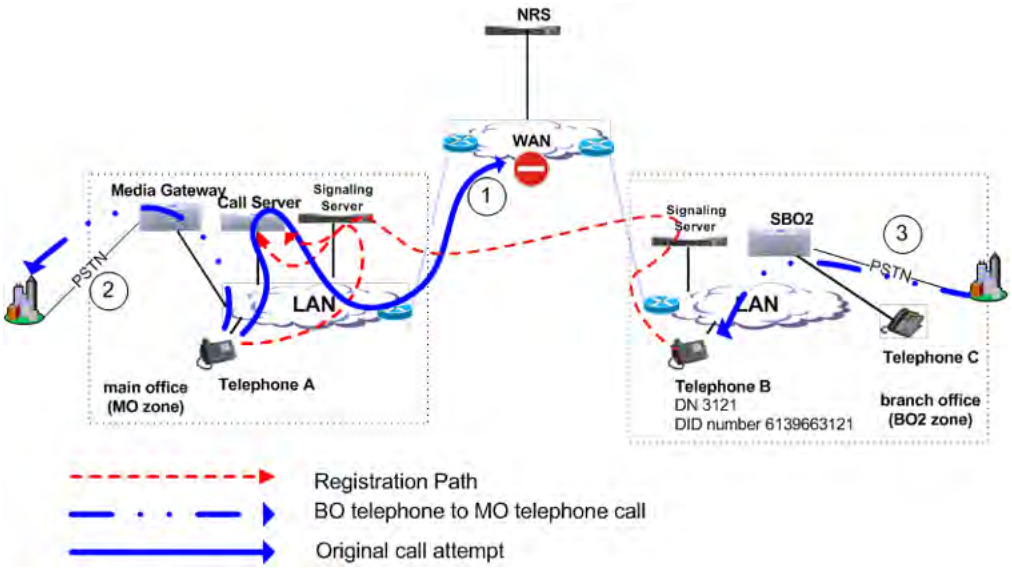


**Figure 68: Call from a main to a branch office telephone**

1. The user of Telephone A in the main office zone dials the user of Telephone B in the Branch Office zone (DN 3121). See action labeled 1 in the previous diagram.
2. The main office Call Server determines there is sufficient bandwidth between the two zones.
3. The Call Server inserts the ALTPrefix configured for the main office zone before the DN of Telephone B. For example, if the ALTPrefix assigned is 777, the dialed number becomes 7773121.
4. The call is routed by CDP or VNR to the outgoing route using an RLI. For example, 7773 is a steering code, translated to go to an RLI where there is one entry, a PSTN trunk route.
5. The main office manipulates the digit and the call is routed to the PSTN in the main office zone. See action labeled 2 in the previous diagram. For example, Use DMI to delete and insert digits on the PSTN trunk route.
    - delete three digits (remove the ALTPrefix 777)
    - insert 966 (to compose the DID number of the destination telephone which is 96663121, a local call.)
6. The call is routed through the PSTN and arrives at the Branch Office. The call is treated as an intrazone zone call and is carried through the PSTN trunk, terminating at IP Phone B in the BO2 zone See action labeled 3 in the previous diagram.

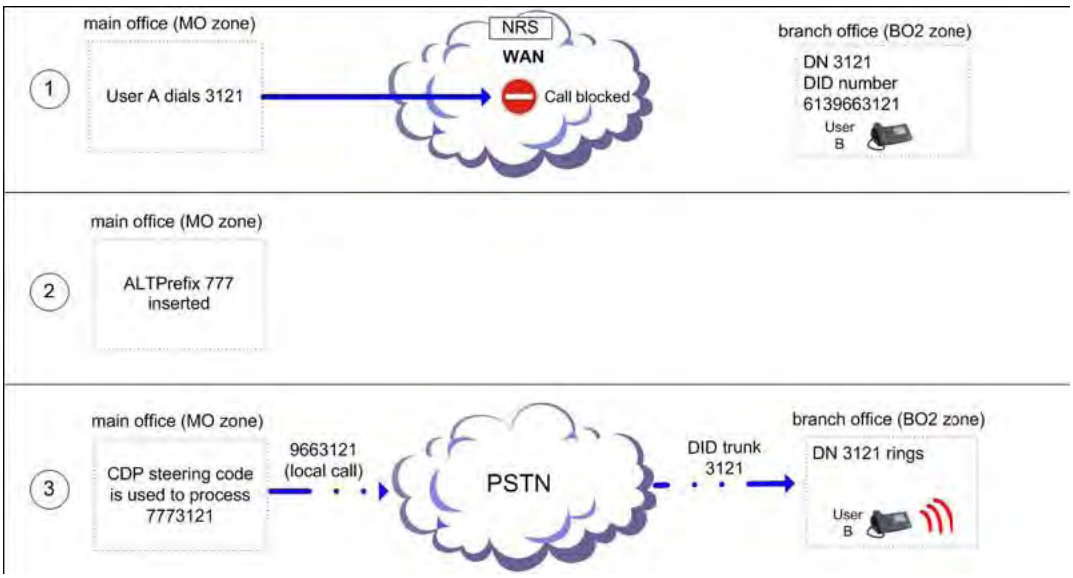


**Figure 69: Digits dialed and outpulsed between main and Branch Office**

1. User A in the MO zone dials User B in the BO2 zone.
2. The Call Servers inserts the ALTPrefix (777).
3. The call comes into User B from the PSTN in the BO2 zone.

## Call between two Branch Office telephones

The following examples present the steps that occur in ACR scenarios between two Branch Office telephones.

## Prerequisites for a call between two Branch Office telephone

At the main office:

- Use one of the dialing plan software packages to process the call, such as CDP or NARS.
- Provision an ALTPrefix for the BO2 zone.
- Provision the ALTPrefix as a Steering Code at the main Route List Index (RLI) so these calls go to the virtual trunk the Vacant Number Routing feature to do the same.

At the Branch Office:

Provision the ALTPrefix as a steering code. Build a Route List Index and DMI associated with this steering code that alternately routes these calls to the PSTN.

At the NRS:

Create a CDP entry for the ALTPrefix in the Branch Office gateway.

The following figure depicts an alternately routed call between two Branch Office telephone with three systems (a main office and two Branch Offices).

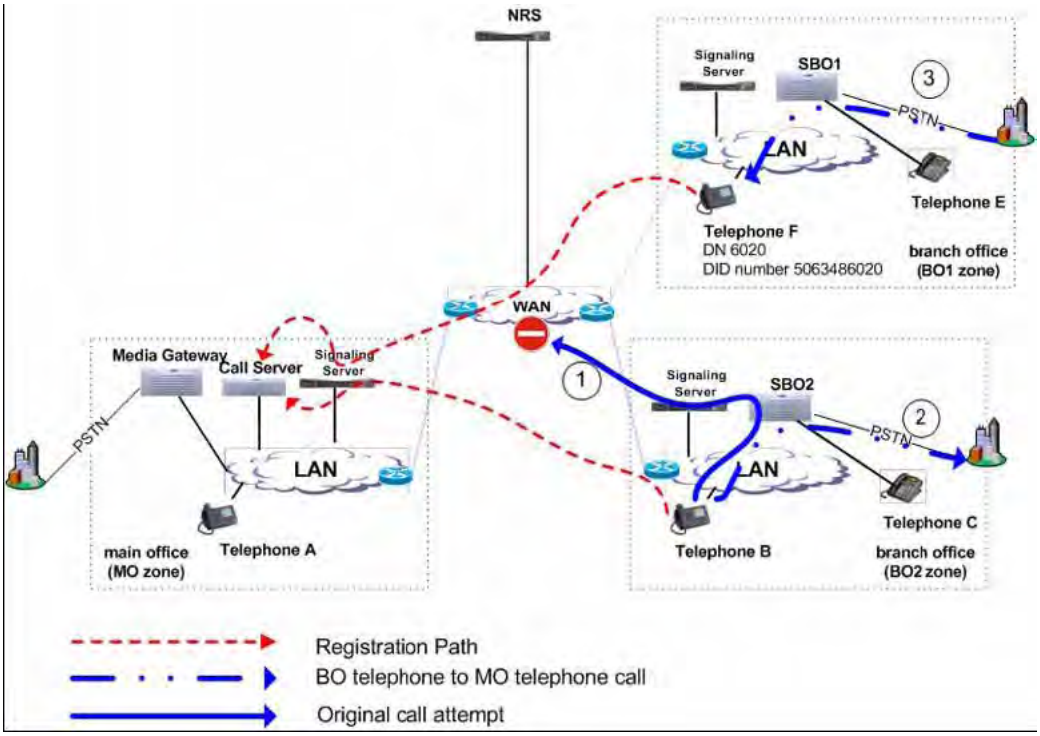


**Figure 70: Call between Branch Office telephones**

1. The user of Telephone B in the Branch Office 2 (BO2) zone dials user of Telephone F in the Branch Office 1 (BO1) zone (DN 6020). See action labeled 1 in the previous diagram.
2. The main office Call Server determines there is insufficient bandwidth between the BO2 and BO1 zones.
3. The Call Server inserts the ALTPrefix configured for the BO2 zone before the DN of Telephone F, dialed by the user. For example, if the ALTPrefix assigned is 222, the dialed number becomes 2226020.
4. The call is routed to the virtual trunk by CDP or VNR. The virtual trunk sends a request to the NRS for address resolution. The digit string sent to the NRS contains the ALTPrefix. The NRS returns the IP address of the Branch Office endpoint to the virtual trunk.
5. The virtual trunk places the call to the Branch Office.

   The Branch Office receives the call and recognizes the first part of the number as a Steering Code. The call is steered to an RLI. The DMI manipulates the number into a PSTN number and the Branch Office outpulses the digits to the Central Office (CO) serving the Branch Office. (This may be the same CO as the one serving the main office.) If the alternate route has MCDN trunks in the BO2 zone, the call is outpulsed on one of these trunks, after the Branch Office uses Digit Manipulation. See action labeled 2 in the previous diagram. For example, the digit string 2226 is

programmed as a Distant Steering Code (DSC) at the Branch Office. Calls starting with this DSC are handled by an RLI with PSTN trunks as an entry. If the Public format number for the destination telephone is a DID number, then the Digit Manipulation Index associated with the PSTN route must:

- delete 3 digits (remove the ALTPrefix 222)
- insert 1506348 (to compose the DID number of the destination telephone, which is 15063486020)

6. The call comes into Telephone F from the PSTN in the BO1 zone. See action labeled 3 in Figure 70: Call between Branch Office telephones on page 277.

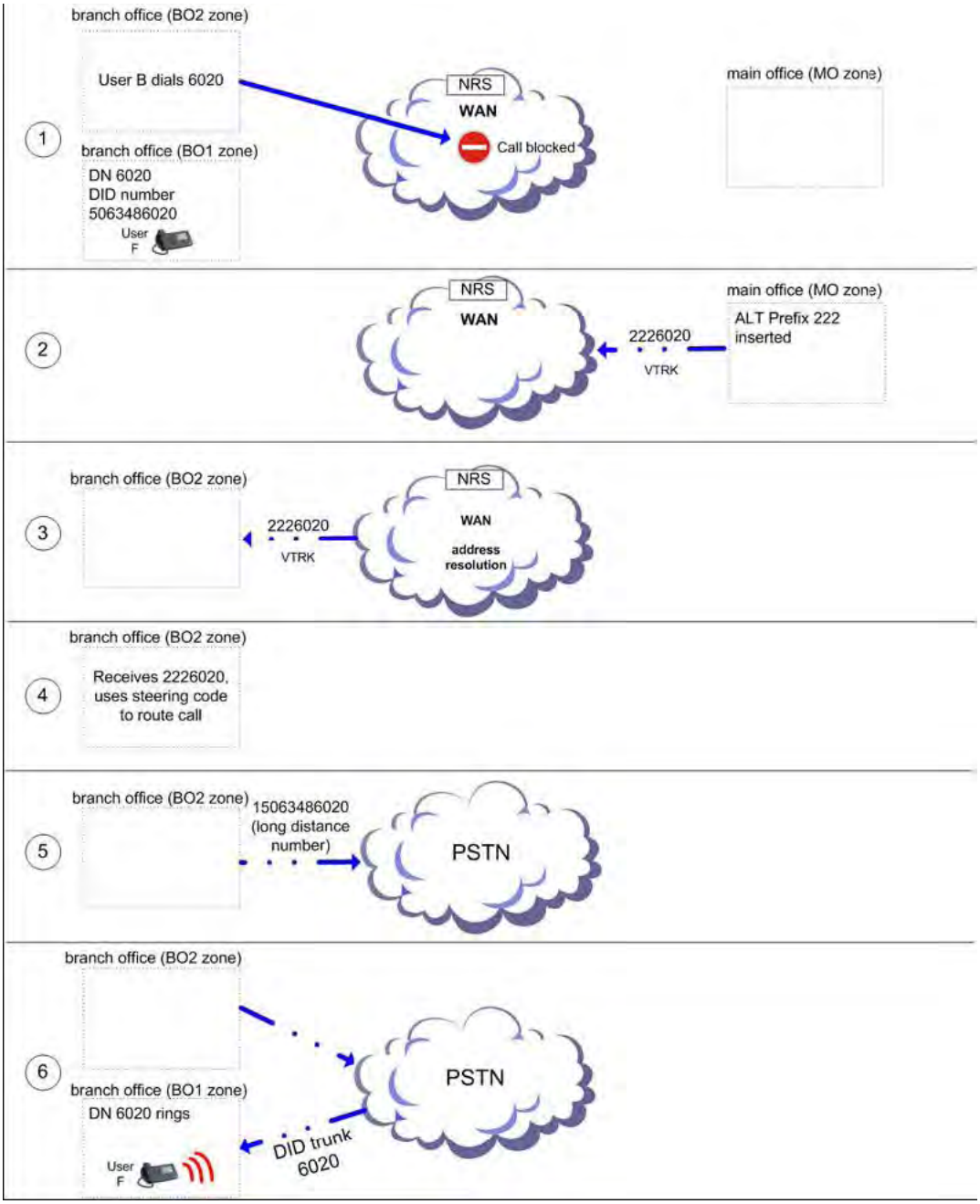


**Figure 71: Digits dialed and outpulsed between two Branch offices**

## Alternate Call Routing used in All Calls mode

The examples depicted in Figure 66: Call from a branch office telephone in normal mode to a main office telephone on page 271 and Figure 70: Call between Branch Office telephones on page 277 also applies to the operation of the All Calls mode feature when it is active all the time regardless of the available bandwidth.

The configuration and provisioning for the All Calls mode is exactly the same as the regular Alternate Call Routing (ACR) for the Network Bandwidth Management feature except that the Alternate Routing for All Calls option is selected in LD 117 or Element Manager.

# Feature implementation using Command Line Interface

Use LD 117 for Alternate Call Routing.

**Table 73: LD 117 – Enable Alternate Call Routing for a particular zone**

| Command | Description |
|---|---|
| ENL ZALT <zone> | Enable Alternate Call Routing for Network Bandwidth Management |
| <zone> | Input zone number (1-8000).<br>Configure the Branch Office zone using LD 117 at the main office. |

**Table 74: LD 117 – Configure Alternate Prefix number for a particular zone and the All Calls option**

| Command | Description |
|---|---|
| CHG ZALT <zone> <ALTPrefix> [<re-route all calls>] | Change ALTPrefix number for zone |
| <zone> | Input zone number (1-8000).<br>Configure the Branch Office zone using LD 117 at the main office. |
| <ALTPrefix> | A digit string, of up to 7 digits, added to the start of the dialed number, if the call will not be routed through the WAN (due to lack of bandwidth, poor QoS, or feature is configured for all calls). |
| [<re-route all calls>] | Allow or Deny Alternate Call Routing for all calls, where:<br>• (NO) = deny<br>• YES = allow |

**Table 75: LD 117 – Print Alternate Prefix number for a particular zone**

| Command | Description |
|---|---|
| PRT ZALT <zone> | Print the ALTPrefix assigned to a particular zone and if the feature operates for all calls from that zone. |
| <zone> | Input zone number (1-8000).<br>If you do not input a zone number, the system prints the information for all configured zones. |

**Table 76: Sample printout**

| # | ZALT | Alternate Prefix | All Calls | Alarms Suppression Time |
|---|---|---|---|---|
| 10 | ENL | 100 | YES | 50 |
| 11 | ENL | 101 | YES | 0 |
| 12 | DIS | 102 | NO | 1000 |

For information on Feature Implementation using Element Manager, see Alternate Routing for Calls between IP stations on page 288.

# Zone configuration

Use Element Manager to configure zone properties:

The following properties can be configured.

- Zone Basic Property and Bandwidth Management on page 281
- Adaptive Network Bandwidth Management and CAC on page 282
- Alternate Routing for Calls between IP stations on page 288
- Branch Office Dialing Plan and Access Codes on page 290
- Branch Office Time Difference and Daylight Saving Time Property on page 291
- Emergency Service Information on page 292

## Zone Basic Property and Bandwidth Management

Use Element Manager to configure the branch office specific Zone properties using the Zone configuration screen required at the branch office. It is an alternative to Zone configuration using LD 117. The following procedure uses Zone 0 as an example.

### Configuring branch office specific Zone properties

1. In the Element Manager navigation tree, click System, IP Network, Zones, Zone 0, Zone Basic Property and Bandwidth Management.

   The Zone Basic Property and Bandwidth Management window appears.

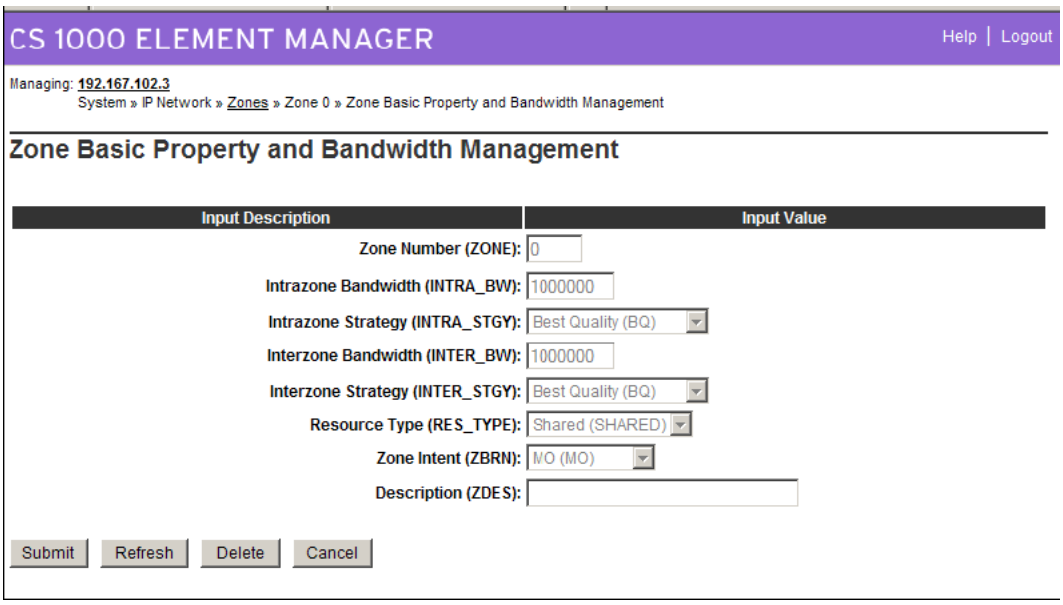


**Figure 72: Zone Basic Property and Bandwidth Management**

2. In the Input Value section, configure the following values:
   - Zone Number (ZONE): 1
   - Intrazone Bandwidth (INTRA_BW): 10000
   - Intrazone Strategy (INTRA_STGY): Best Quality (BQ)
   - Interzone Bandwidth (INTER_BW):10000
   - Interzone Strategy (INTER_STGY):Best Quality (BQ)
   - Resource Type (RES_TYPE):Shared (SHARED)
   - Zone Intent (ZBRN): MO (MO)
   - Description (ZDES):

   At the branch office, (ZBRN) for branch office support must be cleared. This parameter is only applicable to the corresponding zone at the main office.
3. Click Submit.

## Adaptive Network Bandwidth Management and CAC

For information on configuration rules and advanced configuration notes for Adaptive Network Bandwidth Management and CAC, see Adaptive Network Bandwidth Management configuration on page 253

## Configuring Adaptive Network Bandwidth Management and CAC

**⚠ Warning:**

Do not configure Adaptive Network Bandwidth Management for Zone 0 or Virtual Trunk zones.

1. In the Element Manager navigation pane, click System, IP Network, Zones, Zone 1, Adaptive Network Bandwidth Management and CAC.

   The Adaptive Network Bandwidth Management and CAC window appears.

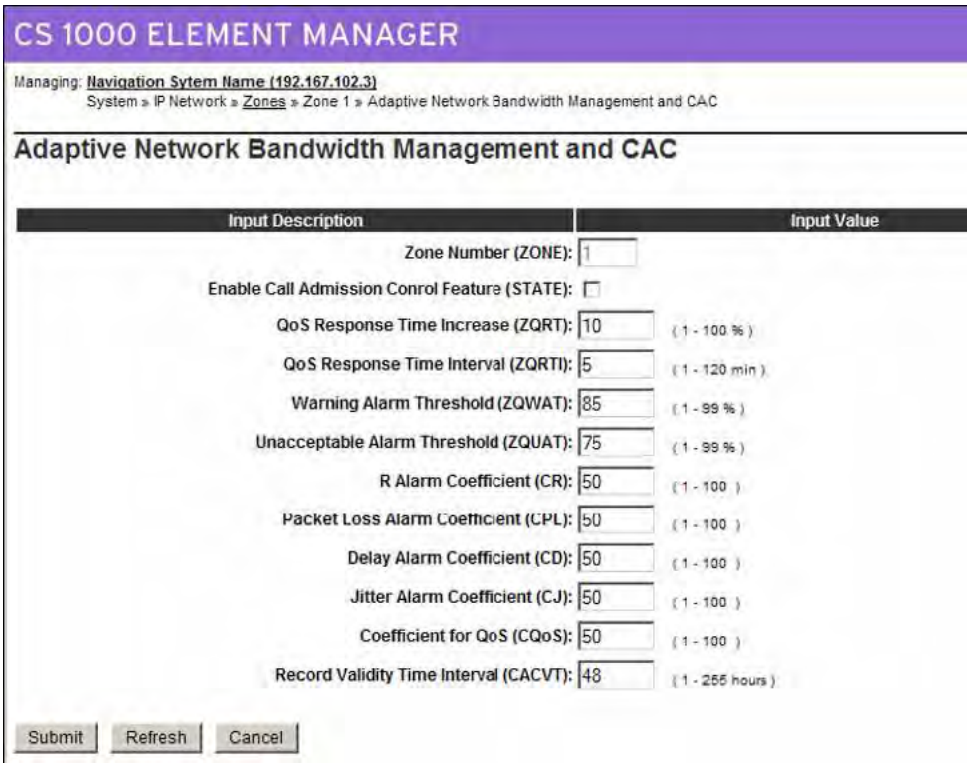


**Figure 73: Adaptive Network Bandwidth Management and CAC**

2. Enable the Call Admission Control Feature (STATE) by selecting the check box. The other parameters can be adjusted as required.
3. In the Input Value section, configure the following parameters:

   - QoS Response Time Increase (ZQRT)
   - QoS Response Time Interval (ZQRTI)
   - Warning Alarm Threshold (ZQWAT)
   - Unacceptable Alarm Threshold (ZQUAT)
   - R Alarm Coefficient (CR)
   - Packet Loss Alarm Coefficient (CPL)
   - Delay Alarm Coefficient (CD)

- Jitter Alarm Coefficient (CJ)
- Coefficient of QoS (CQoS)
- Recent Validity Time Interval (CACVT)

4. Tandem the outbound branch office calls by configuring the NRS.
5. Tandem the inbound branch office calls by creating a dialing plan which routes all calls destined for the branch office through the main office.
6. Click Submit.

The following table shows the fields in the Adaptive Network Bandwidth Management and CAC window, the field definitions, and the LD 117 command equivalent.

**Table 77: Adaptive Network Bandwidth Management and CAC fields**

| Field title | Field definition | LD 117 equivalent |
|---|---|---|
| Enable Call Admission Control Feature (STATE) | Control the CAC feature for the Zone<br>• Enable (select check box )<br>• disable (clear the check box) | ENL ZCAC DIS ZCAC |
| QoS Response Time Increase (ZQRT) | Bandwidth limit increment, as a percentage of the QoS factor for the Zone | CHG ZQRT |
| QoS Response Time Interval (ZQRTI) | Time (in minutes) between bandwidth limit increments | CHG ZQRTI |
| Warning Alarm Threshold (ZQWAT) | A QoS value, which is lower than this value, but higher than the Critical (Unacceptable) Alarm Threshold, triggers a Major Alarm. | CHG ZQWAT |
| Unacceptable Alarm Threshold (ZQUAT) | A QoS value, which is lower than this value, triggers an Unacceptable (Critical) Alarm. | CHG ZQUAT |
| R Alarm Coefficient (CR) | The R (CR) coefficient is used to calculate the QoS value for the Zone. | CHG CR |
| Packet Loss Alarm Coefficient (CPL) | The Packet Loss (Cpl) coefficient is used to calculate the QoS value for the Zone. | CHG CPL |
| Delay Alarm Coefficient (CD) | The Delay (CD) coefficient is used to calculate the QoS value for the Zone. | CHG CD |
| Jitter Alarm Coefficient (CJ) | The Jitter (CJ) coefficient is used to calculate the QoS value for the Zone. | CHG CJ |

| Field title | Field definition | LD 117 equivalent |
|---|---|---|
| Coefficient of QoS (CQoS) | The Coefficient of QoS (CQoS) is used to calculate the overall QoS value for the Zone. | CHG CQOS |
| Recent Validity Time Interval (CACVT) | Amount of time (in hours) for zone-to-zone record validity. After this interval expires, records for unused zones are purged from the tables. | CHG CACVT |

## Command line interface configuration

You can also configure the Adaptive Network Bandwidth Management feature using LD 117.

**Table 78: LD 117 – Configure Adaptive Network Bandwidth Management**

| Command | Description |
|---|---|
| CHG CACVT <Zone> <Interval> | Configure the zone-to-zone record validity time interval, where:<br>• Zone = 1-8000<br>• Interval = 1-(48)-255 |
| CHG CD <Zone> <Cd> | Change the Cd coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where:<br>• Zone = 1-8000<br>• Cd = Cd coefficient = 1-(50)-100 |
| CHG CPL <Zone> <Cpl> | Change the Cpl coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where:<br>• Zone = 1-8000<br>• Cpl = Cpl coefficient = 1-(50)-100 |
| CHG CJ <Zone> <Jitter> | Change the Cj coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where:<br>• Zone = 1-8000<br>• Jitter = Jitter coefficient = 1-(50)-100 |
| CHG CQOS <Zone> <QoS> | Change the QoS coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: |

| Command | Description |
|---|---|
| | • Zone = 1-8000<br>• QoS = QoS coefficient = 1-(50)-100 |
| CHG CR <Zone> <Cr> | Change the Cr coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where:<br>• Zone = 1-8000<br>• Cr = Cr coefficient = 1-(50)-100 |
| CHG ZONE <zoneNumber> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> [<zoneIntent> <zoneResourceType>] | Change the parameters of an existing zone, where:<br>• zoneNumber = 1-8000<br>• intraZoneBandwidth = 1000000 (Mbit/s)<br>• intraZoneStrategy = intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth)<br>• interZoneBandwidth = 100000 (Mbit/s)<br>• interZoneStrategy = intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth)<br>• zoneIntent = type of zone, where:<br>- MO = Main office zone<br>- BMG = Branch Media Gateway (branch office) zone<br>- VTRK = Virtual Trunk zone<br>• zoneResourceType = resource intrazone preferred strategy<br>- shared DSP channels (default) = shared<br>- private DSP channels = private |
| CHG ZQRT <Zone> <Incr> | Change ZQRT, which is Response time increase by percentage. It is used to determine the increase to the Sliding Maximum for the identified zone, where:<br>• Zone = 1-8000<br>• Incr = increase value in percentage = 1-(10)-100 |
| CHG ZQRTI <Zone> <Interval> | Change the QoS Response Time Interval while alarms are not coming, to increase the Sliding Maximum for the identified zone, where:<br>• Zone = 1-8000<br>• Interval = interval in minutes = 1-(5)-120 |
| CHG ZQUAT <Zone> <Thres> | Change the QoS Unacceptable Alarm Threshold value for the identified zone, where: |

| Command | Description |
|---|---|
| | • Zone = 1-8000<br>• Thres = threshold value = 1-(75)-99<br><br>**Important:**<br>When the zone-to-zone QoS value drops below the threshold value, the alarm is presented. This value must be below the value of ZQWAT. |
| CHG ZQWAT <Zone> <Thres> | Change the QoS Warning Alarm Threshold value for the identified zone, where:<br>• Zone = 1-8000<br>• Thres = threshold value = 1-(85)-99<br><br>**Important:**<br>When the zone-to-zone QoS value drops below the threshold value, the alarm is presented. The value for ZQWAT must be higher than the value of ZQUAT. |
| CHG ZQNL <Zonenumber> <level> | Change the Notification Level for the specified zone, where:<br>• Zone = 1-8000<br>• Level = 0-(2)-4, where:<br>- Level 0 = All voice quality alarms are suppressed.<br>- Level 1 = All zone based Unacceptable alarms.<br>- Level 2 = Allow all level 1 alarms PLUS zone based Warning alarms.<br>- Level 3 = Allow all level 1 and 2 alarms PLUS per call Unacceptable alarms.<br>- Level 4 = Allow all level 1, 2, and 3 alarms PLUS per call Warning alarms |
| NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResoureType>] | • zoneNumber = 1-8000<br>• intraZoneBandwidth = 1000000 (Mbit/s)<br>• intraZoneStrategy = BQ (Best Quality) or BB (Best Bandwidth)<br>• interZoneBandwidth = 1000000 (Mbit/s)<br>• interZoneStrategy = intrazone preferred strategy (BQ=Best Quality) or BB (Best Bandwidth)<br>• zoneIntent = type of zone, where:<br>- MO = Main office zone |

| Command | Description |
|---|---|
| | - BMG = Branch Media Gateway (branch office) zone<br>- VTRK = Virtual Trunk zone<br>• zoneResourceType = resource intrazone preferred strategy<br>- shared DSP channels (default) = shared<br>- private DSP channels = private |
| DIS ZCAC <Zone> | Disables the Call Admission Control (CAC) feature for the specified zone, where Zone = 1-8000.<br>**Important:**<br>Disables the feature on a zone-by-zone basis. |
| ENL ZCAC <Zone> | Enables the Call Admission Control (CAC) feature for the specified zone, where Zone = 1-8000.<br>**Important:**<br>Enables the feature on a zone-by-zone basis. |

# Alternate Routing for Calls between IP stations

Use the following procedures for configuring Alternate Routing for Calls between IP stations.

### Configuring Alternate Routing for Calls between IP stations

1. In the Element Manager navigation tree, click **System, IP Network, Zones**.

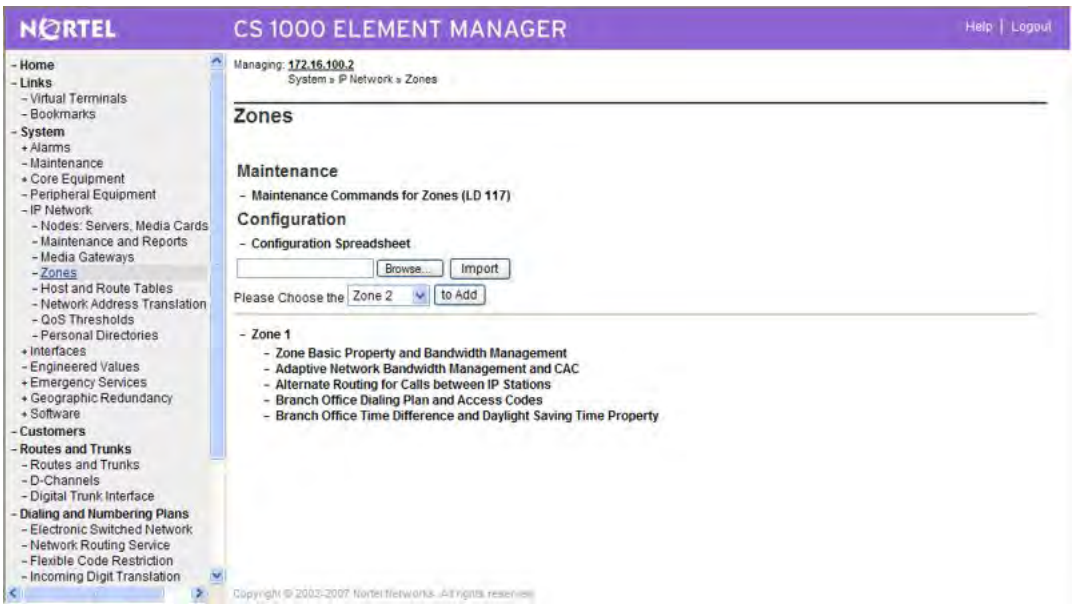


**Figure 74: Element Manager to access Zones**

The Zones window appears.

2. In the **Configuration** section, click the Zone you are programming and click the plus sign to expand the choices under it.
3. Click **Alternate Routing for Calls between IP Stations**.

   The Alternate Routing for Calls between IP Stations window appears and displays the configuration parameters for the Zone you selected in the previous step.

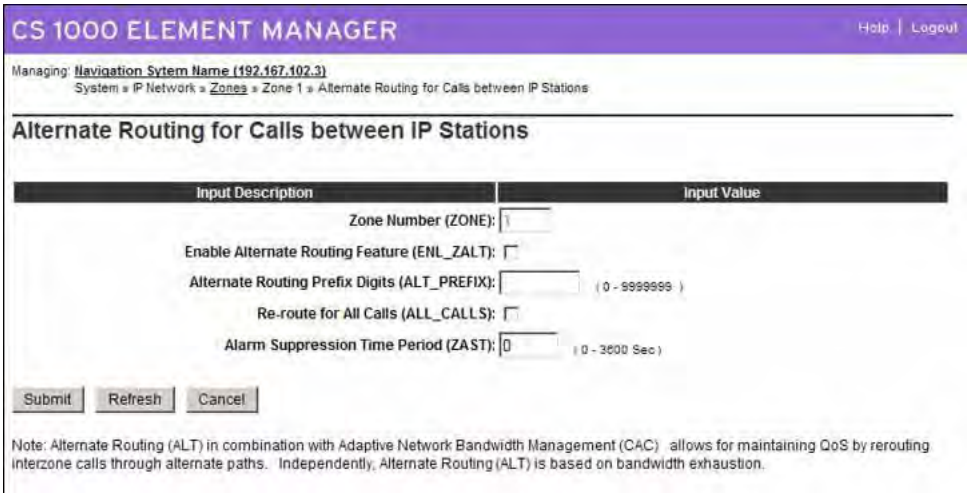


**Figure 75: Alternate Routing for Calls between IP Stations**

4. Select the **Enable Alternate Routing feature (ENL_ZALT)** check box to enable the Alternate Call Routing for Network Bandwidth Management feature.
5. In **Alternate Routing Prefix Digits (ALTPrefix)**, enter a maximum of 7 digits.

6. Select the **Re-route for All Calls (ALL_CALLS)** check box to enable the feature for all calls.
7. Click **Submit** to enter the data.

# Branch Office Dialing Plan and Access Codes

Use the following procedures for configuring Branch Office Dialing Plan and Access Codes.

## Configuring Branch Office Dialing Plan and Access Codes

1. In the Element Manager navigation tree, click **System, IP Network, Zones, Zone 0, Branch Office Dialing Plan and Access Codes**.

   The Zone Dialing Plan and Access Codes window appears.

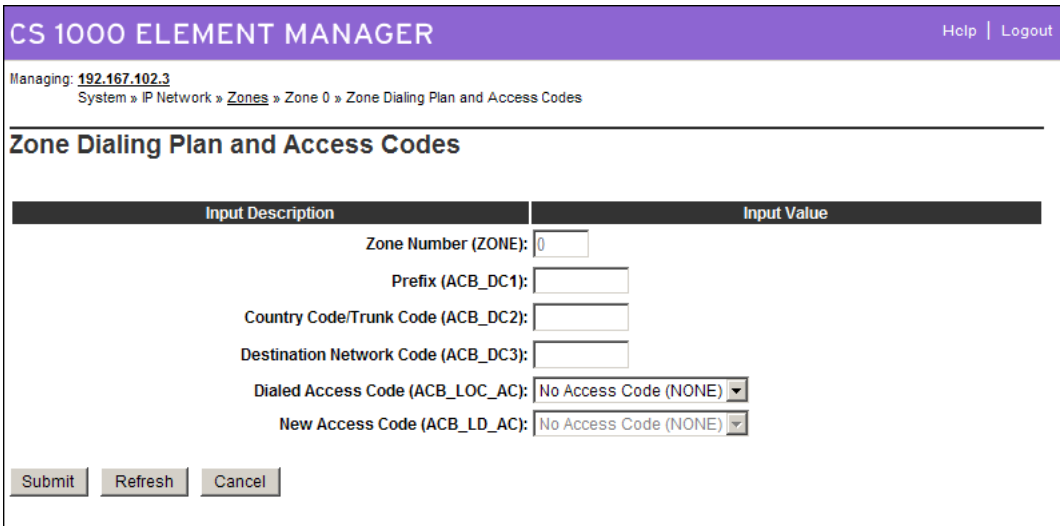


**Figure 76: Zone Dialing Plan and Access Codes**

2. In the **Input Value** section, the following values must be configured:
   - **Zone Number (ZONE)**
   - **Prefix (ACB_DC1)**
   - **Country Code/Trunk Code (ACB_DC2)**
   - **Destination Network Code (ACB_DC3)**
   - **Dialed Access Code (ACB_LOC_AC)**
   - **New Access Code (ACB_LD_AC)**
3. Click **Submit**.

# Branch Office Time Difference and Daylight Saving Time Property

Use the following procedures for configuring Branch Office Time Differences and Daylight Saving Time properties.

### Configuring Branch Office Time Difference and Daylight Saving Time properties

1. In the Element Manager navigation tree, click **System, IP Network, Zones, Zone 0, Branch Office Time Difference and Daylight Saving Time Property**.

   The Time Difference and Daylight Saving Time window appears.

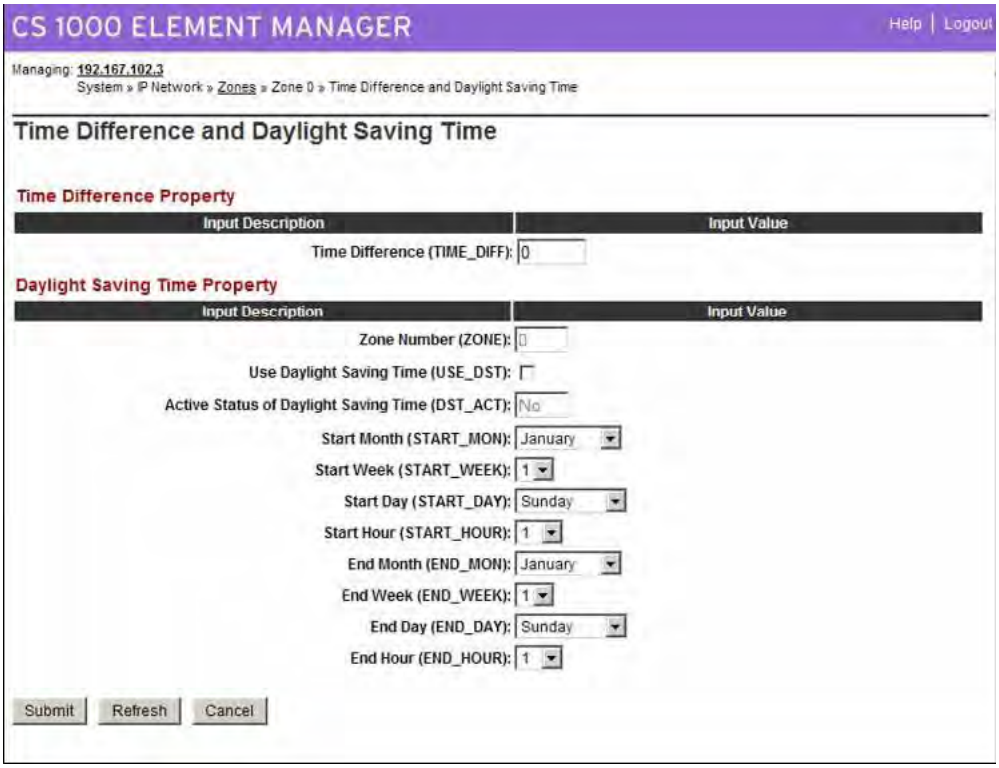


**Figure 77: Time Difference and Daylight Saving Time**

2. In the **Input Value** section, the following values must be configured:

   - **Zone Number (ZONE)**
   - **Use Daylight Saving Time (USE_DST)**
   - **Active Status of Daylight Saving Time (DST_ACT)**
   - **Start Month (START_MON)**
   - **Start Week (START_WEEK)**
   - **Start Day (START_DAY)**
   - **Start Hour (START_HOUR)**

- **End Month (END_MON)**
- **End Week (END_WEEK)**
- **End Day (END_DAY)**
- **End Hour (END_HOUR)**

3. Click **Submit**.

## Emergency Service Information

Use the following procedures for configuring Emergency Service Information.

### Configuring Emergency Service Information

1. In the navigation pane, click **IP Telephony, Zone 0, Zone Emergency Service Information**.

   The Zone Emergency Service Information window appears.

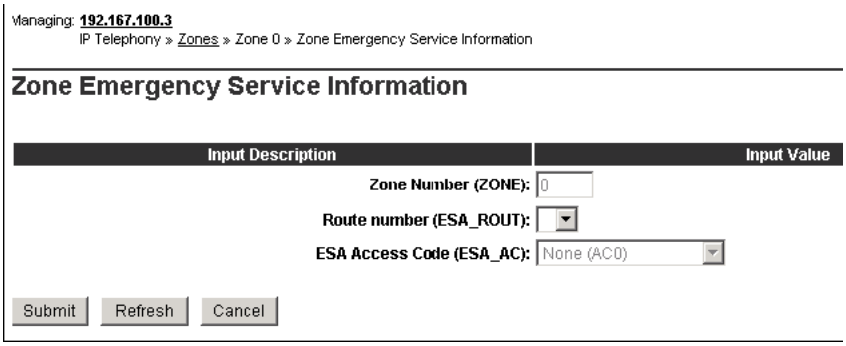


**Figure 78: Zone Emergency Service Information**

2. In the **Input Value** section, the following values must be configured:

   - **Zone Number (ZONE)**
   - **Route number (ESN_ROUT)**
   - **ESA Access Code (ESA_AC)**

3. Click **Submit**.

# The MG 1000B zone configuration

Zone parameters must be configured at both the main office Call Server and MG 1000B CP PM. The procedure for configuration on the MG 1000B CP PM is similar to an IP Peer Network configuration, with the additional Branch office specific configuration outlined in this section.

Zones are defined in LD 117 and applied to IP Phones in LD 11.

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

For more information about configuring MG 1000B at the main office, see *Branch Office Installation and Commissioning,* NN43001-314.

**⚠ Caution:**

Before and after an upgrade, perform a datadump (using LD 43 EDD or Element Manager) on the Server or Gateway Controller to back up the existing data.

## Configuring the MG 1000B zone for the Branch office

1. Configure the current date and time.

   See *Software Input Output Reference — Administration , NN43001-611*.

   **Table 79: LD 2 – Define system time and date**

| Command | Description |
|---|---|
| STAD dd mm yyyy hh mm ss | Configure the time and date: STAD DAY MONTH YEAR HOUR MINUTE SECOND<br>**Note:**<br>You must have a level 2 password to configure the time and date. |

2. Configure the Home Location Code (HLOC) and Virtual Private Network Identifier (VPNI).

   **Table 80: LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier.**

| Prompt | Response | Description |
|---|---|---|
| REQ | new/chg | Add new data or change existing data. |
| TYPE | NET | ISDN and ESN Networking options |
| | 0-99 | Range for Large System and Communication Server 1000E system |
| | 0-31 | Range for Small System and Media Gateway 1000B |
| ... | | |
| 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)-16383 | Virtual Private Network Identifier for Bandwidth Management Feature 0 or X |

| Prompt | Response | Description |
|---|---|---|
| | | = 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 is routed to the main office. VNR at the branch office and the NRS configuration identifies the main office as the endpoint for that user.

   VNR is routed through the Virtual Trunk and enables the NRS 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 is 0 (no digit manipulation required) on the Virtual Trunk route.

   **Table 81: LD 15 – Configure Vacant Number Routing.**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW CHG | Add new data, or change existing data |
| TYPE | NET | Configure networking |
| VNR | YES | Vacant Number Routing |
| - RLI | 0-1999 | 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 using LD 117 or Element Manager. 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.

   **Important:**

   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.

   **Warning:**

   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.

**Table 82: LD 117 – Define zone properties for branch office**

| Command | Description |
|---|---|
| NEW ZONE <xxxxx> <intraZoneBandwidth > <intraZoneStrategy> <interZoneBandwidth > <interZoneStrategy> <zoneResourceType> | Create a new zone with the following parameters:<br>• xxxxx = 1-8000 zone number<br>**⚠ Caution:**<br>Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.<br>• intraZoneBandwidth = Intrazone available bandwidth 0-1 000 000 kbit/s (see Note 1)<br>• intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality)<br>• interZoneBandwidth = Interzone available bandwidth 0-1 000 000 kbit/s (see Note 1)<br>• interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth)<br>• zoneResourceType = zone resource type (shared or private), where<br>- shared = Current default zone type. The IP Phones configured in shared zones use DSP resources configured in shared zones. If all of the shared zone 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 a channel from the same zone as the IP Phone is configured, and then any available channel from the shared zone channels<br>- private = New zone type introduced by IPL 3.0. DSP channels configured in a private zone are only used by IP Phones that have also been configured for that private zone. If more DSP resources are required by these IP Phones than what are available in the zone, DSPs from other zones are used. However, IP Phones configured in shared zones cannot use the private zones channels. The order of selection for the gateway channels is a channel from the same private zone as the IP Phone is configured, and then any available channel from the pool of shared zones channels |
| For more information about Private/Shared Zone configuration, see*Signaling Server IP Line Applications Fundamentals, NN43001-125* . | |

| Command | Description |
|---|---|
| Note 1: If the Network Bandwidth Management feature is going to be used, parameters intraZoneBandwidth and interZoneBandwidth must be configured to the maximum configurable value. See Bandwidth Management on page 73. | |

5. Configure the parameters for IP Phone passwords and modifications.

   For more information about IP Phone installers password, see *Branch Office Installation and Commissioning, NN43001-314*.

## Configuring ESN, MG 1000B or SRG zones

**⚠ Warning:**

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

1. Configure the Home Location Code (HLOC), and the Virtual Private Network Identifier (VPNI).

   **Table 83: LD 15 – Configure Customer Data Home Location Code and Virtual Private Network Identifier.**

| Prompt | Response | Description |
|---|---|---|
| REQ | chg | Change existing data. |
| TYPE | NET | ISDN and ESN Networking options |
| CUST | | Customer number |
| | 0-99 | Range for Large System and Communication Server 1000E system |
| | 0-31 | Range for Small System and Media Gateway 1000B |
| ... | — | — |
| 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)-16383 | 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.

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.

**Table 84: LD 117 – Define zone properties for branch office**

| Command | Description |
|---|---|
| NEW ZONE <xxxxx> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneResourceType> | Create a new zone with the following parameters:<br>• xxxxx = 0-8000 zone number<br>• intraZoneBandwidth = Intrazone available bandwidth 0-1 000 000 kbit/s See Note 1.<br>• intraZoneStrategy = Intrazone preferred strategy (BQ for Best Quality or BB for Best Bandwidth)<br>• interZoneBandwidth = Interzone available bandwidth 0-1 000 000 kbit/s See Note 1.<br>• interZoneStrategy = Interzone preferred strategy (BQ for Best Quality or BB for Best Bandwidth)<br>• zoneResourceType = zone resource type (shared or private), where<br>- shared = Current default zone type. The IP Phones 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 a channel from the same zone as the IP Phone is configured, and then any available channel from the shared zone channels<br>- private = New zone type introduced by IPL 3.0. DSP channels configured in a private zone are only used by IP Phones which have also been configured for that private zone. If more DSP resources are required by these IP Phones than what are available in the zone, DSPs from other zones are used. However, IP Phones configured in shared zones cannot use the private zone channels. The order of selection for the gateway channels is a channel from the same private zone as the IP Phone is configured, and then any available channel from the pool of shared zone channels<br>For more information about Private/Shared Zone configuration, see*Signaling Server IP Line Applications Fundamentals, NN43001-125* |

| Command | Description |
|---|---|
| Note 1: If the Network Bandwidth Management feature is going to be used, parameters intraZoneBandwidth and interZoneBandwidth must be configured to the maximum configurable value. See Bandwidth Management on page 73. | |

**⚠ Warning:**

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.

3. Define the zone parameters at the branch office. Use LD 117 or Element Manager.

**Table 85: 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 the 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.

**Table 86: LD 117—Enable features for MG 1000B zone.**

| Command | Description |
|---|---|
| ENL ZBR <Zone> ALL | Enables features for the branch office <zone>. |

# Abbreviated dialing

Abbreviated Dialing must be configured at the main office and at the branch office.

The main office and branch office must have the same configuration. The DNs, zones, and Pretranslation Groups must be exactly the same in both offices.

Use the following procedures to configure Abbreviated dialing:

- Configuring the Speed Call List on page 299
- Configuring Pretranslation Groups on page 300
- Assigning Pretranslation Groups to the telephones on page 301
- Configuring Incoming DID Digit Conversion (IDC) on page 301

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.

## Configuring the Speed Call List

1. In LD 18, configure the Speed Call List (SCL) for each main office zone.

**Table 87: LD 18—Configure Speed Call Lists (SCL) for each zone**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data |
| TYPE | SCL | Speed Call List |
| LSNO | 4-(16)-31 | Maximum number of DNs allowed for Speed Call Lists |
| DNSZ | 0-(256)-2000 | Maximum number of DNs in Speed Call List |
| WRT | (YES) NO | Data is correct and can be updated in the data store |
| STOR | 0-1999 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 to configure the SCL for each branch office zone.
3. In LD 18, configure the default SCL.

**Table 88: LD 18—Configure default Speed Call List**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data |
| TYPE | SCL | Speed Call List |
| LSNO | 0 | Default SCL |
| DNSZ | 4-(16)-31 | Maximum number of DNs allowed for Speed Call Lists |
| SIZE | 0-(256)-1000 | Maximum number of DNs in Speed Call List |

| Prompt | Response | Description |
|---|---|---|
| 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. |
| | | **Note:**<br>The STOR and WRT prompts are repeated in sequence for each number in the SCL. |

## Configuring Pretranslation Groups

1. In LD 18, configure the Pretranslation Group for each main office zone.

   **Important:**

   While not required, Nortel recommends that the Pretranslation Group number (XLAT) be the same as the number of the zone to which it is assigned.

   **Table 89: LD 18—Configure Pretranslation Group for each zone**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| TYPE | PRE | Pretranslation Group |
| XLAT | 1-8191 | Group number. Correlates Pretranslation Group to Speed Call List. |
| - PRE | 1-8190 | Pretranslation Speed Call List Number. Corresponds to LSNO defined in LD 18, TYPE=SCL |

2. Repeat previous step to configure the Pretranslation Group for each branch office zone.
3. In LD 18, configure the default Pretranslation Group at the main office.

   **Table 90: LD 18—Configure default Pretranslation Group**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| 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.

**Table 91: LD 15—Activate Pretranslation feature**

| Prompt | Response | Description |
|---|---|---|
| REQ | CHG | Change existing data |
| TYPE | FTR | Features and options |
| ... | | |
| PREO | 1 | Activate Pretranslation feature |
| ... | | |

## Assigning Pretranslation Groups to the telephones

1. In LD 11, assign the Pretranslation Group to IP Phones and TDM telephones.

   **Important:**
   The Pretranslation Group must be assigned to all IP Phones and TDM telephones. This procedure describes how to configure a single telephone, and it must be repeated for each telephone in the group.

   **Table 92: LD 11—Pretranslation Group to telephones**

| Prompt | Response | Description |
|---|---|---|
| REQ | CHG | Change existing data. |
| TYPE | a...a | Terminal type. |
| | | Type question mark (?) for a list of possible responses. |
| ... | | |
| XLST | (0)-254 | Pretranslation Group associated with the group. |
| ... | | |

2. Repeat previous step for each telephone in the group.

## Configuring Incoming DID Digit Conversion (IDC)

1. In LD 15, configure Flexible Code Restriction for IDC.

   **Table 93: LD 15—Flexible Code Restriction for Incoming DID Digit Conversion**

| Prompt | Response | Description |
|---|---|---|
| REQ | FCR | Flexible Code Restriction |
| ... | | |
| NFCR | YES | Enable new Flexible Code Restriction. |
| ... | | |
| IDCA | YES | Incoming DID Digit Conversion allowed. |

| Prompt | Response | Description |
|---|---|---|
| - DCMX | 1-255 | Maximum number of IDC conversion tables. |
| ... | | |

2. In LD 49, configure IDC.

**Table 94: LD 49—Incoming DID Digit Conversion (IDC)**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add new data. |
| TYPE | IDC | Incoming Digit Conversion |
| DCNO | 0-254 | Digit Conversion tree number (IDC tree number). |
| ... | | |
| IDGT<br><0-9999> | 0-9999<br>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:<br>Prompt: Response IDGT: 3440 3440: 510 |

3. In LD 49, configure Flexible Code Restriction to allow all codes.

**Table 95: LD 49—Flexible Code Restriction**

| Prompt | Response | Description |
|---|---|---|
| REQ | new | Add new data. |
| 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.

**Table 96: LD 16—Route Data Block**

| Prompt | Response | Description |
|---|---|---|
| REQ | chg | Change existing data |
| 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 |

| Prompt | Response | Description |
|---|---|---|
| ... | | |

## Print branch office zone information

LD 117 contains commands to view branch office zones at the main office Call Server.

**Table 97: Print zone information**

| Command | Description |
|---|---|
| PRT INTERZONE | Print interzone statistics for the range between the near and far zones. |
| PRT INTRAZONE | Print intrazone statistics for all zones or for the specified zone. |
| 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 <0-8000> | Print zone information for a specific zone. |
| PRT ZPAGE [<zone number> <zonesPerPage>] | Print zone information for <zonesPerPage> zones starting at <zoneNumber> 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.

**Table 98: 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. |

**Caution:**

When a zone is created, its default state is enabled.

Zone 0 must be configured in LD 117 first before other zones are configured or all calls associated with Zone 0 are blocked.

## View status of branch office zone at main office Call Server

LD 117 contains commands to review the status of the main office Call Server.

**Table 99: LD 117—Display zone status**

| Command | Description |
|---|---|
| STAT ZONE [<Zone>] | Display zone status table |
| STAT ZBR [<Zone>] | Display status of branch office zones. |

## Change/print Proactive Voice Quality notification levels

The Proactive Voice Quality (PVQ) notification level can be changed on a zone-by-zone basis so that a particular zone, such as a branch office zone, is monitored more closely than others. LD 117 contains commands for changing and viewing the notification level for a zone.

**Important:**

The notification level for a branch office zone must be configured the same at both the main office and the branch office.

**Table 100: LD 117—Change/print PVQ notification levels**

| Command | Description |
|---|---|
| CHG ZQNL ALL <Level> | Change the notification level for all zones. |
| CHG ZQNL <Zone> <Level | Change the notification level for the specified zone. |

| Command | Description |
|---|---|
| PRT ZQNL ALL | Print a table of the notification level for all zones. |
| PRT ZQNL <Zone> | Print a table of the notification level for the specified zone. |

# Print PVQ statistics

LD 117 contains a command to print PVQ statistics for the branch office zone.

**Table 101: LD 117—PVQ statistics**

| Command | Description |
|---|---|
| PRT ZQOS <zone> | Print the PVQ statistics for the branch office zone. |

# Diagnostics

Use the following tables to obtain the status of a particular zone.

## Command line interface diagnostics

LD 117 contains commands to obtain the status of a particular zone.

**Table 102: LD 117—Obtain status for a particular zone**

| Command | Description |
|---|---|
| STAT ZALT <zone> | Display Alternate Call Routing Status, where: zone=bandwidth zone |
| If you do not enter a value in the zone field, the status of all configured zones is displayed. | |

The screen output for all configured zones appears as follows:

| # | Alternate Routing Status |
|---|---|
| 10 | ENL |
| 11 | DIS |
| 12 | DIS |

**Table 103: LD 117—Obtain status for a branch office zone**

| Command | Description |
|---|---|
| STAT ZBR <zone> | Display the status of specified branch office zone, where: zone=bandwidth zone |
| If you do not enter a value in the zone field, the status of all configured zones is displayed. | |

**Table 104: Sample output for all branch office zones**

| # | State | Flags | Des |
|---|---|---|---|
| 10 | ENL | TIM | BVW |
| 11 | DIS | LOC ALT | TOR |
| 12 | DIS | ESA ALT | |
| "Des" entries are codes you assign to each branch office for your own records. | | | |

# Element Manager diagnostics

## Print zone Alternate Call Routing information

The print capability allows the following parameters to be viewed for each zone:

- enable/disable status of the Alternate Call Routing for Network Bandwidth Management feature
- ALTPrefix digits
- enable/disable the status of the All Calls option

## Printing zone ALTPrefix

1. In the navigation tree, click **System, Maintenance**.

   The Maintenance window appears.

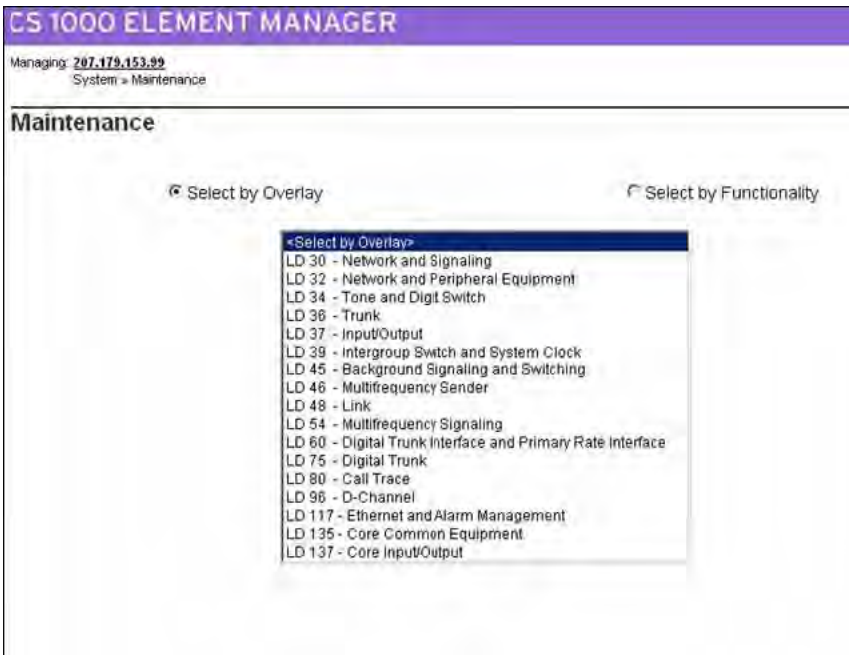


**Figure 79: System Maintenance**

2. Select the **Select by Functionality** option button.

   The Select by Functionality window appears.

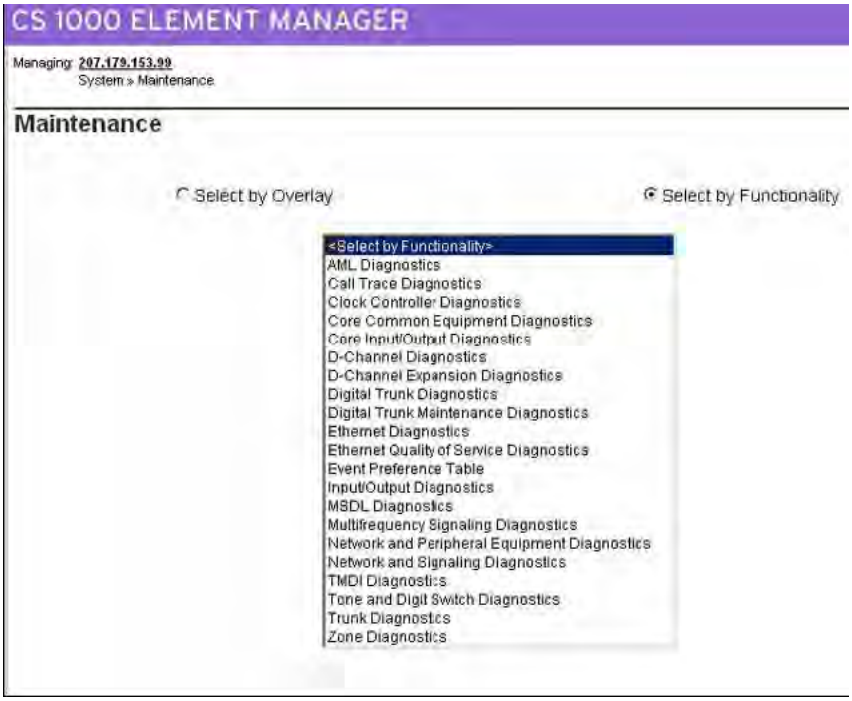


**Figure 80: Select by Functionality**

3. Click **Zone diagnostics**.

The Maintenance Commands for Zones window appears.

You can also access this page from **IP Network, Zones** and click on **Maintenance Commands for Zones (LD 117)**.

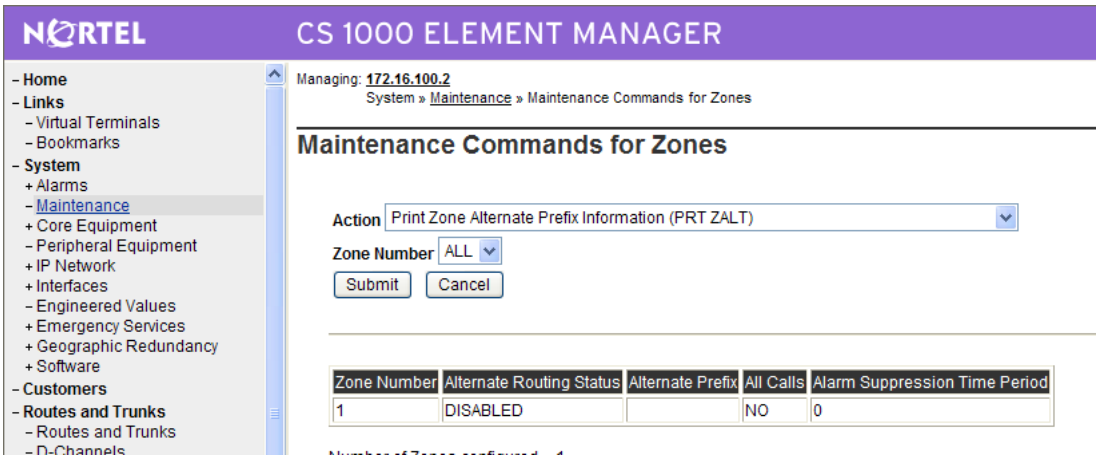


**Figure 81: Maintenance Commands for Zones**

4. In the **Action** list, select **Print Zone Alternate Prefix Information (PRT ZALT)**.

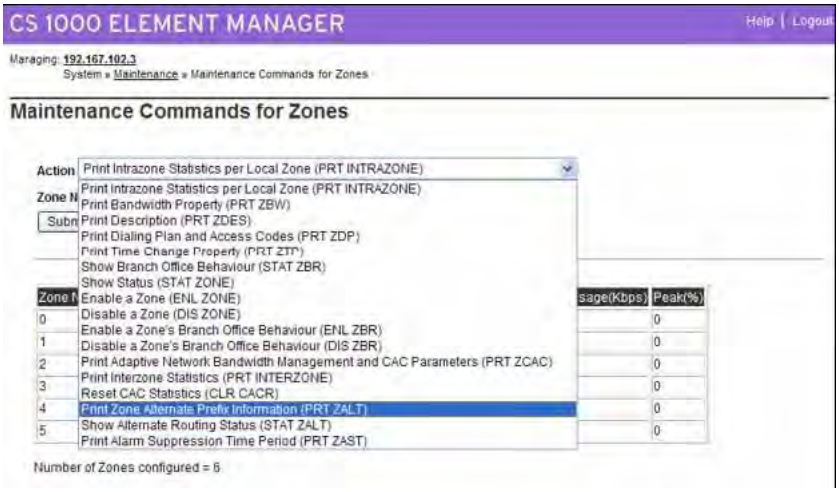


**Figure 82: Maintenance Commands for Zones Action list**

5. In the **Zone Number** list, select **ALL** or a specific zone number.
6. Click **Submit**.

   The Maintenance Commands for Zones window appears, that displays the statistics for the specified zone or zones. A blank field indicates that the statistic is either not available or not applicable to that zone.

## Show status of Alternate Call Routing

The Show Status functionality displays the enable/disable status of Alternate Call Routing for the Network Bandwidth Management feature. The configured zones and the status of the feature for each zone can be listed.

### Showing the status of Alternate Call Routing

1. In the navigation tree, click **System, Maintenance**.

   The Maintenance window appears. See Figure 79: System Maintenance on page 307.

2. Click **Select by Functionality**.

   The Select by Functionality window appears. See Figure 80: Select by Functionality on page 307.

3. Click **Zone diagnostics**.

   The Maintenance Commands for Zones window appears. See Figure 83: Show Alternate Routing Status (STAT ZALT) on page 309.

4. From the **Actions** list, select **Show Alternate Routing Status (STAT ZALT)**.

   See Figure 83: Show Alternate Routing Status (STAT ZALT) on page 309.

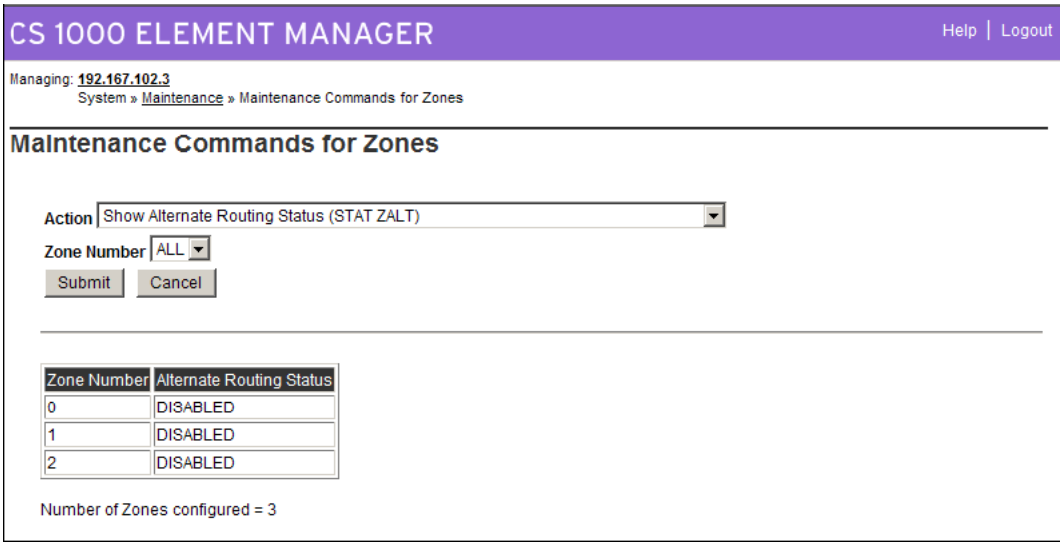


**Figure 83: Show Alternate Routing Status (STAT ZALT)**

5. In the **Zone Number** list, select **ALL**.
6. Click **Submit** to enter the data.

   The window updates with the data associated with that zone. See Figure 83: Show Alternate Routing Status (STAT ZALT) on page 309 for a typical example of the results.

## Maintenance

The features in this section can be maintained using Element Manager or LD 117.

## Adaptive Network Bandwidth Management for CAC

The CAC parameters, intrazone, and interzone statistics for one of more zones are available in Element Manager from the Zones window.

### Maintenance using Element Manager — Displaying CAC parameters for one or more zones

1. In Element Manager navigation tree, select **System, IP Network, Zones**.

   The Zones window appears.

2. Click **Maintenance Commands for Zones (LD 117)**.

   The Maintenance Commands for Zones pane appears and lists all the configured zones and the intrazone statistics by default.

3. In the **Action** list, select **Print Adaptive Network Bandwidth Management and CAC Parameters (PRT ZCAC)**.

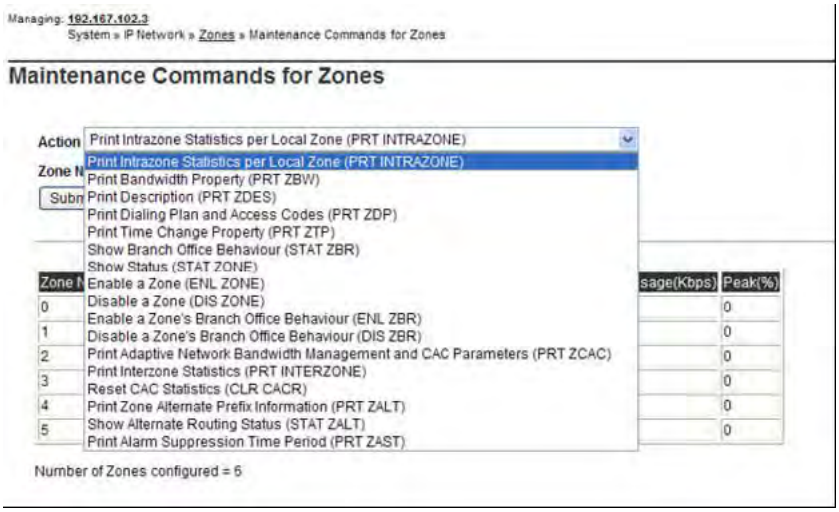


**Figure 84: Zone action list**

4. In the **Zone Number** list, select **ALL** or a specific zone number to display statistics for a specific zone.
5. Click **Submit**.

   The Maintenance Commands for Zones window appears, which displays the statistics for the specified zone or zones. A blank field indicates that the statistic is not available or not applicable to that zone.

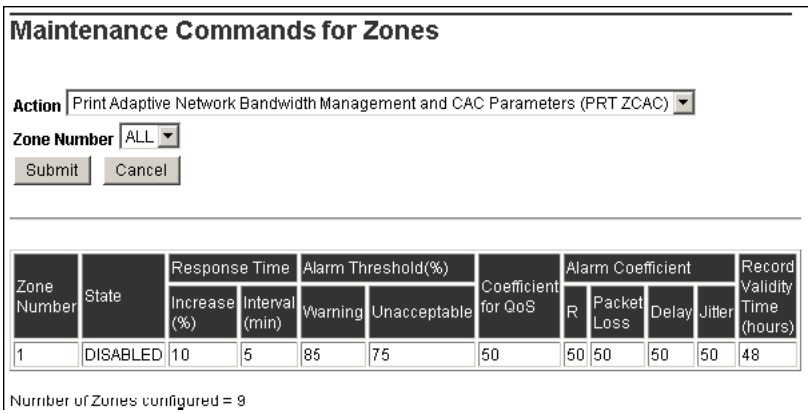


**Figure 85: Element Manager CAC parameters**

## Command line interface maintenance

### Table 105: LD 117—Display Adaptive Network Bandwidth Management information

| Command | Description |
|---|---|
| CLR CACR <Near Zone> <Near VPNI> <Far Zone> <Far VPNI> | Clear zone-to-zone record for near (VPNI-Zone) or far (VPNI-Zone) zones, where:<br>• Near Zone = 1–8000<br>• Near VPNI = 1–16383<br>• Far Zone = 1–8000<br>• Far VPNI = 1–16383 |
| PRT INTRAZONE <zone> | Print intrazone statistics for the identified zones, where zone = ALL or 1–8000 The output of this command displays the following information:<br>• Zone<br>• State = ENL/DIS<br>• Type = PRIVATE/SHARED<br>• Strategy = BB/BQ<br>• MO/BMG/VTRK = ZoneIntent<br>• Bandwidth = kbit/s<br>• Usage = kbit/s<br>• Peak = % |
| PRT INTERZONE <near Zone> <nearVPNI> <farZone> <farVPNI> | Print interzone statistics for the specific VPNI zone; where:<br>• nearZone = ALL or 1–8000<br>• nearVPNI = 1–16383<br>• farZone = 1–8000<br>• farVPNI = 1–16383 |

| Command | Description |
|---|---|
| | The output of this command displays the following information:<br>• Near end Zone<br>• Near end VPNI<br>• Far end Zone<br>• Far end VPNI<br>• State = ENL/DIS<br>• Type = PRIVATE/SHARED<br>• Strategy = BB/BQ<br>• MO/BMG/VTRK = Zone Intent<br>• QoS factor = %<br>• Bandwidth configured = Kbps<br>• Sliding max = Kbps<br>• Usage = Kbps<br>• Peak = %<br>• Call = Cph<br>• Alarm = Aph<br>The report rows are grouped as:<br>• First row = summary bandwidth usage per near zone<br>• Next rows = bandwidth usage for near (VPNI–Zone) and far (VPNI–Zone) zones |
| PRT ZCAC <zone> | Print CAC parameters for the specified zone, or for all zones, where zone = ALL or 1–8000<br>The output of this command displays the following information:<br>• Local ZONE = 1–8000<br>• State = ENL/DIS<br>• CR = 1–100<br>• CPL = 1–100<br>• CD = 1–100<br>• CJ = 1–100<br>• CQOS = 1–100<br>• ZQRT = 1–100<br>• ZQRTI = 10–120<br>• ZQUAT = 1–99 |

| Command | Description |
|---|---|
| | • ZQWAT =1–99<br>• CACVT = 1–255 |

To view sample output for PRT commands, see Figure 22: Sample output for prt intrazone command on page 88 and Figure 23: Sample output for prt interzone command on page 88.

# Alternate Call Routing for Network Bandwidth Management

## Command Line Interface (CLI) maintenance

### Table 106: LD 117—Enable and disable Alternate Call Routing for a zone

| Command | Description |
|---|---|
| ENL ZALT <zone> | Enable Alternate Call Routing (ACR) for Bandwidth Management for the zone specified, where: Input zone number (1–8000). Configure the branch office zone using LD 117 at the main office. |
| DIS ZALT <zone> | Disable ACR for Bandwidth Management for the zone specified. |
| ENL ZBR <zone> [ALL] [LOC][ESA][TIM] [ALT] | Enable features for the branch office zone. If you do not input features, then all are enabled. |
| DIS ZBR [ALL] [LOC][ESA][TIM][ALT] | Disable features for the branch office zone. If you do not input features, then all are disabled. |
| The system responds with ok , if operation is successful. | |

### Table 107: LD 117—Configure Alternate Prefix number for a particular zone and the All Calls option

| Command | Description |
|---|---|
| CHG ZALT <zone> <ALTPrefix> [<reroute all calls>] | Change ALTPrefix number for zone. |
| <zone> | Input zone number 1–8000 Configure the branch office zone using LD 117 at the main office. |
| <ALTPrefix> | A digit string, of up to 7 digits, added to the start of the dialed number, if the call will not be routed through the WAN (due to lack of |

| Command | Description |
|---|---|
| | bandwidth, poor QoS, or feature is configured for all calls). |
| [<rereoute all calls>] | Allow or Deny ACR for all calls, where:<br>• (NO) = deny<br>• YES = allow |

**Table 108: LD 117—Print Alternate Prefix number for a particular zone**

| Command | Description |
|---|---|
| PRT ZALT <zone> | Print the ALTPrefix assigned to a particular zone and if the feature operates for all calls from that zone, where: |
| <zone> | Input zone number 1–8000 If you do not input a zone number, the system prints the information for all configured zones. |

**Table 109: Sample Print Alternate Prefix number output**

| # | ZALT | Alternate Prefix | All Calls | Alarms Suppression Time |
|---|---|---|---|---|
| 10 | ENL | 100 | YES | 50 |
| 11 | ENL | 101 | YES | 0 |
| 12 | DIS | 102 | NO | 1000 |

**Table 110: LD 117—Change and Print Zone Alarm Suppression Time Interval**

| Command | Description |
|---|---|
| CHG ZAST <zone> <Alarm Suppression Interval> | Change Suppression Time Interval for QoS alarms related to ACR for Network Bandwidth Management feature for zone specified. Time Interval is measured in seconds from the time the last alarm was printed. Default is 0. Range is 0–3600 seconds. |
| PRT ZAST <zone> | Print Suppression Time Interval for QoS alarms related to ACR for the Network Bandwidth Management feature for zone specified. No entry for zone number results in printout for all zones. |

**Table 111: Sample Change and Print Zone Alarm Suppression Time Interval output**

| # | Alarms Suppression Time |
|---|---|
| 10 | 50 |
| 11 | 0 |
| 12 | 1000 |
| Where # is the column header for zone number. | |

# Element Manager maintenance

## Enable zone Branch Office behavior

You can configure the Alternate Call Routing (ACR) for the Network Bandwidth Management feature while you configure the zone Branch Office behavior.

## Enabling a zone Branch Office behavior

1. In the Element Manager navigation tree, select **System, Maintenance**.

   The Maintenance pane appears. See Figure 79: System Maintenance on page 307.

2. Click **Select by Functionality**.

   The Select by Functionality window appears. See Figure 80: Select by Functionality on page 307.

3. Click **Zone diagnostics**.

   The Maintenance Commands for Zones window appears.

4. From the **Action** list, select **Enable a Zone's Branch Office Behavior (ENL ZBR)**.

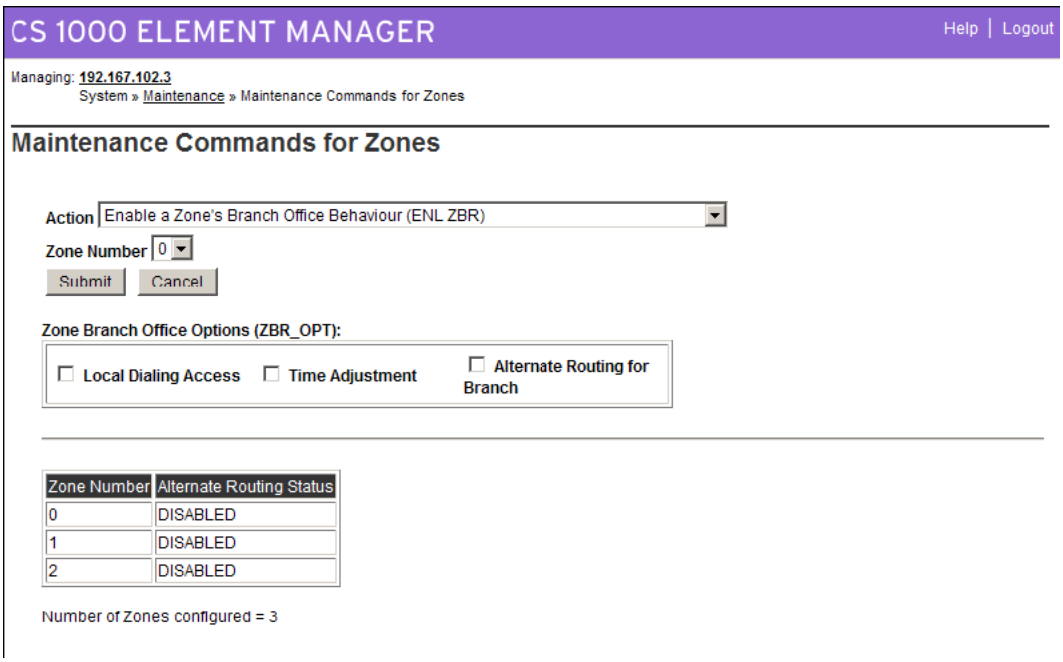


**Figure 86: Enable zone Branch Office behavior**

5. From the **Zone Number** list, select the zone number you want to configure.
6. Select the **Alternate Routing for Branch** check box to enable the feature.
7. Click **Submit**.

   The window updates with new configuration data for the zone you specified.

## Suppress Alarms

Use the following procedure to suppress alarms QoS0038 and QoS0039 for a configurable amount of time (0–3600 seconds).

### Suppressing Alternate Call Routing for alarms

1. Click System, IP Network, Zones
2. Select the Zone you are programming by clicking the plus sign to expand the choices under it.
3. Click Alternate Routing for Calls between IP Stations.
4. In the Alarm Suppression Time Period (ZAST) box, enter the desired time period.

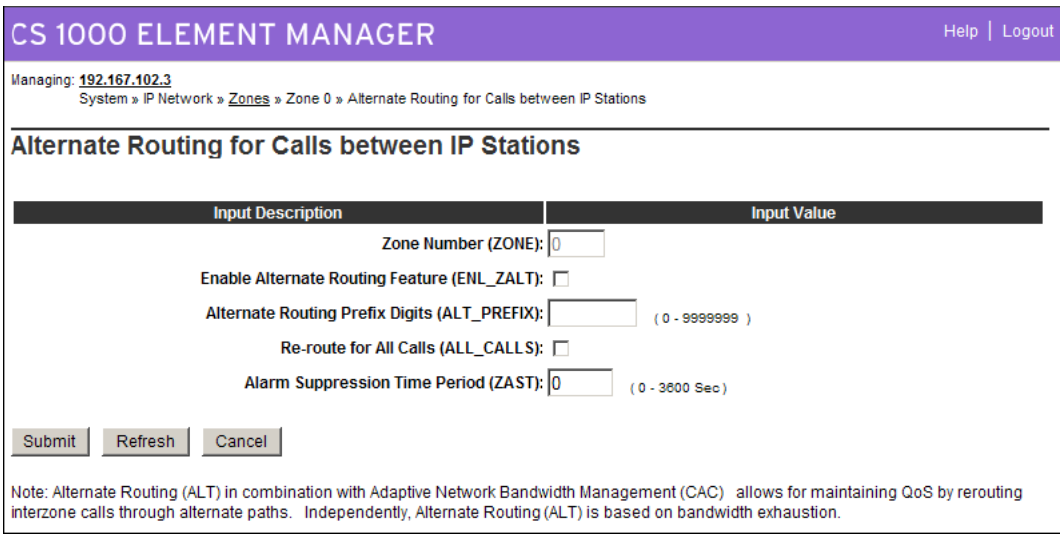


**Figure 87: Alarm Suppression Time Period (ZAST)**

5. Click Submit to enter the data.

# SIP Line service

Use Element Manager (EM) and BCC applications running inside the Communication Server 1000 Unified Common Manager (UCM) to configure and enable SIP Line Service for Communication Server 1000.

The SIP Line service package, 417, must be installed in order to enable SIP Line service on Communication Server 1000. The SIP Line service is enabled at the customer level.

A new SIP Line Service link exists on the customer page inside EM. Package 417 must be installed to activate the link. The following figure, Figure 88: Customer edit page for SIP Line service on page 318shows the Edit page for SIP Line Service in EM.

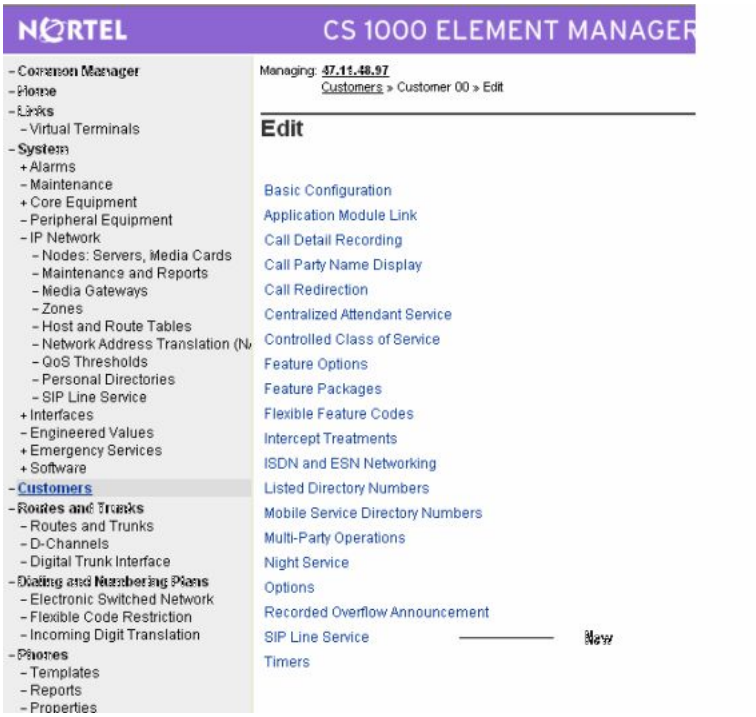


**Figure 88: Customer edit page for SIP Line service**

# Appendix A: Subnet mask conversion

## Subnet mask conversion from CIDR to dotted decimal format

Subnet masks are expressed in Classless InterDomain Routing (CIDR) format, appended to the IP address, such as 10.1.1.1/20. The subnet mask must be converted from CIDR format to dotted decimal format to configure IP addresses.

The CIDR format expresses the subnet mask as the number of bits counted from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. A typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format has a value from 0 to 255, where decimal 255 represents binary 1111 1111.

Follow the steps in the following procedure to convert a subnet mask from CIDR format to dotted decimal format.

### Converting a subnet mask from CIDR format to dotted decimal format

1. Divide the CIDR format value by 8.

   The result is a quotient (a zero or a positive number) and a remainder between 0 and 7.

2. The quotient designates the number of dotted decimal fields containing 255.

   In the example above, the subnet mask in CIDR format is /20. Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.

3. Use Table 112: CIDR format remainders on page 320to obtain the dotted decimal value for the field following the last field that contains 255.

   In the example of /20, the remainder is four. In Table 112: CIDR format remainders on page 320, a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next field is 240. Therefore the first three fields of the subnet mask are 255.255.240.

4. The last field in the dotted decimal format has a value of 0. Therefore, the complete subnet mask in dotted decimal format is 255.255.240.0.

**Table 112: CIDR format remainders**

| Remainder of CIDR format value divided by eight | Binary value | Dotted decimal value |
|---|---|---|
| 0 | 0000 0000 | 0 |
| 1 | 1000 0000 | 128 |
| 2 | 1100 0000 | 192 |
| 3 | 1110 0000 | 224 |
| 4 | 1111 0000 | 240 |
| 5 | 1111 1000 | 248 |
| 6 | 1111 1100 | 252 |
| 7 | 1111 1110 | 254 |

# Appendix B: Port number tables

All ports specified in the following tables are Listen ports and specify the destination IP address and port number. The tables do not specify the source IP address or port.

The Task column specifies the software task listening on the specified port. You can view the current port tables listed below by clicking the following Avaya Support link:

http://support.avaya.com

## Navigation

This appendix contains port number tables for all Meridian 1 and CS 1000M VoIP products.


Ephemeral ports on page 322

VXWorks Call Server port numbers on page 322

Voice Gateway Media Card port numbers on page 328

Media Gateway Controller port numbers on page 337

Co-resident (Linux) Call Server port numbers on page 344

Signaling Server port numbers on page 351

SIP Lines Gateway Port Numbers on page 358

Element Manager Port Numbers on page 364

Network Routing Service Port Numbers on page 369

Unified Communications Manager Port Numbers on page 374

Telephony Manager port numbers on page 379

IP Phone port numbers on page 381

Remote Office port numbers on page 381

CallPilot port numbers on page 382

Application Gateway (AG) 1000 port numbers on page 385

Contact Center port numbers on page 386

TLAN subnet stateless packet filtering on page 387

TLAN subnet stateful packet filtering on page 388

ELAN subnet packet filtering on page 390

## Ephemeral ports

Ephemeral ports are short lived ports that are dynamically assigned. Typically ephemeral ports are assigned on the client side of a TCP or UDP interaction. With FTP, ephemeral ports are also assigned on the server side as part of the protocol.

The most effective method to manage ephemeral ports in a firewall is through the use of connection tracking. These features examine the application protocol (e.g. FTP, RPC) to open the required firewall ports temporarily. Connection tracking for TCP, FTP is commonly available. UDP connection tracking is available in some firewalls. RPC connection tracking is no longer required with CS 1000 because fixed server ports are used.

When connection tracking is not used in firewalls for TCP, RPC or FTP protocols it is necessary to open all the ports in the ephemeral port ranges.

## Linux considerations

There can be various applications deployed and provisioned on a Linux server. Therefore, for any given Linux server, you must consider both the deployed applications (e.g. Call Server, Signaling Server, etc.) and the provisioned applications (e.g. on the Signaling Server - VTRK, LTPS, etc.). when determining the set of ports required.

## VXWorks Call Server port numbers

- MGMT = Management
- SC = System Control

**Table 113: VXWorks Call Server port numbers**

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. | |
| MGMT | TCP | 20 | ELAN | MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | FTP data port | Not Req'd if TCP connection tracking used. | |
| MGMT | TCP | 21 | ELAN | MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | FTP Control Port | Internal and external file transfers | |
| MGMT | TCP | 22 | ELAN | UCM, management stations | SSH | Secure Interactive logon, file transfers | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | TCP | 111 | ELAN | | Sunrpc-portmapper | Open but not used. Can be blocked in Firewall. | |
| MGMT | TCP | 513 | ELAN | SS, Management stations | rlogin | Remote Login | |
| SC | TCP | 600-1023 | ELAN | MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | Ephemeral ports for FTP data transfers & RLOGIN | Typically handled using TCP and FTP connection tracking in the firewalls | |
| SC | TCP | 1024-5000 | ELAN | UCM, MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | Ephemeral ports for TCP | Typically handled using TCP connection tracking in the firewalls | |
| SC | TCP | 5007 | ELAN | | High Availability | Open but not used. | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | | Communication Manager | Can be blocked in Firewall. | |
| SC | TCP | 6666 | ELAN | UCM | Config Process | Used for SNMP and NTP configuration propagation. | |
| SC | TCP | 8888 | ELAN | Contact Center, Call Pilot, MLS, SS | AML | 3rd Party Call Control | |
| SC | TCP | 15000 | ELAN | MGC, VGMC, SS | pbxLink | | |
| SC | TCP | 15081 | ELAN | EM | Xmsg Server | For CS 1000 Element Manager | |
| SC | TCP | 32781 | ELAN | MGC | Signaling for Sets & IPE cards on MGC | | |
| SC | TCP | 32784 | ELAN | MGC | IPMG TTY | | |
| SC | TCP | 32788 | ELAN | MGC | RPC MAIN / RPC GW | preassigned RPC port. | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | TCP | 32789 | ELAN | MGC | RPC INSTALL/ RPC GW INSTALL | preassigned RPC port. | |
| SC | UDP | 69 | ELAN | SS (TPS), VGMC (TPS) | tFTPd | Tone and Cadence File Transfers | |
| SC | UDP | 111 | ELAN | MGC | Sunrpc-portmapper | RPC Service for MGC | |
| SC | UDP | 123 | ELAN | External NTP Server | NTP | Time Synchronization. Source port 500. | |
| MGMT | UDP | 161 | ELAN | Management Systems, TM | SNMP query | | |
| SC | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500 | |
| SC | UDP | 600-1023 | ELAN | MGC | Ephemeral UDP ports for Sun RPC portmapper requests | | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| MGMT | UDP | 1929 | ELAN | TM | DBA CDR/ TRF | Used by TM | |
| MGMT | UDP | 2058-2185 | ELAN | TM | DBA Data | Used by TM | |
| SC | UDP | 5018 | ELAN | HA CS mate ELAN | High Availability Communications | HA Call server only. | |
| SC | UDP | 15000 | ELAN | MGC, VGMC, GR CS, HS CS Mate | rudp HB | source port 15000 | |
| SC | UDP | 15010 | ELAN | SS, MGC, VGMC, inactive CS | AFS | source port 15010 | |
| SC | UDP | 15011 | ELAN | SS, MGC, VGMC, inactive CS | AFS | source port 15011 | |
| SC | UDP | 31500-31504 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication | |
| SC | UDP | 32779 | ELAN | MGC | IPMG HeartBeat | source port 32779 | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source Element | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | UDP | 32780 | ELAN | MGC | IPMG HeartBeat Monitor | source port 32779 | |
| SC | TCP | 5007 | HSP | HA CS mate HSP | High Availability Communication Manager | HA Call server only. | |
| SC | UDP | 5010 | HSP | HA CS mate HSP | used for exchanging time and date information | HA Call Server Only | |
| SC | UDP | 5020 | HSP | HA CS mate HSP | HSP stop and copy | HA Call Server Only | |

# Voice Gateway Media Card port numbers

- MGMT = Management
- SC = System Control

**Table 114: Voice Gateway Media Card port numbers**

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | ESP (protocol number 50) | | ELAN | CS, EM, VGMCs | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. | n/a |
| MGMT | TCP | 20 | ELAN | EM, management systems, etc. | FTP data port | Not Req'd if TCP connection tracking used. | D |
| MGMT | TCP | 21 | ELAN | EM, management systems, etc. | FTP Control Port | File Transfers | D |
| MGMT | TCP | 22 | ELAN | UCM, EM, SS, CS, management stations | SSH | Secure Interactive logon, file transfers | M |
| MGMT | TCP | 23 | ELAN | EM, management systems, etc. | Telnet | Interactive login | D |
| SC | TCP | 111 | ELAN | | sunrpc-portmapper | Open but not used. Can be | M |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. | |
| MGMT | TCP | 513 | ELAN | ECM, SS(EM), SS, CS, management stations | RLOGIN | Remote Login | D |
| SC | TCP | 600-1023 | ELAN | CS, EM, Management Stations | Ephemeral ports for FTP data transfers & RLOGIN | Typically handled using TCP and FTP connection tracking in the firewalls | M |
| SC | TCP | 1024-5000 | ELAN | UCM, SS (EM), TM, CS, alternate CS, management stations | Ephemeral ports | Typically handled using FTP & TCP connection tracking in the firewalls | M |
| SC | TCP | 6666 | ELAN | CS, UCM | Config Process | Used for SNMP and NTP configuration propagation. | D |
| SC | TCP | 15080 | ELAN | EM | xmsg | Required for EM | M |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | TCP | 32788 | ELAN | | RPC MAIN / RPC GW | preassigned RPC port | M |
| SC | UDP | 68 | ELAN | SS(TPS) | Reples from bootp server | Initial configuration | M |
| SC | UDP | 111 | ELAN | | Sunrpc-portmapper | Remote Procedure Calls | M |
| MGMT | UDP | 161 | ELAN | TM, Management Systems | SNMP query | Required for SNMP Management | D |
| MGMT | UDP | 162 | ELAN | | SNMP Trap Receiver | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500 | D |
| | UDP | 514 | ELAN | | Syslog | Open on 32 port VGMC but not used. Can be blocked in Firewall. | |
| SC | UDP | 600-1023 | ELAN | CS | Ephemeral UDP ports for | Typically handled | M |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | | Sun RPC portmapper requests | using TCP, RPC and FTP connection tracking in the firewalls | |
| SC | UDP | 15000 | ELAN | CS (active, inactive, alternatives) | RUDP Heartbeat | source port 15000 | M |
| SC | UDP | 15001 | ELAN | CS (active, inactive, alternates) | CS State Change broadcasts | source port 15000 | M |
| SC | UDP | 15010 | ELAN | CS | AFS | source port 15010 | M |
| SC | UDP | 15011 | ELAN | CS | AFS | source port 15011 | M |
| | UDP | 17185 | ELAN | | proprietary | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 31500-31504 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication | D |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| SC | UDP | 32780 | ELAN | CS | HeartBeat Monitor | | M |
| SC | ESP (protocol number 50) | | TLAN | | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. | n/a |
| MG MT | TCP | 20 | TLAN | EM, Management Stations | FTP data port | Not Req'd if TCP connection tracking used. | |
| MG MT | TCP | 21 | TLAN | Management Stations, SS | FTP Control Port | | |
| MG MT | TCP | 22 | TLAN | Management Stations, SS | SSH | Secure Interactive logon, file transfers | |
| MG MT | TCP | 23 | TLAN | Management Stations, SS | Telnet | Interactive login | D |
| SC | TCP | 111 | TLAN | | Sunrpc-portmapper | Open but not used. Can be blocked in Firewall. | D |
| MG MT | TCP | 513 | TLAN | ECM, SS(EM), | RLOGIN | Remote Login | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | SS, CS, management stations | | | |
| | TCP | 1024-5000 | TLAN | UCM, EM, Management Stations | Ephemeral ports for FTP and TCP | Typically handled using FTP & TCP connection tracking in the firewalls | M |
| SC | TCP | 6666 | TLAN | | Config Process | Open but not used. Can be blocked in Firewall. | D |
| SC | TCP | 32788 | TLAN | | RPC MAIN / RPC GW | preassigned RPC port. Open but not used. Can be blocked in Firewall. | |
| | UDP | 68 | TLAN | | bootp | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 111 | TLAN | | Sunrpc-portmapper | Open but not used. Can be | D |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. | |
| MG MT | UDP | 162 | TLAN | | SNMP Trap Receiver | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 500 | TLAN | Any ISSS Target, source port 500 | IPSec IKE | Required if ISSS is used | |
| | UDP | 514 | TLAN | | Syslog | Open on 32 port VGMC by not used. Can be blocked in Firewall. | |
| SC | UDP | 15001 | TLAN | | CS State Change broadcasts | Open but not used. May be blocked in firewall. | M |
| SC | UDP | 15010 | TLAN | CS | AFS | Open but not used. May be blocked in firewall. source port 15010 | M |
| SC | UDP | 15011 | TLAN | CS | AFS | Open but not used. | M |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| | | | | | | May be blocked in firewall. source port 15011 | |
| | UDP | 17185 | TLAN | | proprietary | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 31500-31504 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication | D |
| VoIP Media | UDP (RTP, SRTP) | 5200-5246 | TLAN | IP phones, MGCs, VGMCs, voice GWs | RTP, SRTP | even numbers-ITGP | n/a |
| VoIP Media | UDP (RTP, SRTP) | 5200-5262 | TLAN | IP phones, MGCs, VGMCs, voice GWs | RTP, SRTP | even numbers-Media Card | n/a |
| VoIP Media | UDP(RTCP) | 5201-5247 | TLAN | IP phones, MGCs, VGMCs, voice GWs | RTCP | odd numbers-ITGP | n/a |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | M = Mandatory, always open. D = Default, included in AR Default rules file n/a = not controlled by AR. |
|---|---|---|---|---|---|---|---|
| VoIP Media | UDP(RTCP) | 5201-5263 | TLAN | IP phones, MGCs, VGMCs, voice GWs | RTCP | odd numbers-Media Card | n/a |

# Media Gateway Controller port numbers

- MGMT = Management
- MEDIA = Voice media streams
- SC = System Control

**Table 115: Media Gateway Controller port numbers**

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| SC | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. | n/a |
| MGMT | TCP | 20 | ELAN | EM, managem | FTP data port | Not Req'd if TCP connection | D |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| | | | | ent stations | | tracking used. | |
| MGMT | TCP | 21 | ELAN | EM, management stations | FTP Control Port | File Transfers | D |
| MGMT | TCP | 22 | ELAN | UCM, EM, SS, CS, management stations | SSH | Secure Interactive logon, file transfers | M |
| MGMT | TCP | 23 | ELAN | UCM, EM, SS, CS, management stations | TELNET | Interactive login | D |
| SC | TCP | 111 | ELAN | | Sunrpc-portmapper | Open but not used. Can be blocked in Firewall. | M |
| SC | TCP | 600-1023 | ELAN | CS, EM, Management Stations | Ephemeral ports for FTP data transfers & RLOGIN | Typically handled using TCP and FTP connection tracking in the firewalls | M |
| SC | TCP | 1024-5000 | ELAN | SS (EM), TM, CS, alternate CS, management stations | Ephemeral ports | Typically handled using TCP connection tracking in the firewalls | M |
| | TCP | 2010 | ELAN | CS | CEMUX (PRI/BRI D-Channels) | | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| SC | TCP | 6666 | ELAN | CS, UCM | Config Process | Used for SNMP and NTP configuration propagation. | D |
| MGMT | TCP | 15080 | ELAN | EM | XMSG | Used by Element Manager | M |
| SC | TCP | 32782 | ELAN | CS | CEMUX (PRI/BRI D-Channels) | | M |
| SC | TCP | 32783 | ELAN | CS | CEMUX (PRI/BRI D-Channels) | | |
| SC | TCP | 32786 | ELAN | CS | IPMG DB Sync | | D |
| SC | TCP | 32788 | ELAN | CS | RPC MAIN / RPC GW | preassigned RPC port. | M |
| SC | TCP | 32789 | ELAN | CS | RPC INSTALL/ RPC GW INSTALL | preassigned RPC port. Applicable for Co-res and VxWorks | M |
| SC | UDP | 111 | ELAN | CS (active and any alternates) | Sunrpc-portmapper | Remote Procedure Calls | M |
| MGMT | UDP | 161 | ELAN | TM, Management Systems | SNMP query | SNMP Management | D |
| MGMT | UDP | 162 | ELAN | | SNMP Trap Receiver | Open but not used. Can be | D |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. | |
| SC | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500. | D |
| SC | UDP | 600-1023 | ELAN | CS | Ephemeral UDP ports for Sun RPC portmapper requests | Typically handled using TCP, RPC and FTP connection tracking in the firewalls | M |
| SC | UDP | 15000 | ELAN | CS (active, inactive, alternates) | rudp HB | source port 15000 | M |
| SC | UDP | 15001 | ELAN | CS (active, inactive, alternates) | CS State Change broadcasts | source port 15000 | |
| SC | UDP | 15010 | ELAN | CS | AFS | source port 15010 | M |
| SC | UDP | 15011 | ELAN | CS | AFS | source port 15011 | M |
| | UDP | 17185 | ELAN | | proprietary | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 31500-31504 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| SC | UDP | 32779 | ELAN | CS | IPMG HeartBeat | source port 32779 | M |
| SC | UDP | 32780 | ELAN | CS | IPMG HeartBeat Monitor | source port 32779 | M |
| SC | ESP (protocol number 50) | | TLAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. | n/a |
| MGMT | TCP | 20 | TLAN | EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. | |
| MGMT | TCP | 21 | TLAN | EM, management stations | FTP Control Port | File Transfers | |
| MGMT | TCP | 22 | TLAN | UCM, EM, SS, CS, management stations | SSH | Secure Interactive logon, file transfers | |
| MGMT | TCP | 23 | TLAN | Management Stations | TELNET | Remote Login | D |
| SC | TCP | 111 | TLAN | | Sunrpc-portmapper | Open but not used. Can be blocked in Firewall. | |
| MGMT | TCP | 513 | TLAN | UCM, EM, SS, CS, management stations | RLOGIN | Remote Login | D |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| SC | TCP | 600-1023 | TLAN | Management Stations | Ephemeral ports for FTP data transfers & RLOGIN | Typically handled using TCP and FTP connection tracking in the firewalls | M |
| SC | TCP | 1024-5000 | TLAN | Management Stations | Ephemeral ports | Typically handled using TCP connection tracking in the firewalls | M |
| SC | TCP | 6666 | TLAN | | Config Process | Open but not used. Can be blocked in Firewall. | D |
| SC | TCP | 32786 | TLAN | | IPMG DB Sync | Open but not used. Can be blocked in Firewall. | |
| SC | TCP | 32788 | TLAN | | RPC MAIN / RPC GW | preassigned RPC port. Open but not used. Can be blocked in Firewall. | |
| SC | TCP | 32789 | TLAN | | RPC INSTALL/ RPC GW INSTALL | preassigned RPC port. Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 111 | TLAN | | Sunrpc-portmapper | Open but not used. Can be | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. | |
| MGMT | UDP | 162 | TLAN | | SNMP Trap Receiver | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 500 | TLAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500. | D |
| SC | UDP | 15001 | TLAN | | CS State Change broadcasts | Open but not used. May be blocked in firewall. | |
| SC | UDP | 15010 | TLAN | | AFS | Open but not used. May be blocked in firewall. source port 15010 | M |
| SC | UDP | 15011 | TLAN | | AFS | Open but not used. May be blocked in firewall. | M |
| | UDP | 17185 | TLAN | | proprietary | Open but not used. Can be blocked in Firewall. | |
| SC | UDP | 31500-31504 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication | D |
| SC | UDP | 32779 | TLAN | | IPMG HeartBeat | Open but not used. Can be | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments | AR Rules * |
|---|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. | |
| SC | UDP | 32780 | TLAN | | IPMG HeartBeat Monitor | Open but not used. Can be blocked in Firewall. | |
| Media | UDP (RTP, SRTP) | 5200–5263 (DB32 in DB2) 5200–5391 (DB96 in DB2) 5392–5455 (DB32 in DB1) 5392–5583 (DB96 in DB1) 5392–5647 (DB128 in DB1) | TLAN of DSP DBs | IP phones, MGCs, VGMCs, voice GWs | RTCP, RTP (Odd are RTCP, even are RTP) | Voice Media | n/a |

**Note:**

* AR Rules — D = Default, M = Mandatory

# Co-resident (Linux) Call Server port numbers

- BASE = Linux Base
- CS = Coresident Call Server

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | ICMP | | ELAN | UCM, SS, CS | | |
| Base | TCP | 20 | ELAN | MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | ELAN | MGC, VGMC, SS, TM, GR CS, mate CS, backup servers, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | ELAN | UCM, management stations, EM | SSH | Secure Interactive logon, file transfers |
| Base | TCP | 23 | ELAN | Management Systems, UCM, MGC, VGMC, CS | TELNET | Interactive logon |
| Base | TCP | 80 | ELAN | Management Stations | http | Web Interface |
| CS | TCP | 111 | ELAN | | Sunrpc-portmapper | Open but not used. Can be blocked in Firewall. |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 443 | ELAN | Management Systems | https | Secure Web Interface |
| Base | TCP | 513 | ELAN | SS, Management stations | rlogin | Remote Login |
| SS | TCP | 705 | Loopback | Internal | SS-Subagent | Loopback Interface Only, can be blocked on ELAN/TLAN by firewall. |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | ELAN | CS, SS, VGMC, MGC, UCM | Config Process | Used for SNMP and NTP configuration propagation. |
| CS | TCP | 8888 | ELAN | Contact Center, Call Pilot, MLS, SS | AML | 3rd Party Call Control |
| CS | TCP | 15000 | ELAN | MGC, VGMC, SS | pbxLink | |
| CS | TCP | 15081 | ELAN | EM | Xmsg Server | For CS 1000 Element Manager |
| Base | TCP | 15086 | ELAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | ELAN | Management Stations, MGC, VGMC, SS, Backup Servers | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| CS | TCP | 32781 | ELAN | MGC | IPMG SSD | |
| CS | TCP | 32784 | ELAN | MGC | IPMG TTY | |
| CS | TCP | 32788 | ELAN | MGC | RPC MAIN / RPC GW | preassigned RPC port. |
| CS | TCP | 32789 | ELAN | MGC | RPC INSTALL/ RPC GW INSTALL | preassigned RPC port. |
| Base | TCP | 33700-61000 | ELAN | UCM, SS, MGC, VGMC, TM, Management Stations, Contact Center, CallPilot | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| Base | UDP | 53 | TLAN | SS | DNS | |
| CS | UDP | 111 | ELAN | MGC | Sunrpc-portmapper | RPC Service for MGC |
| Base | UDP | 123 | ELAN | External NTP Server | NTP | Time Synchronization. Source port 500. |
| Base | UDP | 161 | ELAN | Management Systems, TM | SNMP query | |
| Base | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500 |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| CS | UDP | 1929 | ELAN | TM | DBA CDR/ TRF | Used by TM |
| CS | UDP | 2058-2185 | ELAN | TM | DBA Data | Used by TM |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| CS | UDP | 15000 | ELAN | CS | RUDP PBXlink from CS | |
| Base | UDP | 15010 | ELAN | SS, MGC, VGMC, inactive CS | AFS | Source Port 15010 |
| Base | UDP | 15011 | ELAN | SS, MGC, VGMC, inactive CS | AFS | Source Port 15011 |
| CS | UDP | 31500-31504 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| CS | UDP | 32779 | ELAN | MGC | IPMG HeartBeat | source port 32779, 32780 |
| CS | UDP | 32780 | ELAN | MGC | IPMG HeartBeat Monitor | source port 32779 |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | ESP (protocol number 50) | | TLAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | TLAN | UCM, SS, CS | | |
| Base | TCP | 20 | TLAN | backup servers, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | TLAN | backup servers, managem | FTP Ctrl Port | Insecure File Transfers |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | ent stations | | |
| Base | TCP | 22 | TLAN | UCM, management stations | SSH | Secure Interactive logon, file transfers |
| Base | TCP | 23 | TLAN | UCM, management stations | TELNET | Interactive logon |
| Base | TCP | 80 | TLAN | Management Stations | http | Web Interface |
| Base | TCP | 443 | TLAN | Management Stations | https | Secure Web Interface |
| Base | TCP | 513 | TLAN | Remote Management Systems | rlogin | Interactive logon (when rlogin is enabled) |
| Base | TCP | 705 | Loopback | Internal | SS-Subagent | Loopback Interface Only, can be blocked on ELAN/TLAN by firewall. |
| Base | TCP | 2000 | TLAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | TLAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | TLAN | CS, SS, VGMC, MGC, UCM | Config Process | Typically uses ELAN only |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | TLAN | backup servers, management stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 31500-31504 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | TCP | 33700-61000 | TLAN | UCM, Management Stations, Backup Servers | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| Base | UDP | 53 | TLAN | SS | DNS | |
| Base | UDP | 123 | TLAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| Base | UDP | 500 | TLAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500 |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| Base | UDP | 15010 | TLAN | SS, MGC, VGMC, CS | AFS | |
| Base | UDP | 15011 | TLAN | SS, MGC, VGMC, CS | AFS | |
| Base | UDP | 33600-33699 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |

# Signaling Server port numbers

**Note:**

Various combinations of the following Linux applications can be configured in co-resident configurations. The resulting port usage for a "co-resident" server is the superset of the ports for the constituent elements.

- BASE = Linux Base
- VTRK = IP Virtual Trunks
- TPS = UNIStim Terminal Proxy Server

**Table 116: Signaling Server port numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | ELAN | UCM, SS, CS | | |
| Base | TCP | 20 | ELAN | UCM, VGMCs, EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | ELAN | UCM, VGMCs, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | ELAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | ELAN | Management Stations, UCM | TELNET | Interactive logon |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 80 | ELAN | UCM, management stations | http | Web Interface |
| Base | TCP | 443 | ELAN | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | ELAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | ELAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | TCP | 15080 | ELAN | EM | xmsg server | Used by Element Manager |
| Base | TCP | 15086 | ELAN | | Gryphon | PCAP Control |
| Base | TCP | 25100-25200 | ELAN | VGMC, CS, SS, Management Stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | ELAN | ANY | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| Base | UDP | 53 | ELAN | | DNS | |
| Base | UDP | 67 | ELAN | VGMC | bootp server | VGMC boot |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 123 | ELAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | ELAN | TM, SNMP Management Systems | SNMP query | |
| Base | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500. |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| Base | UDP | 15000 | ELAN | CS (active, inactive) | RUDP | source port 15000 |
| Base | UDP | 15001 | ELAN | CS | CS State Change broadcasts | source port 15000 |
| Base | UDP | 15002 | ELAN | Internal | RUDP from CS in Co-Res Mode | source port 15000 |
| Base | UDP | 15010 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| TPS | UDP | 16540 | ELAN | Other SS(tps) in same node. | TPS -> TPS, communications for Load Balancing | Primarily uses TLAN |
| TPS (ncs) | UDP | 16501 | ELAN | Other SS(tps), NRS in network. | Network Connect Server for Network Virtual Office | Primarily uses TLAN |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 33600-33699 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | ESP (protocol number 50) | | TLAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | TLAN | UCM, SS, CS | Health Checks, etc. | |
| | TCP | 20 | TLAN | UCM, VGMCs, EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | TLAN | UCM, VGMCs, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | TLAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | TLAN | Management Stations, UCM | TELNET | Interactive logon |
| Base | TCP | 80 | TLAN, TLAN-nodeIP | UCM, management stations | http | Web Interface |
| Base | TCP | 443 | TLAN, TLAN-nodeIP | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | TLAN | Internal | SS-Subagent | Loopback Interface Only |
| VTRK | TCP | 1718 | TLAN (nodeIP) | | H.323 | Not Used. |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| VTRK | TCP | 1719 | TLAN (nodeIP) | SS(vtrk), NRS (gk), other H.323 devices | H.323/H.245 | H.323 Vtrk signaling between GW's. |
| VTRK | TCP | 1720 | TLAN (nodeIP) | SS(vtrk), other H.323 devices | H.323/H.245 | H.323 Vtrk signaling between GW's. |
| Base | TCP | 2000 | TLAN, TLAN (nodeIP) | Management Stations | Gryphon | |
| Base | TCP | 3306 | TLAN | Internal | MySQL | Local Database Access |
| VTRK | TCP | 5060 | TLAN (nodeIP) | SS(vtrk), NRS, other SIP devices | SIP | SIP Signaling |
| VTRK | TCP | 5061 | TLAN (nodeIP) | SS(vtrk), NRS, other SIP devices | SIP/TLS | Secure SIP (TLS) Signaling |
| Base | TCP | 6666 | TLAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| VTRK (amlfe) | TCP | 8888 | TLAN | Contact Center, Call Pilot, MLS | AML | 3rd Party Call Control |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 15080 | TLAN | EM | xmsg server | Used by Element Manager |
| Base | TCP | 25100-25200 | TLAN | Management Stations, UCM | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 33700-61000 | TLAN | UCM, management stations, EM, NRS, SS(GK), SS(vtrk), Other SIP or H.323 GW | Ephemeral ports | Typically handled using TCP & FTP connection tracking in the firewalls |
| VTRK | TCP | 40000-42400 | TLAN (nodeIP) | SS (vtrk), other H.323 devices | H.245 Signaling | |
| Base | UDP | 53 | TLAN | | DNS | |
| TPS | UDP | 69 | TLAN | IP Phones | tftp | Firmware Download for IP Phones (Req'd for Phase 1 phones) |
| Base | UDP | 123 | TLAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| Base | UDP | 500 | TLAN | Any ISSS Target | IPsec IKE, source port 500 | Required if ISSS is used. |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| VTRK | UDP | 1718 | TLAN (nodeIP) | | H.323 | Not Used. |
| VTRK | UDP | 1719 | TLAN (nodeIP) | SS(vtrk), NRS (gk), other H.323 devices | H.323 | RAS Signaling between VTRK and NRS (gk) |
| VTRK | UDP | 1720 | TLAN (nodeIP) | SS(vtrk), other | H.323 | H.323 Vtrk signaling |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | H.323 devices | | between GW's. |
| TPS (csv) | UDP | 4100 | TLAN (nodeIP) | UNISTIM IP Phones | UNIStim | Connection Server |
| TPS (csv) | UDP | 4101 | TLAN (nodeIP) | UNISTIM IP Phones | UNIStim / DTLS | Connection Server (secure) |
| VTRK | UDP | 5060 | TLAN (nodeIP) | SS(vtrk), NRS (sps) | SIP (source port 5060) | SIP Signaling |
| TPS | UDP | 5100 | TLAN | IP Phones | UNIStim | Terminal Proxy Server |
| TPS | UDP | 5101 | TLAN | IP Phones | UNIStim / DTLS | Terminal Proxy Server (secure) |
| TPS | UDP | 5105 | TLAN | Phase 2 and later IP Phones | UFTP | Firmware Download UNISTM IP Phones |
| TPS | UDP | 7300 | TLAN | IP Phones | UNIStim | TPS Load Balancing |
| TPS | UDP | 7301 | TLAN | IP Phones | UNIStim / DTLS | TPS Load Balancing (secure) |
| TPS | UDP | 10000 | TLAN | IP Phones | Echo Server | NAT Discovery |
| Base | UDP | 15010 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| TPS (ncs) | UDP | 16501 | TLAN | Other SS(tps), NRS in network. | Network Connect Server | Network Virtual Office |
| TPS (ncs) | UDP | 16502 | TLAN | NRS (ncs) <-> TPS (ncs) | Network Connect Server | NCS - CS2100 |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| TPS | UDP | 16540 | TLAN | Other SS (tps) in same node. | TPS -> TPS (TPS) | TPS to TPS communications for Load Balancing |
| Base | UDP | 16550 | TLAN | Other SS in node | SS <-> SS | Leader/ Follower Election |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |

# SIP Lines Gateway Port Numbers

**Note:**

Various combinations of the following Linux applications can be configured in co-resident configurations. The resulting port usage for a "co-resident" server is the superset of the ports for the constituent elements.

- Base = Linux Base
- SIPL = SIP Lines

**Table 117: SIP Lines Gateway Port Numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | |
| Base | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | ELAN | UCM, SS, CS | | |
| Base | TCP | 20 | ELAN | UCM, EM, management stations | FTP data port | Not Req'd if TCP connection |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | tracking used. |
| Base | TCP | 21 | ELAN | UCM, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | ELAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | ELAN | Management Stations, UCM | TELNET | Interactive logon |
| Base | TCP | 80 | ELAN | UCM, management stations | http | Web Interface |
| Base | TCP | 443 | ELAN | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | ELAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | ELAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | UDP | 15010 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | TCP | 15080 | ELAN | EM | xmsg server | Used by Element Manager |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 15086 | ELAN | | Gryphon | PCAP Control |
| Base | TCP | 25100-25200 | ELAN | CS, SS, Management Stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | ELAN | CS, SS, EM, UCM, Management Stations | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| Base | UDP | 53 | ELAN | | DNS | |
| Base | UDP | 67 | ELAN | | bootp server | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 123 | ELAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | ELAN | TM, SNMP Management Systems | SNMP query | |
| Base | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500. |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| Base | UDP | 15000 | ELAN | CS (active, inactive, alternatives) | RUDP | source port 15000 |
| Base | UDP | 15001 | ELAN | CS (active, inactive, alternates) | CS State Change broadcasts | source port 15000 |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 15002 | ELAN | Internal | RUDP from CS in Co-Res Mode | source port 15000 |
| Base | UDP | 15010 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | ESP (protocol number 50) | | TLAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | TLAN | UCM, SS, CS | Health Checks, etc. | |
| Base | TCP | 20 | TLAN | UCM, EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | TLAN | UCM, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | TLAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | TLAN | Management Stations, UCM | TELNET | Interactive logon |
| Base | TCP | 80 | TLAN | UCM, management stations | http | Web Interface |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 443 | TLAN | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | TLAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | TLAN | Management Stations | Gryphon | |
| Base | TCP | 3306 | TLAN | Internal | MySQL | Local Database Access |
| SIPL | TCP | 5070 | TLAN | SIP Phones | SIP | SIP Signaling with SIP Phones. |
| SIPL | TCP | 5071 | TLAN | SIP Phones | SIP/TLS | Secure SIP Signaling with SIP Phones. |
| Base | TCP | 6666 | TLAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 15080 | TLAN | EM | xmsg server | Used by Element Manager |
| Base | TCP | 25100-25200 | TLAN | Management Stations, UCM, EM | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | TLAN | UCM, management stations, EM, SIP Phones | Ephemeral ports | Typically handled using TCP & FTP connection tracking in the firewalls |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 53 | TLAN | | DNS | |
| Base | UDP | 123 | TLAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| Base | UDP | 500 | TLAN | Any ISSS Target | IPsec IKE, source port 500 | Required if ISSS is used. |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| SIPL | UDP | 5070 | TLAN | SIP Phones | SIP | SIP Signaling with SIP Phones. |
| Base | UDP | 15010 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 16550 | TLAN | Other SS in node | SS <-> SS | Leader/ Follower Election |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |

# Element Manager Port Numbers

**Note:**

Various combinations of the following Linux applications can be configured in co-resident configurations. The resulting port usage for a "co-resident" server is the superset of the ports for the constituent elements.

- BASE = Linux Base
- EM = Element Manager

**Table 118: Element Manager Port Numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | |
| Base | ESP (protocol number 50) | | ELAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | ELAN | UCM, SS, CS | | |
| Base | TCP | 20 | ELAN | UCM, VGMCs, EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | ELAN | UCM, VGMCs, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | ELAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | ELAN | Management Stations, UCM | TELNET | Interactive logon |
| Base | TCP | 80 | ELAN | UCM, management stations | http | Web Interface |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 443 | ELAN | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | ELAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | Internal | MySQL | Local Database Access |
| EM | TCP | 4789 | ELAN | Management Stations | EM Virtual Terminal Java app to EM | |
| Base | TCP | 6666 | ELAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | TCP | 15086 | ELAN | | Gryphon | PCAP Control |
| Base | TCP | 25100-25200 | ELAN | VGMC, CS, SS, Management Stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | ELAN | ANY | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| Base | UDP | 53 | ELAN | | DNS | |
| Base | UDP | 67 | ELAN | VGMC | bootp server | VGMC boot |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 123 | ELAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | ELAN | TM, SNMP Management Systems | SNMP query | |
| EM | UDP | 162 | ELAN | CS | SNMP Traps | BCC |
| Base | UDP | 500 | ELAN | Any CS1K element | IPsec IKE | Required if ISSS is used. Source port 500. |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| Base | UDP | 15010 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | ESP (protocol number 50) | | TLAN | Any CS1K element | IPsec, ESP - Encapsulating Security Payload | Required if ISSS is used. |
| Base | ICMP | | TLAN | UCM, SS, CS | Health Checks, etc. | |
| | TCP | 20 | TLAN | UCM, VGMCs, EM, management stations | FTP data port | Not Req'd if TCP connection tracking used. |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 21 | TLAN | UCM, VGMCs, EM, management stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | TLAN | Management Stations, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | TLAN | Management Stations, UCM | TELNET | Interactive logon |
| Base | TCP | 80 | TLAN, TLAN-nodeIP | UCM, management stations | http | Web Interface |
| Base | TCP | 443 | TLAN, TLAN-nodeIP | Management Stations | https | Secure Web Interface |
| Base | TCP | 705 | TLAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | TLAN, TLAN (nodeIP) | Management Stations | Gryphon | |
| Base | TCP | 3306 | TLAN | Internal | MySQL | Local Database Access |
| EM | TCP | 4789 | TLAN | Management Stations | EM Virtual Terminal Java app to EM | |
| Base | TCP | 6666 | TLAN | CS | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | TLAN | Management Stations, UCM | FTP Data Ports | Typically handled using FTP connection |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | tracking in the firewalls |
| Base | TCP | 33700-61000 | TLAN | UCM, management stations, EM, NRS, SS(GK), SS(vtrk), Other SIP or H.323 GW | Ephemeral ports | Typically handled using TCP & FTP connection tracking in the firewalls |
| Base | UDP | 53 | TLAN | | DNS | |
| Base | UDP | 123 | TLAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| EM | UDP | 162 | TLAN | | SNMP Traps | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 500 | TLAN | Any ISSS Target | IPsec IKE, source port 500 | Required if ISSS is used. |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| Base | UDP | 15010 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 33600-33699 | TLAN | UCM | Radius | Central Authenticat |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | ion. (source port 1812) |

# Network Routing Service Port Numbers

**Note:**

Various combinations of the following Linux applications can be configured in co-resident configurations. The resulting port usage for a "co-resident" server is the superset of the ports for the constituent elements.

- BASE = Linux Base
- NRS(GK) = H.323 Gatekeeper
- NRS(SIP) = SIP Proxy Server or SIP Redirect Server
- NRS (NCS) = Network Connect Server

**Table 119: Network Routing Service Port Numbers**

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | |
| Base | ICMP | | ELAN | UCM, NRS, SS | Health Check between NRS primary/ backup, etc. | |
| Base | TCP | 20 | ELAN | Management Stations, UCM, NRS, 4.x/5.x failsafe NRS | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | ELAN | Management Stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | ELAN | Management Stations, UCM, NRS | SSH / sFTP | Secure Interactive logon & File Transfers |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | TCP | 23 | ELAN | Management Stations, UCM | TELNET | Insecure Interactive logon |
| Base | TCP | 80 | ELAN | Management Stations | http | Web Interface |
| Base | TCP | 443 | ELAN | Management Stations | https | Web Interface |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | NRS <-> NRS | MySQL | Database Access, typically uses TLAN |
| NRS (sip) | TCP | 5060 | ELAN | SS(vtrk), NRS, other SIP devices | SIP | SIP Signaling |
| NRS (sip) | TCP | 5061 | ELAN | SS(vtrk), NRS, other SIP devices | SIP/TLS | Secure SIP (TLS) Signaling |
| Base | TCP | 6666 | ELAN | UCM | Config Process | Used for SNMP and NTP configuration propagation. |
| Base | TCP | 15086 | ELAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | ELAN | 4.x/5.x Failsafe NRS, Management Stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | ELAN | Backup Servers, NRS, Failsafe NRS, etc. | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 53 | ELAN | | DNS | |
| Base | UDP | 123 | ELAN | External NTP Server | NTP, source port 123 | Time Synchroniz ation |
| Base | UDP | 161 | ELAN | TM, SNMP Managemen t Systems | SNMP query | |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| NRS (gk) | UDP | 1719 | ELAN | SS (vtrk), NRS (gk) | H.323 - RAS Signaling between Vtrk GW and GK/ NRS | Typically not used on ELAN. |
| NRS (sip) | UDP | 5060 | ELAN | SS(vtrk), NRS, other SIP devices | SIP | SIP Signaling |
| Base | UDP | 15010 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| Base | UDP | 15011 | ELAN | | AFS | Open but not used. Can be blocked in Firewall. |
| NRS (ncs) | UDP | 16500 | ELAN | SS(tps) | Network Connect Server for Network Virtual Office | Primarily uses TLAN |
| NRS (ncs) | UDP | 16501 | ELAN | SS(tps) | Network Connect Server for Network Virtual Office | Primarily uses TLAN |
| Base | UDP | 33434-335 24 | ELAN | ANY | Traceroute | |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 33600-33699 | ELAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |
| Base | ICMP | | TLAN | UCM, NRS, SS | Health Check between NRS primary/ backup, etc. | |
| | TCP | 20 | TLAN | Management Stations, UCM, NRS, 4.x/5.x failsafe NRS | FTP data port | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | TLAN | Management Stations | FTP Ctrl Port | Insecure File Transfers |
| Base | TCP | 22 | TLAN | Management Stations, UCM, NRS | SSH / sFTP | Secure Interactive logon & File Transfers |
| Base | TCP | 23 | TLAN | Remote Management Systems | TELNET | Insecure Interactive logon |
| Base | TCP | 80 | TLAN | Management Stations | http | Web Interface |
| Base | TCP | 443 | TLAN | Management Stations | https | Web Interface |
| Base | TCP | 2000 | TLAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | TLAN | Mate NRS | MySQL | Remote Data Sync |
| NRS (sip) | TCP | 5060 | TLAN | SS(vtrk), NRS, other SIP devices | SIP | SIP Signaling |
| NRS (sip) | TCP | 5061 | TLAN | SS(vtrk), NRS, other SIP devices | SIP/TLS | Secure SIP (TLS) Signaling |
| Base | TCP | 6666 | TLAN | UCM | Config Process | Used for SNMP and |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | NTP configuration propagation. |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | TLAN | 4.x/5.x Failsafe NRS, Management Stations | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| Base | TCP | 33700-61000 | TLAN | Backup Servers, NRS, Failsafe NRS, etc. | Ephemeral ports | Typically handled using TCP & FTP connection tracking in the firewalls |
| Base | UDP | 53 | TLAN | | DNS | |
| Base | UDP | 123 | TLAN | External NTP Server | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| NRS (gk) | UDP | 1719 | TLAN | SS(vtrk), NRS (gk), other H.323 devices | H.323 | RAS Signaling between VTRK and NRS (gk) |
| NRS (sip) | UDP | 5060 | TLAN | SS(vtrk), NRS, other SIP devices | SIP (source port 5060) | SIP Signaling |
| Base | UDP | 15010 | TLAN | | AFS | Open but not used. Can be |

| Task | L4 protocol (TCP/ UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | blocked in Firewall. |
| Base | UDP | 15011 | TLAN | | AFS | Open but not used. Can be blocked in Firewall. |
| NRS (ncs) | UDP | 16500 | TLAN | SS(tps) | Network Connect Server for Network Virtual Office | |
| NRS (ncs) | UDP | 16501 | TLAN | SS(tps) | Network Connect Server for Network Virtual Office | |
| Base | UDP | 33434-33524 | TLAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | TLAN | UCM, Primary, UCM Backup | Radius Replies (source port 1812) | Central Authentication |

# Unified Communications Manager Port Numbers

**Note:**

Various combinations of the following Linux applications can be configured in co-resident configurations. The resulting port usage for a "co-resident" server is the superset of the ports for the constituent elements.

- BASE = Linux Base
- UCM = Unified Communications Manager

**Table 120: Unified Communications Manager Port Numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | |
| Base | ICMP | | ELAN | UCM, SS, CS | | |
| | TCP | 20 | ELAN | Management Stations, UCM, SRG, MGC, VGMC, CS, SS, TM | Ephemeral source FTP data port when using "active" mode. | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | ELAN | Management Stations, UCM, SRG, MGC, VGMC, CS, SS, TM | FTP Ctrl Link | File Transfers |
| Base | TCP | 22 | ELAN | Management Stations, UCM, SS, MGC, VGMC, CS | SSH | Secure Interactive logon |
| Base | TCP | 23 | ELAN | Management Stations, UCM, MGC, VGMC, CS | TELNET | Insecure Interactive logon |
| Base | TCP | 80 | ELAN | Management Stations | http | Web Interface |
| Base | TCP | 443 | ELAN | Management Stations | https | Web Interface |
| Base | TCP | 705 | ELAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | ELAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | ELAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | ELAN | CS, SS, VGMC, MGC, UCM | Config Process | Used for SNMP and NTP configuration propagation. |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| UCM | TCP | 8193 | ELAN | UCM Members (not VxWorks) | jboss-jms | FQDN is used |
| Base | TCP | 15086 | ELAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | ELAN | ANY | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| UCM | TCP | 31000 | ELAN | UCM Members (not VxWorks) | clustered JNDI Stub Download | FQDN is used |
| UCM | TCP | 31001 | ELAN | UCM Members (not VxWorks) | clustered JNDI RMI queries | FQDN is used |
| UCM | TCP | 31002 | ELAN | UCM Primary, Backup | | FQDN is used |
| Base | TCP | 32768-61000 | ELAN | ANY | Ephemeral ports | Typically handled using TCP and FTP connection tracking in the firewalls |
| UCM | TCP | 45566 - 45568 | ELAN | UCM Primary, Backup | JGroup protocol | FQDN is used |
| Base | UDP | 53 | ELAN | | DNS | |
| Base | UDP | 67 | ELAN | VGMC | bootp server | VGMC boot |
| Base | UDP | 123 | ELAN | Any | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | ELAN | TM, SNMP Management Systems | SNMP query | |
| Base | UDP | 514 | ELAN | Linux Elements | Syslog | |
| UCM | UDP | 1812 | ELAN | | RADIUS | |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| Base | UDP | 15010 | ELAN | | AFS | |
| Base | UDP | 15011 | ELAN | | AFS | |
| Base | UDP | 33434-33524 | ELAN | ANY | Traceroute | |
| Base | UDP | 33600-33699 | ELAN | UCM | Radius | Central Authenticati on. (source port 1812) |
| Base | ESP (protocol number 50) | | TLAN | | IPSEC, ESP - Encapsulated payload | Not Used. |
| Base | ICMP | | TLAN | | | |
| | TCP | 20 | TLAN | Management Systems, UCM, SRG, MGC, VGMC, CS, SS, TM | Ephemeral source FTP data port when using "active" mode. | Not Req'd if TCP connection tracking used. |
| Base | TCP | 21 | TLAN | Management Systems, UCM, SRG | FTP Ctrl Link | File Transfers |
| Base | TCP | 22 | TLAN | Management Systems, UCM | SSH | Secure Interactive logon |
| Base | TCP | 23 | TLAN | Remote Management Systems | TELNET | Insecure Interactive logon |
| Base | TCP | 80 | TLAN, TLAN-nodeIP | Management Stations | http | Web Interface |
| Base | TCP | 443 | TLAN, TLAN-nodeIP | Management Stations, UCM members (not VxWorks) | https | Web Interface |
| | TCP | 636 | TLAN | UCM Primary, Backup | LDAPS protocol for LDAP replication | requires X.509 client certificate for mutual authenticati |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | on, uses FQDN |
| Base | TCP | 705 | TLAN | Internal | SS-Subagent | Loopback Interface Only |
| Base | TCP | 2000 | TLAN | Management Stations | Gryphon | Web Interface |
| Base | TCP | 3306 | TLAN | Internal | MySQL | Local Database Access |
| Base | TCP | 6666 | TLAN | CS, SS, VGMC, MGC, UCM | Config Process | Used for SNMP and NTP configuration propagation. |
| UCM | TCP | 8193 | TLAN | UCM Primary, Backup, Members (not VxWorks) | jboss-jms | FQDN is used |
| Base | TCP | 15086 | TLAN | | Gryphon | pcap Control |
| Base | TCP | 25100-25200 | TLAN | ANY | FTP Data Ports | Typically handled using FTP connection tracking in the firewalls |
| UCM | TCP | 31000 | TLAN | UCM Primary, Backup | clustered JNDI Stub Download | FQDN is used |
| UCM | TCP | 31001 | TLAN | UCM Primary, Backup | clustered JNDI RMI queries | FQDN is used |
| UCM | TCP | 31002 | TLAN | UCM Primary, Backup | | FQDN is used |
| Base | TCP | 32768-61000 | TLAN | ANY | Ephemeral ports | Typically handled using TCP & FTP |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Source | Description | Comments |
|---|---|---|---|---|---|---|
| | | | | | | connection tracking in the firewalls |
| UCM | TCP | 45566 - 45568 | TLAN | UCM Primary, Backup | JGroup protocol | FQDN is used |
| Base | UDP | 53 | TLAN | | DNS | |
| Base | UDP | 123 | TLAN | Any | NTP, source port 123 | Time Synchronization |
| Base | UDP | 161 | TLAN | TM, SNMP Management Systems | SNMP query | It is recommended to use ELAN |
| Base | UDP | 514 | TLAN | Linux Elements | Syslog | |
| UCM | UDP | 1812 | TLAN | UCM Members | RADIUS | |
| Base | UDP | 15010 | TLAN | | AFS | |
| Base | UDP | 15011 | TLAN | | AFS | |
| Base | UDP | 33600-33699 | TLAN | UCM | Radius | Central Authentication. (source port 1812) |

# Telephony Manager port numbers

- MGMT = Management

**Table 121: Telephony Manager (TM) port numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | TCP | 20 | | FTP: Corporate directory and DBA | Microsoft default port |
| | TCP | 21 | | FTP: Corporate directory and DBA | Microsoft default port |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | TCP | 21 | | FTP: TM 3.0 | Microsoft default port |
| | TCP | 25 | | SMTP: Alarm notification | Microsoft default port |
| MGMT | TCP | 80 | any | HTTP Web CS, Desktop Services, Web telecom billing system | Microsoft default port |
| MGMT | TCP | 135 | any | Login | RPC, SCM used by DCOM |
| | UDP | 135 | | Login | RPC, SCM used by DCOM |
| MGMT | TCP | 139 | any | NetBEUI: Windows client file sharing | Microsoft default port |
| | UDP | 161 | | SNMP: Alarm management and maintenance | Microsoft default port |
| MGMT | UDP | 162 | any | SNMP: Alarm traps (LD117) and maintenance window | Microsoft default port |
| | TCP | 389 | | CND synchronization | Microsoft default port |
| | TCP | 513 | | Rlogin: Session Connect, System Terminal, Station Admin, CPND, list manager, and ESN. | Using netstat |
| | TCP | 636 | | CND synchronization | Microsoft default port (CND SSL) |
| MGMT | TCP | 1583 | any | Btrieve | Station Admin |
| MGMT | UDP | 1929:2057 | any | DBA note: 1 port per session | Session ports |
| | UDP | 2058:2185 | | Data ports | |
| MGMT | TCP | 3351 | any | Btrieve | Station Admin |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| MGMT | TCP | 5099 | any | RMI: TM 3.0 DECT | Using netstat command |
| MGMT | TCP | 4789 : 5045 (based on default port of 4789) | any | Virtual System Terminal: Note : VT uses 1 port per session. Start with 4789 | The base port can be changed from 4789 |
| | TCP | 8080 | | HTTP: Web station | Apache Tomcat Web server |

# IP Phone port numbers

**Table 122: IP Phone 200x, I20xx, and 11xx port numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | UDP | 4100 | Ethernet | UNIStim | is the TPS |
| | UDP | variable | Ethernet | RTP | specified by the TPS |
| | UDP | 5000 | Ethernet | Net 6 | |
| | UDP | 5200 | Ethernet | RTP | src from phone |
| | UDP | 5201 | Ethernet | RTCP | src from phone |

# Remote Office port numbers

**Table 123: Remote Office port numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| Remote Office | TCP | 12800 | TLAN | signaling | |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| Remote Office | UDP/RTP | 20480, 20482 | TLAN | RTP | voice |

# CallPilot port numbers

**Table 124: CallPilot port numbers**

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | TCP | 20 | | FTP | |
| | TCP | 21 | CLAN/ ELAN | FTP | |
| | TCP | 25 | CLAN/ ELAN | SMTP | |
| | TCP | 80 | CLAN/ ELAN | HTTP | WWW |
| | TCP | 135 | CLAN/ ELAN | RTP/DCOM | Location Service |
| | UDP | 135 | CLAN/ ELAN | RTP/DCOM | Location Service |
| | TCP | 137 | CLAN/ ELAN | NETBIOS | Name Service |
| | UDP | 137 | CLAN/ ELAN | NETBIOS | Name Service |
| | TCP | 138 | CLAN/ ELAN | NETBIOS | Datagram Service |
| | TCP | 139 | CLAN/ ELAN | NETBIOS | Session Service |
| | TCP | 143 | CLAN/ ELAN | IMAP2 | |
| | UDP | 161 | CLAN/ ELAN | SNMP | (if enabled) |
| | UDP | 162 | CLAN/ ELAN | SNMP trap | (if enabled) |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | TCP | 389 | CLAN/ ELAN | LDAP | |
| | TCP | 443 | CLAN/ ELAN | HTTP | over SSL |
| | TCP | 465 | CLAN/ ELAN | SSMTP | (Secure SMTP) |
| | TCP | 636 | CLAN/ ELAN | LDAP | over SSL |
| | TCP | 993 | | IMAP | over SSL |
| | TCP | 1025 | CLAN/ ELAN | MSDTC | |
| | TCP | 1026 | CLAN/ ELAN | MSDTC | |
| | TCP | 1027 | CLAN/ ELAN | Microsoft Distribute COM Services | |
| | TCP | 1028 | CLAN/ ELAN | Microsoft Distribute COM Services | |
| | TCP | 1029 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 1030 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 1031 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 1032 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 1036 | CLAN/ ELAN | CallPilot Middleware Maintenance Service Provider | |
| | TCP | 1037 | CLAN/ ELAN | CallPilot Call Channel Resource | |
| | TCP | 1038 | CLAN/ ELAN | CallPilot Multimedia Resource | |
| | TCP | 1039 | CLAN/ ELAN | CallPilot MCE Notification Service | |
| | TCP | 1040 | CLAN/ ELAN | CallPilot MCE Notification Service | |
| | TCP | 1041 | CLAN/ ELAN | CallPilot MCE Notification Service | established connection to |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | | | | | local ports 2019 |
| | TCP | 1042 | CLAN/ ELAN | CallPilot MTA | established connection to local ports 2019 |
| | TCP | 1045 | CLAN/ ELAN | CallPilot Access Protocol | established connection to local ports 2019 |
| | TCP | 1046 | CLAN/ ELAN | CallPilot SLEE | established connection to local ports 2019 |
| | TCP | 1047 | CLAN/ ELAN | IIS | |
| | TCP | 1048 | CLAN/ ELAN | IIS | |
| | TCP | 1095 | CLAN/ ELAN | CallPilot Blue Call Router | |
| | TCP | 1096 | CLAN/ ELAN | CallPilot Blue Call Router | established connection to local ports 2019 |
| | TCP | 1148 | CLAN/ ELAN | TAPI | established connection to port 8888 on the switch |
| | TCP | 1499 | | ODBC for reporter database | |
| | TCP | 2019 | CLAN/ ELAN | Dialogic CTMS | established connection to local ports 1041, 1042, 1045, 1046, 1096 |
| | TCP | 2020 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 5631 | CLAN/ ELAN | pcAnywhere data | |

| Task | L4 protocol (TCP/UDP) | Port number or range | Interface | Description | Comments |
|---|---|---|---|---|---|
| | UDP | 5000 | | Call Pilot AOS DCOM (RPC)*5 | |
| | TCP | 5000 | | Call Pilot AOS DCOM (RPC)*5 | |
| | TCP | 5631 | | pcAnywhere data | if installed |
| | UDP | 5632 | CLAN/ ELAN | pcAnywhere data | if installed |
| | TCP | 7934 | CLAN/ ELAN | IIS | |
| | TCP | 8000 | CLAN/ ELAN | Dialogic CTMS | |
| | TCP | 10008 | CLAN/ ELAN | CallPilot Access Protocol | |
| | TCP | 38037 | CLAN/ ELAN | msgsys Intel CBA:Message System | |
| | TCP | 56325 | CLAN/ ELAN | CallPilot SLEE | |

# Application Gateway (AG) 1000 port numbers

**Table 125: AG 1000 port numbers**

| Application Protocol | L4 protocol (TCP/UDP) | Port number or range | Description | Comments |
|---|---|---|---|---|
| Telnet | TCP | 23 | Connection to Signaling Server to obtain DN | Voice mail applications |
| SMTP | TCP | 25 | Connection to SNMP server for message forwarding | Visual voice mail |
| HTTP | TCP | 80 | HTTP service port | General |
| HTTP | TCP | 80 | Broadcast Server push port | Broadcast server |
| IMAP | TCP | 143 | Connection to IMAP | Visual voice mail |
| SNMP | TCP | 161 | SNMP service prot | |

| Application Protocol | L4 protocol (TCP/UDP) | Port number or range | Description | Comments |
|---|---|---|---|---|
| LDAP | TCP | 389 | Connection to LDAP server | Voice mail applications |
| LDAP | TCP | 389 | Message forwarding | Visual voice mail |
| HTTPS | TCP | 443 | Smart agent service port | Smart agent |
| Syslog | UDP | 514 | Syslog service port | |
| Proprietary | TCP | 5000 | RUDP/UNIStim port for signaling with phones | Voice office applications |
| HTTP | TCP | 8080 | Outbound connection to a proxy server | |
| HTTPS | TCP | 9001 | AG admin tool service port | General |
| Proprietary | TCP | 9005 | Design studio configuration port | General |
| HTTP | TCP | 9998 | Broadcast Server push port | |
| Proprietary | TCP | 44443 | GXAS service port | IP phone 2007 |
| RTP | TCP | 50004 | RTP traffic for Broadcast Server | |
| RTCP | UDP | 50005 | RTCP receive port for monitoring RTP traffic statistics | Voice office applications |
| HTTP | TCP | 9014, 9025 | AG cluster communications port | General |
| RTP | UDP | 20480:20511 | RTP receive ports for visual voice mail | Visual voice mail and zone paging |
| Proprietary | TCP | configurable | Connection to property management system | Guest service |

# Contact Center port numbers

For Contact Center port numbers, see Symposium documentation.

# TLAN subnet stateless packet filtering

Table 126: TLAN subnet : Stateless packet filtering configuration on page 387 describes a stateless packet filtering configuration. The primary intent of this configuration is to secure management access to the Communication Server 1000 system using the TLAN subnet.

The table rules are for the TLAN subnet only. IP Phones are assumed to be deployed on client subnets throughout the IP network. All other TCP and UDP ports that run on the TLAN network interfaces are for system control traffic, which should not be sent through the packet filter. Optionally, drop all management traffic into the TLAN subnet.

**Table 126: TLAN subnet : Stateless packet filtering configuration**

| Rule # | Task App/ Interface | Source IP address | Source TCP/ UDP port | Dest. IP address | Protocol type | Dest. TCP/ UDP port | Action | Description |
|---|---|---|---|---|---|---|---|---|
| **System Management** | | | | | | | | |
| 1 | System MGMT | MGMT | ignore | TLAN subnet | any | any | Forward | Allow MGMT System |
| 2 | System MGMT | any | ignore | TLAN subnet | TCP | 21 | Drop | FTP |
| 3 | System MGMT | any | ignore | TLAN subnet | TCP | 23 | Drop | Telnet |
| 4 | System MGMT | any | ignore | TLAN subnet | TCP | 80 | Drop | HTTP Element Management |
| 5 | System MGMT | any | ignore | TLAN subnet | TCP | 111 | Drop | RPC |
| 6 | System MGMT | any | ignore | TLAN subnet | UDP | 162 | Drop | SNMP |
| 7 | System MGMT | any | ignore | TLAN subnet | TCP | 513 | Drop | rlogin |
| Firewall | | | | | | | | |
| 8 | Default Rule | any | ignore | TLAN subnet | UDP | any | Forward | Default Action |

# TLAN subnet stateful packet filtering

Table 127: TLAN subnet : stateful packet filtering on page 388 describes rules for a stateful firewall only; they do not apply to a non:stateful firewall. IP Phones are assumed to be deployed on client subnets throughout the IP network. All other TCP and UDP ports running on the TLAN network interfaces are for system control traffic, which should not be sent through the packet filter. Optionally, drop all management traffic into the TLAN subnet.

**Table 127: TLAN subnet : stateful packet filtering**

| Rule # | Task App/ Interface | Source IP add. | Source TCP/ UDP port | Dest. IP add. | Protocol type | Dest. TCP/ UDP port | Action | Description |
|---|---|---|---|---|---|---|---|---|
| System Management | | | | | | | | |
| 1 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 21 | Forward | FTP |
| 2 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 22 | Forward | SSH |
| 3 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 23 | Forward | Telnet |
| 4 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 80 | Forward | Element Manager |
| 5 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 513 | Forward | rlogin |
| 6 | System MGMT | MGMT | ignore | TLAN subnet | UDP | 162 | Forward | SNMP |
| VoIP Signaling | | | | | | | | |
| 7 | SigSvr / Gatekpr | any | ignore | TLAN subnet | TCP | 1720 | Forward | H.323 Signaling |
| 8 | SIP | any | ignore | TLAN subnet | TCP | 5060 | Forward | SIP Signaling (configurable) |
| 9 | Firmware Download | any | ignore | TLAN subnet | UDP | 69 | Forward | TFTP |
| 10 | H.323 | any | ignore | TLAN subnet | UDP | 1718 | Forward | H.323 Signaling |

| Rule # | Task App/ Interface | Source IP add. | Source TCP/ UDP port | Dest. IP add. | Protocol type | Dest. TCP/ UDP port | Action | Description |
|---|---|---|---|---|---|---|---|---|
| 11 | H.323 | any | ignore | TLAN subnet | UDP | 1719 | Forward | H.323 Signaling |
| 12 | TPS | any | ignore | TLAN subnet | UDP | 4100 | Forward | IP Phone 200x signaling |
| 13 | SIP | any | ignore | TLAN subnet | UDP | 5060 | Forward | SIP Signaling (configurable) |
| 14 | TPS | any | ignore | TLAN subnet | UDP | 5100 | Forward | IP Phone 200x signaling (configurable) |
| 15 | Firmware Download | any | ignore | TLAN subnet | UDP | 5105 | Forward | UNIStim FTP |
| 16 | TPS | any | ignore | TLAN subnet | UDP | 7300 | Forward | IP Phone 200x signaling |
| 17 | Virtual Office | any | ignore | TLAN subnet | UDP | 16500 | Forward | Virtual Office signaling Network connect server configurable |
| 18 | Virtual Office | any | ignore | TLAN subnet | UDP | 16501 | Forward | Virtual Office Signaling |
| 19 | SIP GW SPS | any | ignore | TLAN subnet | TCP | 5061 | Forward | SIP Signaling |
| VoIP Media | | | | | | | | |
| 20 | SMC | any | ignore | TLAN subnet | UDP | 5200: 5263 | Forward | RTP/RTCP voice media |
| Firewall | | | | | | | | |
| 21 | Firewall | any | ignore | TLAN subnet | ignore | any | Drop | Default Action |

# ELAN subnet packet filtering

Table 128: ELAN subnet : packet filtering on page 390 describes a packet filtering configuration suitable for a routable ELAN subnet. These filters are effective for stateless and stateful packet filters.

**Table 128: ELAN subnet : packet filtering**

| Rule # | Task (App./ Interface) | Source IP add. | Source TCP/ UDP port | Dest. IP add. | Protocol type | Dest. TCP/ UDP port | Action | Description |
|---|---|---|---|---|---|---|---|---|
| **System Management** | | | | | | | | |
| 1 | System MGMT | MGMT | ignore | ELAN subnet | TCP | 21 | Forward | FTP |
| 2 | System MGMT | MGMT | ignore | TLAN subnet | TCP | 22 | Forward | SSH |
| 3 | System Magma | MGMT | ignore | ELAN subnet | TCP | 23 | Forward | Telnet |
| 4 | System Magma | MGMT | ignore | ELAN subnet | TCP | 80 | Forward | HTTP Element Management |
| 5 | System Magma | MGMT | ignore | ELAN subnet | TCP | 513 | Forward | rlogin |
| 6 | System Magma | MGMT | ignore | ELAN subnet | UDP | 162 | Forward | SNMP query |
| 7 | System Magma | MGMT | ignore | ELAN subnet | UDP | 1929: 2185 | Forward | DBA for TM |
| System Signaling | | | | | | | | |
| 8 | System Signaling | CC6 | ignore | Call Server | TCP | 8888 | Forward | CC6 AML Link |
| **Note:** Rule 8 applies only to a system with a Contact Center 6 system using a single network interface to the Nortel server subnet. | | | | | | | | |
| Firewall | | | | | | | | |
| 9 | Firewall | any | Ignore | ELAN subnet | ignore | any | Drop | Default action |

# Appendix C: DHCP supplemental information

To understand how the IP Phones 200x and the IP Softphone 2050 acquire the needed network configuration parameters automatically, this chapter briefly describes the Dynamic Host Configuration Protocol (DHCP).

Read this section if you are unfamiliar with DHCP. Topics are helpful for the configuration and future maintenance of the DHCP server and ensure correct implementation with IP Phones.

DHCP is an extension of BootP. Like BootP, it operates on the client server model. However, DHCP has more message types than BootP. DHCP enables the dynamic allocation of IP addresses to different clients. It can be used to configure clients by supplying the network configuration parameters, such as gateway or router IP addresses.

DHCP also includes a lease system that controls the duration an IP address is leased to a client. The client can request a specific lease length, or the administrator can determine the maximum lease length. A lease can range from 1 minute to 99 years. When the lease is up or released by the client, the DHCP server automatically retrieves it and reassigns it to other clients, if necessary. This is an efficient and accurate way to configure clients quickly and saves the administrator from an otherwise repetitive task. IP addresses can be shared among clients that do not require permanent IP addresses.

## Navigation


Introduction to DHCP on page 392

- DHCP messages on page 392
- DHCP message format on page 392
- DHCP message exchange on page 393
- DHCP options on page 394
- Vendor Specific/Encapsulated option on page 394
- Site Specific option on page 394

IP acquisition sequence on page 395

- Case 1 on page 395
- Case 2 on page 396
- Case 3 on page 396

Multiple DHCPOFFER messages on page 397

IP Phone support for DHCP on page 398

Full DHCP on page 398

Partial DHCP on page 402

DHCP Auto Discovery on page 402s

# Introduction to DHCP

## DHCP messages

There are seven different DHCP messages. Each message relays certain information between the client and server. See Table 129: DHCP message types on page 392.

**Table 129: DHCP message types**

| DHCP Message Types | Description |
|---|---|
| DHCPDISCOVER | Initiates a client request to all servers. |
| DHCPOFFER | Offer from server following client request. |
| DHCPREQUEST | Requests a particular server for services. |
| DHCPAK | Notifies client that requested parameters can be met. |
| DHCPNAK | Notifies client that requested parameters cannot be met. |
| DHCPDECLINE | Notifies server that the offer is unsatisfactory and will not be accepted. |
| DHCPRELEASE | Notifies server that IP address is no longer needed. |

## DHCP message format

The DHCP message format shown in Figure 89: DHCP message format on page 393 is common to all DHCP messages. Each message consists of 15 fields– 14 fixed length fields and one variable length field. The fixed length fields must be the specified number of bytes, as indicated in the parentheses. If there is not enough data, or there is no data at all, zeros are used to fill in the extra spaces.

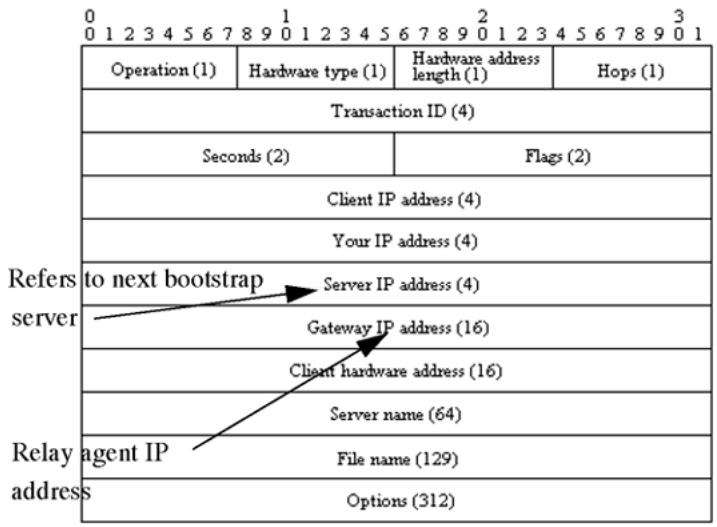


**Figure 89: DHCP message format**

The Options field is the only field with a variable length. It is optional, but very important, as it transports additional network configuration parameters. The DHCP options are the actual subfields used in a project.

## DHCP message exchange

For a client to receive services from a DHCP server, an exchange of DHCP messages between the client and server must take place. The sequence and types of DHCP message exchanged can differ, but the mechanism of acquiring and supplying information remains the same.

Usually the client initiates the exchange with a DHCP message broadcast. Using a broadcast enables the client to send messages to all servers on the network without having an associated IP address. The broadcast is local to the LAN, unless a DHCP relay agent is present to forward the packet.

At this point, the client has no information about the server or the IP address it is going to receive (unless it is requesting a renewal), so the fields in the DHCP message are empty. However, the client knows its own MAC address and includes it in the Client hardware address field. The client can also have a list of parameters it would like to acquire and can request them from the DHCP server by including the Parameter Request List option (Option Code 55) in the DHCPDISCOVER message.

When the DHCP server sees the broadcast, it responds by broadcasting its own DHCP message. The server, as it knows more about the network, can fill in most of the information in the message. For example, information such as the server IP address and gateway IP address are included in their respective fields. As the client does not have an IP address yet, the server uses the client MAC address to uniquely identify it. When the client sees the broadcast, it matches its MAC address against the one in the message.

## DHCP options

DHCP options are the subfields of the Options field. They carry additional network configuration information requested by the client, such as the IP address lease length and the subnet mask.

Each DHCP option has an associated option code and a format for carrying data. Usually the format is as follows:

Option code Length Data

There are two categories of DHCP options– standard and non-standard. The standard options are predefined by the industry. The non-standard options are user defined to fit the needs of a particular vendor or site.

There are a total of 255 DHCP option codes, where option codes 0 and 255 are reserved, 1 to 77 are predefined, 1 to 254 can be used for Vendor Specific Options, and 128 to 254 are designated for Site Specific Options. This arrangement enables future expansion and is used as a guideline for choosing option codes.

## Vendor Specific/Encapsulated option

The Vendor Specific DHCP options are vendor defined options for carrying vendor related information. It is possible to override predefined standard options; however, doing so can cause conflict when used with components that follow the industry standard.

A useful option is the standard Vendor Encapsulated option – code 43. It is used to encapsulate other DHCP options as suboptions. For example, the IP Phone 2004 requires Vendor Specific Voice Gateway Media Card information. The vendor, Nortel, decides to carry this information in one of several Site Specific options and then encapsulate it into option 43. As the information is specific to a Nortel product, it is vendor specific. After encapsulation, the information appears as one or more suboptions inside option 43, which the IP Phone decodes.

## Site Specific option

Another way to transport the Voice Gateway Media Card information is through Site Specific options. These are unused DHCP options that have not been predefined to carry standard information. Unlike the Vendor Specific options, the information transported is site specific and option codes 128 to 254 are used for encoding.

For Nortel IP Phones, the Voice Gateway Media Card information involves the location of the Voice Gateway Media Card in the network. This varies for different sites and can be implemented in a Site Specific option. If the Vendor Encapsulation option is used, the information is first encoded in a Site Specific option. Nortel has provided a list of five possible

Site Specific option codes to implement the Voice Gateway Media Card information. Only one of the five codes must be configured to carry the information, but the choice is available to offset the possibility that the option code chosen has been used for other purposes.

# IP acquisition sequence

This section focuses on the mechanics and sequence of the DHCP message exchange as the IP Phone uses DHCP for IP acquisition. Although the IP Phone requests many network configuration parameters as well as an IP address, the following cases focus on the concept of how instead of what information is acquired. The IP Phone is used as the sample client, but the situations apply to other DHCP clients as well.

## Case 1

Case 1 is a typical situation where an IP Phone 2004 requests services from a DHCP server, shown in the following figure.

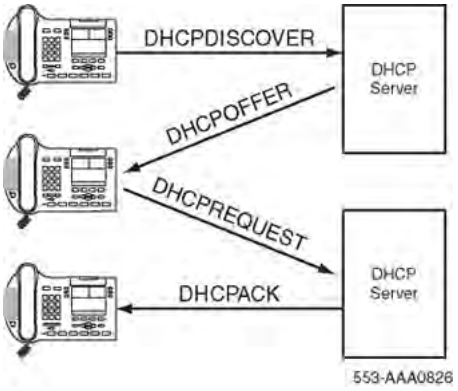


**Figure 90: IP acquisition phase: Case 1**

1. The IP Phone initiates the sequence by broadcasting a DHCPDISCOVER message.
2. A DHCP server on the network sees the broadcast, reads the message, and records the MAC address of the client.
3. The DHCP server checks its own IP address pools for an available IP address and broadcasts a DHCPOFFER message if one is available. Usually the server ensures the IP address is free using ARP or ping.
4. The IP Phone sees the broadcast and after matching its MAC address with the offer, reads the rest of the message to find out what else is being offered.
5. If the offer is acceptable, the IP Phone sends out a DHCPREQUEST message with the DHCP server IP address in the Server IP address field.

6. The DHCP server matches the IP address in the Server IP address field against its own, to find out to whom the packet belongs.
7. If the IP addresses match and there is no problem supplying the requested information, the DHCP server assigns the IP address to the client by sending a DHCPACK message.
8. If the final offer is not rejected, the IP acquisition sequence is complete.

## Case 2

The IP acquisition is unsuccessful if either the server or the client decides not to participate, as follows:

- If the DHCP server cannot supply the requested information, it sends a DHCPNAK message and no IP address is assigned to the client. This can happen if the requested IP address has already been assigned to a different client. See Figure 91: IP acquisition sequence: Case 2 on page 396.
- If the client decides to reject the final offer (after the server sends a DHCPACK message), the client sends a DHCPDECLINE message to the server, to tell the server the offer is rejected. The client must restart the IP acquisition by sending another DHCPDISCOVER message in search of another offer.

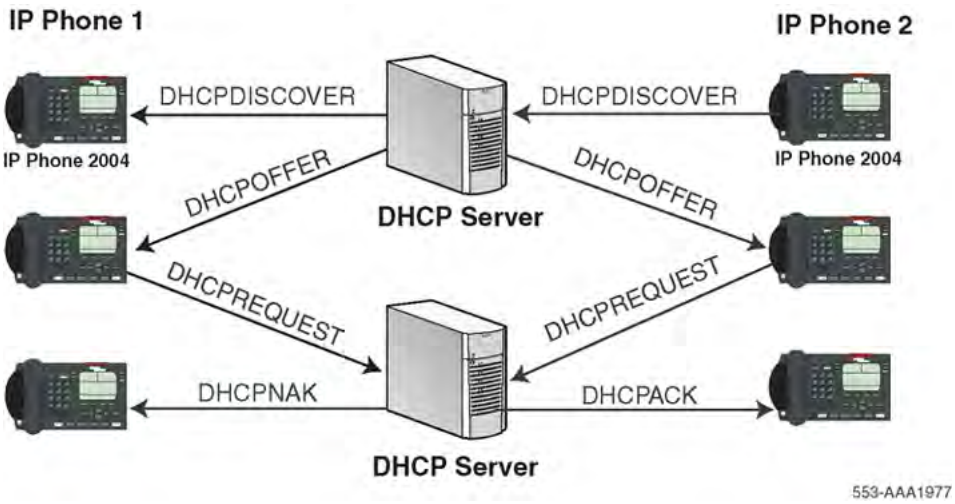


**Figure 91: IP acquisition sequence: Case 2**

## Case 3

When a client is finished with a particular IP address, it sends a DHCPRELEASE message to the server which reclaims the IP address. If the client requires the same IP address again, it can initiate the process as follows:

1. The IP Phone broadcasts a DHCPREQUEST to a particular DHCP server by including the server IP address in the Server IP Address field of the message. As it knows the IP address it wants, it requests it in the DHCP message.
2. The DHCP server sends a DHCPACK message if all the parameters requested are met.

Case 1 is similar to Case 3, except the first two messages have been eliminated. This reduces the amount of traffic produced on the network. See Figure 92: IP acquisition sequence: Case 3 on page 397.

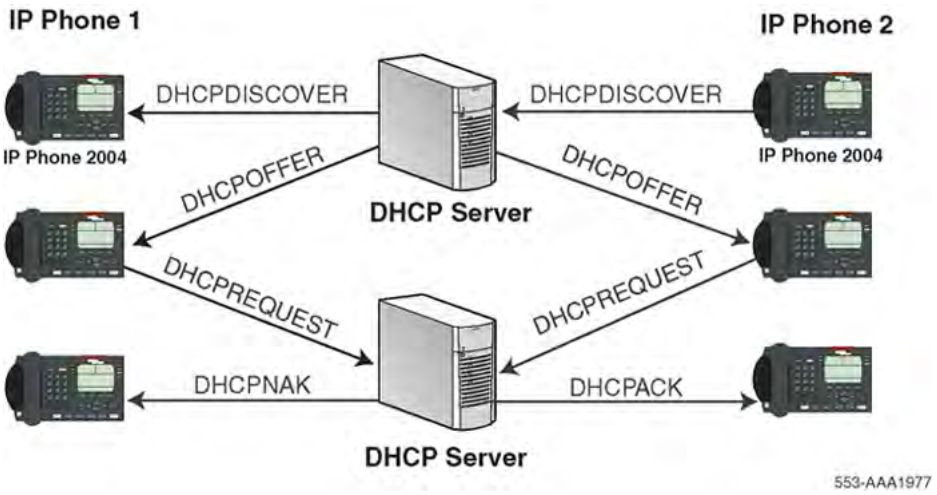


**Figure 92: IP acquisition sequence: Case 3**

## Multiple DHCPOFFER messages

In some networks, if more than one DHCP server is present, a client can receive multiple DHCPOFFER messages. Under these situations, the IP acquisition sequence depends on the client. The client can wait for multiple offers, or accept the first offer it receives. If it accepts multiple offers, it compares them before choosing one with the most fitting configuration parameters. When a decision is made, the message exchange is the same as if there is only one DHCP server and proceeds as in the previous cases. The servers that were not chosen to provide the service do not participate in the exchange.

For example, the IP Phone 2004 responds only to DHCPOFFER messages that have the same unique string identifier, (Nortel-i2004-A), as the IP Phone 2004. This string must appear in the beginning of the list of Voice Gateway Media Card parameters. Without this string, the IP Phone 2004 does not accept the DHPCOFFER, even if all parameters requested and Voice Gateway Media Card information are present. If no valid DHCPOFFER messages are sent, the IP Phone 2004 keeps broadcasting in search of a valid offer.

With multiple DHCP servers on the same network, a problem can occur if any two of the servers have overlapping IP address ranges and no redundancy. DHCP redundancy is a property of DHCP servers. Redundancy enables different DHCP servers to serve the same IP address

ranges simultaneously. Administrators must be aware that not all DHCP servers have this capability.

## IP Phone support for DHCP

This section covers the three uses of DHCP (Full, Partial, and VLAN Auto Discovery) by IP Phones 2002, 2004, and 2007.

An IP Phone 2004 aware DHCP server is needed only for the Full DHCP and VLAN Auto discovery. An IP Phone can obtain its IP address and subnet mask using Partial DHCP. The IP Phone 2004 aware part returns the Node IP and registration port number. In the case of the DHCP Auto Discovery, it returns the VLAN IDs. Separate DHCP vendor specific entries are needed for the Full DHCP data and the VLAN Auto Discovery data. When using VLAN Auto Discovery, both Full DHCP and VLAN Auto Discovery must be configured. Full DHCP and Auto VLAN are implemented as separate functions in the IP Phone firmware. However, in practice, Full DHCP and Auto VLAN are frequently used together.

## Full DHCP

DHCP support in the IP Phone requires sending a Class Identifier option with the value (Nortel-i2004-A) in each DHCP DHCPOFFER and DHCPACK message. Additionally, the telephone checks for either a Vendor Specific option message with a specific, unique to Nortel IP Phone 2004, encapsulated subtype, or a Site Specific DHCP option.

In either case, an IP Phone 2004-specific option must be returned by the IP Phone 2004 aware DHCP server in all Offer and Acknowledgement (ACK) messages. The IP Phone uses this option's data it to configure the information required to connect to the TPS.

The DHCP response is parsed to extract the IP Phone IP address, subnet mask, and gateway IP address. The Vendor Specific field is then parsed to extract the Server 1 (minimum) and optional Server 2. By default, Server 1 is always assumed to be the primary server after a DHCP session.

For the IP Phone to accept Offers/Acks, the messages must contain all of the following:

- A router option (requires a default router to function)
- A subnet mask option
- A Vendor Specific or Site Specific option as specified below.
  - Initial DHCP implementation required only the Vendor Specific encapsulated suboption. In interoperations testing with Windows NT (up to Service Release 4), it was discovered that Windows NT does not properly adhere to RFC 1541. As a result this option is not possible. The implementation was changed to add support for either Vendor Specific suboptions or Site Specific options. This new extension has been tested and verified to work with Windows NT.
  - The site specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for Site Specific use by the DHCP RFCs.

## Format for IP Phone 2004 Terminal DHCP Class Identifier Field

All IP Phones (IP Phones 2x and IP Softphone 2050) fill in the Class ID field of the DHCP Discovery and Request messages with the following:

Nortel-i2004-A Where:

- ASCII encoded, NULL (0x00) terminated
- unique to IP Phone 2004
- -A is the unique identifier for this version

## Format for IP Phone 2004 Terminal DHCP Encapsulated Vendor Specific Field

This suboption must be encapsulated in a DHCP Vendor Specific Option (see RFC 1541 and RFC 1533) and returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone to accept these messages as valid.

The IP Phone parses this option data and uses it to configure the information required to connect to the TPS.

**Note:**

Either this encapsulated suboption must be present, or a similarly encoded site specific option must be sent. See Format of the Encapsulated Vendor Specific Suboption field on page 400. Configure the DHCP server to send one or the other but not both.

**Note:**

The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

## Format for IP Phone 2004 Terminal DHCP Site Specific option

This option uses the reserved for Site Specific use DHCP options (number 128 to 254, see RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone to accept these messages as valid.

The IP Phone pulls the relevant information out of this option and uses it to configure the IP address and so on for the primary and (optionally) secondary TPSs.

**Note:**

Either this Site Specific option must be present or a similarly encoded vendor specific option must be sent (as previously described). For example, configure the DHCP server to send one or the other but not both.

**Note:**

The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

## Format of the Encapsulated Vendor Specific Suboption field

The format of the Encapsulated Vendor Specific Suboption field is as follows:

- Type (1 octet): 5 choices are provided (0x80, 0x90, 0x9d, 0xbf, 0xfb [128, 144, 157, 191, 251]), which allow the IP Phone to operate when one or more value is already in use by a different vendor. Select only one TYPE byte.
- Length (1 octet): variable—depends on message content.
- Data (length octets): ASCII based with the following format:

  Nortel-i2004 -A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.

  The components in this string are described in Table 130: Encapsulated Vendor Specific Suboption field on page 400.

**Table 130: Encapsulated Vendor Specific Suboption field**

| Parameter | Description |
|---|---|
| Nortel-i2004-A | Uniquely identifies this as the Nortel option<br>Signifies this version of this specification |
| iii.jjj.kkk.lll:ppppp | Identifies the IP address port for server (ASCII encoded decimal) |
| aaa | Identifies the Action for server (ASCII encoded decimal, range 0–255) |
| rrr | Identifies the retry count for server (ASCII encoded decimal, range 0–255). This string can be NULL terminated although the NULL is not required for parsing. |
| ACSII symbols | The comma (,) is used to separate fields<br>The semicolon (;) is used to separate Primary from Secondary server information<br>The period (.) is used to signal the end of the structure |

Table 131: Nortel option string on page 400 shows the pieces of the Nortel option string. The Nortel designator Nortel-i2004-A is separated from the Connector Server stings using a comma. The Connect Servers are separated using a semicolon.

**Table 131: Nortel option string**

| Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr. |
|---|

| Nortel Class Identifier Field | comma | Primary Connect Server | semicolon | Secondary Connect Server | period |
|---|---|---|---|---|---|
| Nortel-i2004-A | , | iii.jjj.kkk.lll:ppppp,aaa,rrr | ; | iii.jjj.kkk.lll:ppppp,aaa,rrr | . |

**Note:**

aaa and rrr are ASCII encoded decimal numbers with a range of 0 to 255. They identify the Action Code and Retry Count, respectively, for the associated TPS server. Internally to IP Phone 2004 they are stored as 1 octet (0x00 to 0xFF). Note that these fields must be no more than 3 digits long.

**Note:**

The string enables the configuration of information for two Connect Servers. One Connect Server exists for each IP node. In the typical system configuration of a single IP node, only the primary Connect Server is required. In this case, the primary Connect Server string must be ended with a period (.) instead of a semicolon (;). For example, Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr.

If the secondary Connect Server portion of the string is specified, then the string information is typically the same as the primary Connect Server information. For example: Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr.

When the Enhanced Redundancy for IP Line Nodes feature is used, two different Connect Server strings can be configured, separated with a semicolon (;). This enables the telephone to register to two different nodes. For more information about the Enhanced Redundancy for IP Line Node feature, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

**Note:**

Action code values (0 to 255): 1—UNIStim Hello (currently only this type is a valid choice) all other values (0, 2 to 255)—reserved

**Note:**

iii,jjj,kkk,lll are ASCII encoded, decimal numbers representing the IP address of the server. They do not need to be 3 digits long as the period (.) and colon (:) delimiters guarantee parsing. For example, 001, 01, and 1 would all be parsed correctly and interpreted as value 0x01 internal to the IP Phone 2004. Note that these fields must be no more than three digits long each.

**Note:**

ppppp is the port number in ASCII encoded decimal. The port number must be configured as 4100.

**Note:**

In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

### Format of the DHCP Site Specific field

The format of the DHCP Site Specific field is the same as the format of the Encapsulated Vendor Specific Suboption field. See Format of the Encapsulated Vendor Specific Suboption field on page 400.

## Partial DHCP

Partial DHCP is the default DHCP response from a DHCP server that has not been configured to provide the Vendor Specific information. Using Partial DHCP, an IP Phone can obtain its IP address, subnet mask, and gateway IP address. The remainder of the configuration information is manually entered at the IP Phone.

## DHCP Auto Discovery

DHCP Auto Discovery must be used only if the telephone and PC are:

- connected to the same Layer 2 switch port through a three-port switch
- on separate subnets

The DHCP server can be configured to supply the VLAN information to the IP Phones. The server uses the Site Specific option in the DHCP offer message to convey the VLAN information to the IP Phone.

Configuring a DHCP Server for VLAN Discovery is optional. This configuration is done in addition to that for Full DHCP configuration and it is required only when configuring the VLAN Auto Discovery.

This method is based on the assumption that the default VLAN is the data VLAN and the tagged VLAN is the voice VLAN. Enter the voice VLAN information into the data VLAN and subnet's DHCP server. Enter the standard IP Phone configuration string into the voice VLAN and subnet DHCP server pool.

The following definition describes the IP Phone 2004-specific, Site Specific option. This option uses the reserved for Site Specific use DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the IP Phone to accept these messages as valid. The IP Phone extracts the relevant information and uses the information to configure itself.

### Format of the field

The format of the field is: Type, Length, Data.

## Type (1 octet):

There are five choices:

- 0x80 (128)
- 0x90 (144)
- 0x9d (157)
- 0xbf (191)
- 0xfb (251)

Providing a choice of five types enables the IP Phones to operate if a value is already in use by a different vendor. Select only one Type byte.

## Length (1 octet):

This is variable; it depends on message content.

## Data (length octets):

ASCII based format: VLAN-A:XXX+YYY+ZZZ. where:

- VLAN– A: – uniquely identifies this as the Nortel DHCP VLAN discovery. Additionally, the –A signifies this version of this spec. Future enhancements could use –B for example.
- ASCII plus (+) or comma (,) is used to separate fields.
- ASCII period (.) is used to signal the end of the structure.
- XXX, YYY and ZZZ are ASCII encoded decimal numbers with a range of 0 to 4095. The number is used to identify the VLAN IDs. There are a maximum of 10 VLAN IDs can be configured in the current version. The strings none or NONE means no VLAN (default VLAN).

The DHCP OFFER message carrying VLAN information is sent from the DHCP server without a VLAN tag. However, the switch port adds a VLAN tag to the packet. The packet is untagged at the port of the IP Phone.

# Appendix D: Setup and configuration of DHCP servers

## Navigation


- Install a Windows NT 4 or Windows 2000 server on page 405
- Configure a Windows NT 4 server with DHCP on page 405
- Configure a Windows 2000 server with DHCP on page 408
- Install ISC DHCP Server on page 413
- Configure ISC DHCP Server on page 413
- Install and configure a Solaris 2 server on page 416


## Install a Windows NT 4 or Windows 2000 server

To configure the Windows NT 4 or Windows 2000 server, follow the instructions provided in the installation booklet. After completion, install the latest Service Pack and make sure the DHCP Manager is included.

**Important:**

If you install a Windows NT 4 server with Service Pack 4 or later, follow the installation instructions included with the server hardware.

## Configure a Windows NT 4 server with DHCP

Configure a Windows NT 4 server with DHCP services using the DHCP Manager provided. Follow the steps in Launching the DHCP Manager In Windows NT 4 on page 406 to launch the DHCP Manager.

### Launching the DHCP Manager In Windows NT 4

1. Click the Windows **Start** button.
2. Select **Programs, Administrative tools (Common), DHCP Manager**.

   The DHCP Manager window appears.
3. Double-click **Local Machines** in the left pane.

   The Create Scope: (Local) window appears.

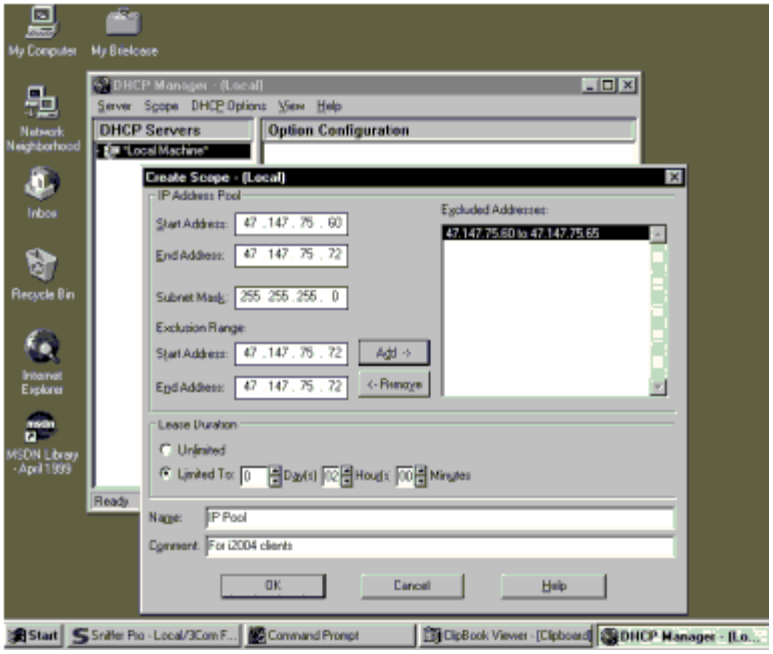


**Figure 93: Define a new scope**

4. Create and fill in the information.
5. Click **OK** when finished.
6. In the DHCP Manager: (Local) window, highlight the scope that serves the IP Phones clients.
7. From the **DHCP Options** menu, select **Default Values**.

   The DHCP Options: Default Values window appears.
8. Click the **New** button. See Figure 94: Define the Nortel specific option on page 407.

   The Change Option Type window appears.

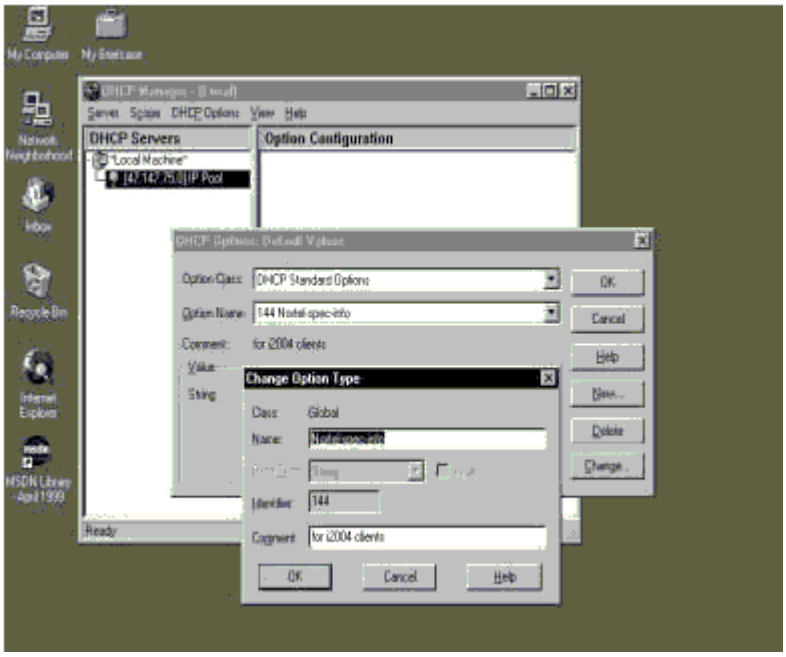


**Figure 94: Define the Nortel specific option**

9. Fill in the information and click **OK** when finished.
10. Click **OK** again.
11. From the DHCP Manager: (Local) window, highlight the scope to which you want to add the DHCP options.
12. From the **DHCP Options** menu, select **Scope**.

    The DHCP Options Scope window appears.
13. Choose standard DHCP options from the left panel and click **Add** to add them to the right panel.

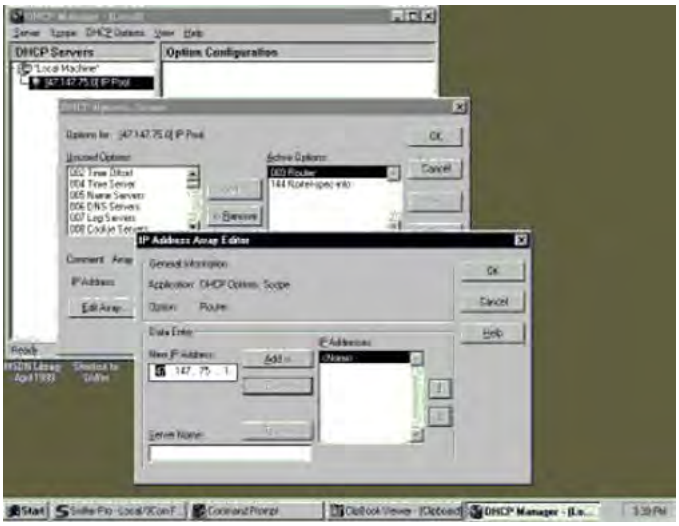


**Figure 95: Add standard DHCP options to scope**

14. Click **Edit Array** .

    The IP Address Array Editor window appears.

15. Edit the default value and then click **OK**.
16. Click OK again.
17. From the DHCP Manager: (Local) window, highlight the scope that needs to be activated.
18. From the **DHCP Options** menu, select **Scope**.

    The DHCP Options Scope window appears.

19. Click **Activate**.

    The light bulb next to the scope should turn yellow. See Figure 96: Activate the scope on page 408 on Figure 96: Activate the scope on page 408.

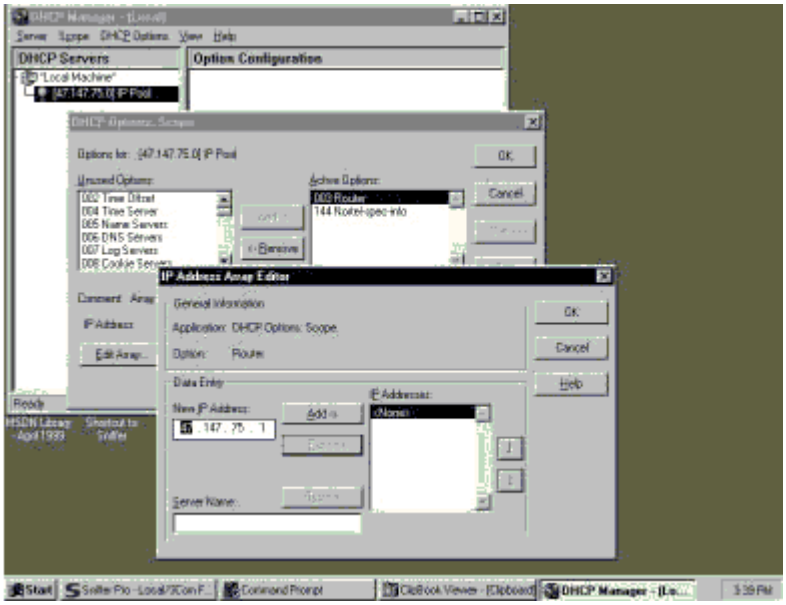


**Figure 96: Activate the scope**

If DHCP Auto Discovery needs to be configured, see DHCP Auto Discovery on page 402.

# Configure a Windows 2000 server with DHCP

Configure a Windows 2000 server with DHCP services using the DHCP Manager.

## Launching the DHCP Manager in Windows 2000

1. Click the Windows **Start** button.
2. Select **Programs, Administrative Tools, DHCP**.

   The administrative console window appears. See Figure 97: Windows 2000 administration console on page 409.

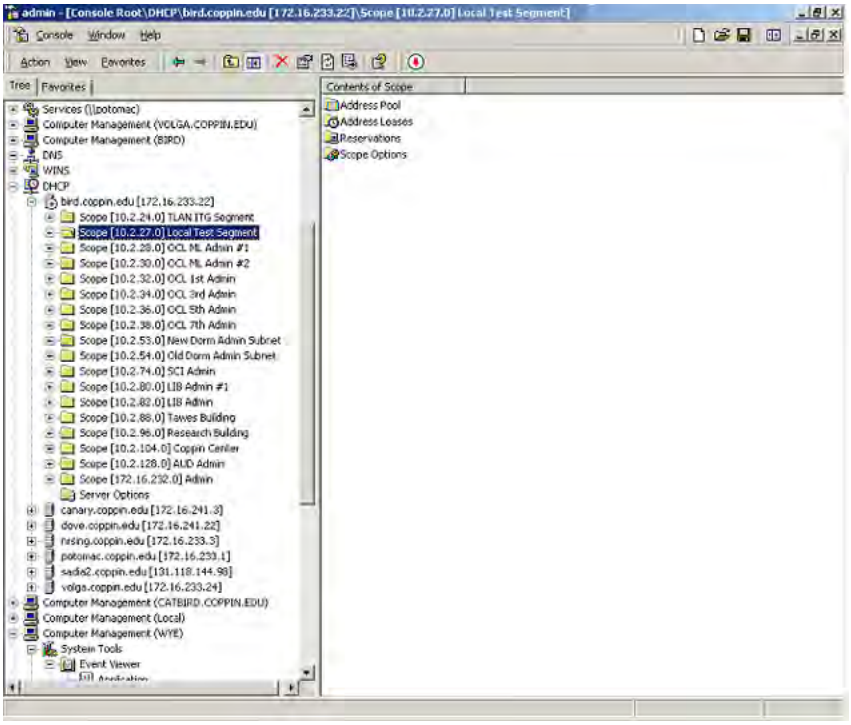


**Figure 97: Windows 2000 administration console**

3. Highlight DHCP and expand the DHCP option (if it is not already expanded).
4. Highlight the server and right-click to display the shortcut menu.
5. Select **Set Predefined Options** from the menu.

   Do not go into the Vendor Specific settings. The Predefined Options and Values window appears.

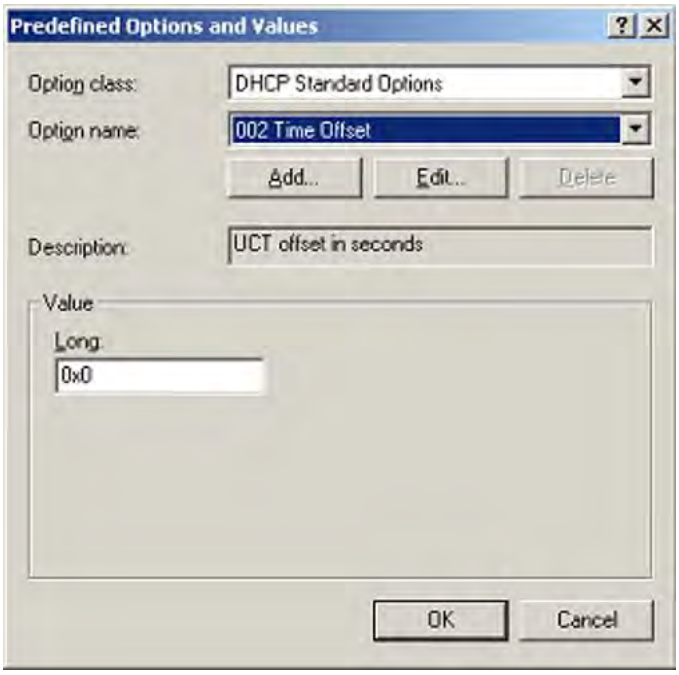


**Figure 98: Predefined Options and Values**

6. Click **Add**.

   The Change Option Type window appears.

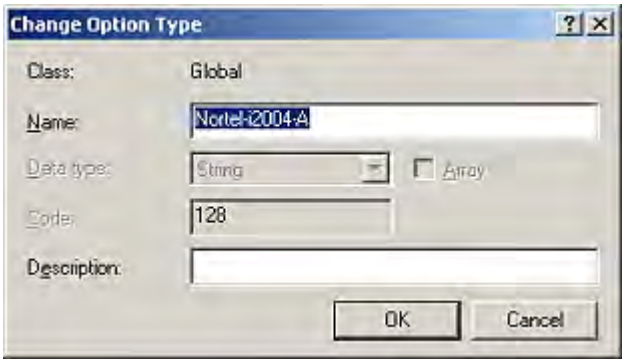


**Figure 99: Change Options Type**

7. In the Name box, enter the desired **Name**.

   For this example, the name of **Nortel-i2004-A** is entered. See Figure 99: Change Options Type on page 410.

8. From the Code box, select Code 128.
9. Click **OK** to close the window.

   The Predefined Options and Values window appears with the string 128 Nortel-i2004-A entered in the Option name field.

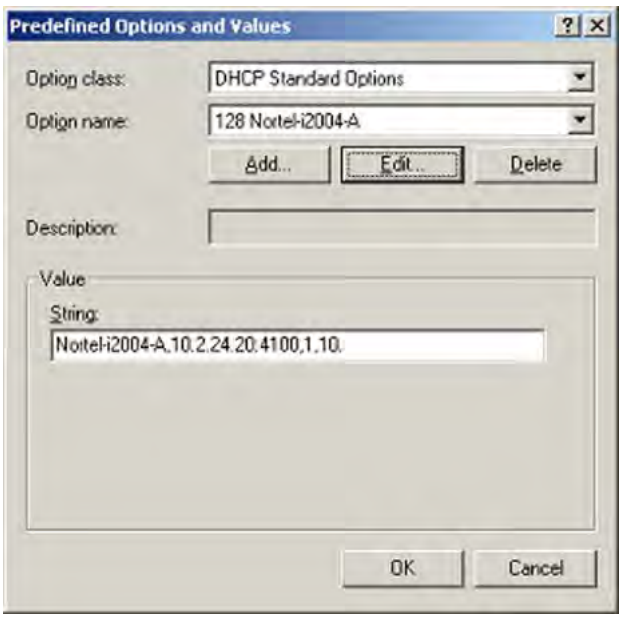


**Figure 100: Predefined Options and Values with data entered**

10. In the **Value** area, enter the following string in the **String** field: **Nortel-i2004-A,x.x.x.x:4100,1,10**; using the following guidelines:

    - The string is case-sensitive.
    - Place a period at the end of the string.
    - Commas are used as separators.
    - Spaces are not allowed.
    - x.x.x.x is the IP address of the IP Telephony node.
    - If it is a BCM, replace the 4100 value with 7000.

11. Click **OK**.
12. Click the scope **(Scope [x.x.x.x] name)** to expand, and then click **Scope Options**.

    The Scope Options window appears.

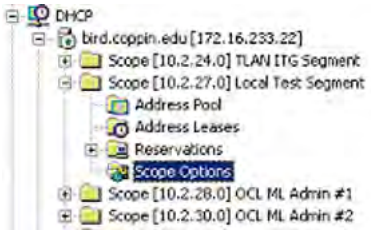


**Figure 101: Scope and Scope Options**

13. On the **General** tab, scroll to the bottom of the list and select the **128 Nortel-i2004-A** check box.

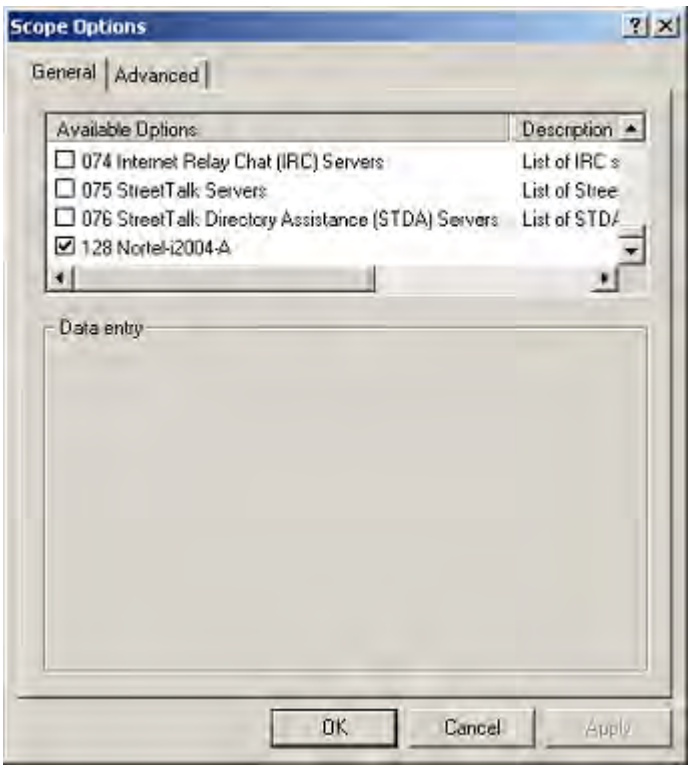


**Figure 102: Scope Options**

14. Click **OK**.

    The Option Name and Value appear in the right pane of the administrative console window.

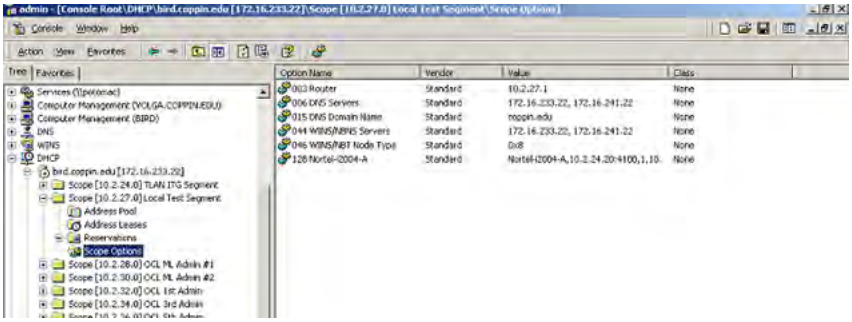

**Figure 103: Options Name and Value in administrative console**

If DHCP Auto Discovery needs to be configured, see DHCP Auto Discovery on page 402.

# Install ISC DHCP Server

To configure the ISC DHCP server, read the README file and follow the instructions about how to compile, make, and build the server. After setup is complete, configure the server by following the description in Configure ISC DHCP Server on page 413.

**⚠ Caution:**

Although, Windows NT 4 has the Vendor Encapsulation Option (option code 43), do not use it to encode the Voice Gateway Media Card information needed by the IP Phones. Windows NT 4 enables only 16 bytes of data to be encapsulated, which is not enough to encode all the information needed.

Windows NT 4 DHCP server transmits any user defined option associated within a scope, if the client requests it. It cannot distinguish among different types of clients; therefore, it cannot make decisions based on this information. It is impossible to create a client specific IP address pool/scope.

# Configure ISC DHCP Server

To configure the ISC DHCP server, a text based configuration process is used. Configuration is done by adding definitions and declarations in the dhcpd.conf file located at /etc/. Various man files are provided that contain information about how to configure the server, configure the lease system, use options and conditions, and run the server. Obtain the dhcpd.conf.man5 file in the server directory and read it carefully. It provides explanations about relevant topics, as well as the location of other man files to read for additional information.

## Configure ISC DHCP to work with the IP Phones

There is a particular format for encoding the Voice Gateway Media Card information. In addition to the configuration statements provided, other network and subnet declarations must also be included in the configuration file.

Read the man files and use Example 1: Configuration file on page 414to configure the ISC DHCP server to work with the IP Phones. Also, a copy of the configuration file used for this project is provided at the end of this section.

### Configuring the ISC DHCP server

1. Configure the server to identify a client correctly as an IP Phone 2001, IP Phone 2002, IP Phone 2004, or IP Phone 2007. Using a match statement with a conditional if enclosed inside a class declaration, as follows:

   class "i2004-clients"{

match if option vendor-class-identifier = 4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;}

The Hex string represents the text string Nortel-i2004-A. If the vendor class identifier obtained from the client DHCPDISCOVER message matches this Hex encoded string, then the server adds this client to the i2004-clients class. After a client is classified as a member of a class, it must follow the rules of the class.

2. Declare a pool of IP addresses exclusively for the members of the i2004-clients class. The pool declaration is used to group a range of IP addresses together with options and parameters that apply only to the pool.
3. Restrict access to the pool using the allow or deny statement to include or exclude the members of a particular class.

   For example, the following configuration code enables only members of i2004-clients to use this IP address pool:

```
pool{
     allow members of "i2004-clients";
           range 47.147.75.60 47.147.75.65;
           option routers 47.147.75.1;
# Nortel special string
option vendor-encapsulated-options
80:3d:4e:6f:72:É;}
```

   **Note:**

   If a client is not a member of this class, it is not assigned an IP address from this pool, even if there are no other available IP addresses.

4. There are two methods to encode the necessary information for the IP Phone 2004 client using the vendor-encapsulated-options option (as in the previous example) to encode the information as a sub option or define a Site Specific option to carry the necessary information. To define a Site Specific option:

   Give a declaration in the form of the name of the option, the option code, and the type of data it carries outside any pool or network declarations. For example, option Nortel-specific-info code 144 = string; OR replace the vendor-encapsulated option inside the pool statement with the definition, option Nortel-specific-info = "Nortel É";

   The DHCPOFFER message from the ISC server must include the Voice Gateway Media Card information if the client is an IP Phone 2001, IP Phone 2002, IP Phone 2004, or IP Phone 2007.

   If DHCP Auto Discovery needs to be configured, see DHCP Auto Discovery on page 402.

## Example 1: Configuration file

The following format must be used for encoding the Voice Gateway Media Card information. In addition to the configuration statements provided, other network and subnet declarations must also be included in the configuration file. As mentioned in the beginning of this section, read the man files and use the following example as a guideline:

```
    # File name: dhcpd.conf
```

```
     # Location: /etc/
     # Description: Configuration file for ISC dhcpd server
    # Author: Cecilia Mok
     # Date: September 24, 1999
# Global option definitions common for all supported
# networks...
default-lease-time 300;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 255.255.255.255;
# Defining Nortel-specific option for IP Phone 2004 client
option my-vendor-specific-info code 144 = string;
# Declaring a class for IP Phones type 2002, 2004, and 2007
# clients.
# Add new clients to the class if their Class Identifier
# match the special IP Phone 2004 ID string.
class "i2004-clients"
{
     match if option vendor-class-identifier =
4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;
}
# Declaring another class for PC clients
class "pc-clients"
{}
# Declaring a shared network
# This is to accommodate two different subnets on the same
# physical network; see dhcpd.conf.man5 for more details
shared-network "myNetwork"
{
      # Declaring subnet for current server
      subnet 47.147.77.0 netmask 255.255.255.0
      {}
# Declaring subnet for DHCP clients
      subnet 47.147.75.0 netmask 255.255.255.0
      {
      # Pool addresses for i2004 clients
      pool
        {
        allow members of "i2004-clients";
      range 47.147.75.60 47.147.75.65;
option routers 47.147.75.1;
# Nortel special string
      option Nortel-specific-info = "NortelÉ";
}
      default-lease-time 180;
      max-lease-time 300;
}
```

Before you start the server, create a blank dhcpd.leases file in the /etc/ directory, which is the same location as the dhcpd.conf file. To start the server, go to /var/usr/sbin/ and type:

```
./dhcpd
```

To run in debug mode, type:

```
./dhcpd –d –f
```

# Install and configure a Solaris 2 server

## Install a Solaris 2 Server

To configure the Solaris 2 server, consult the accompanying manual and online documentation.

## Configure a Solaris 2 server

Follow the steps in Configuring a Solaris 2 server on page 416 to configure Solaris 2 with DHCP.

### Configuring a Solaris 2 server

1. Read the following man pages:
   - dhcpconfig
   - dhcptab
   - in.dhcpd

   There are also directions at the end of each page that refer to other sources that are helpful.
2. Collect information about the network, such as subnet mask and router/Media Gateway and DNS server IP addresses as specified and ensure this information is current.
3. Log on as **root** and invoke the interface by typing **dhcpconfig** at the prompt.

   A list of questions is presented and the administrator must supply answers that are then used to configure the DHCP server.

   **Note:**
   Solaris 2 uses a text-based interface for configuring DHCP services.

   **Note:**
   If DHCP Auto Discovery needs to be configured, see DHCP Auto Discovery on page 402.

### Configuring Solaris 2 to work with IP Phones

1. Perform one of the following:

Create a symbol definition for defining a Site Specific option by typing the following in the dhcptab configuration table located at /etc/default/dhcp:

```
NI2004  s  Site,128,ASCII,1,0
```

OR

Use the dhtadm configuration table management utility by typing the following command at the prompt:

```
dhtadm -A -s NI2004 –d 'Site,128,ASCII,1,0'
```

Where-

NI2004:symbol name s:identify definition as symbol Site:Site Specific option 128:option code ASCII:data type 1:granularity 0:no maximum size of granularity, that is, infinite

2. Create a Client Identifier macro by performing one of the following:
   - Enter the following:

     ```
     Nortel-i2004-A   m:NI2004="NortelÉ":
     ```

   - Use the dhtadm command:

     ```
     dhtadm  -A  -m  Nortel-i2004-A  -d   ':NI2004="NortelÉ":'
     ```

3. Invoke the DHCP services on the Solaris server by entering the following command at the prompt:

   ```
   in.dhcpd,
   ```

   Specify –d and/or –v options for debug mode. See man page in.dhpcd for more details.

An example of the tables used in this project is as follows:

## DhcptabTable

```
Locale                  m    :UTCoffst=18000:
nbvws286                m
:Include=Locale:LeaseTim=150:LeaseNeg:DNSdmain=ca.nortel.com:/
                              DNSserv=47.108.128.216 47.211.192.8 47.80.12.69:
47.147.75.0             m    :NISdmain=bvwlab:NISservs=47.147.64.91:
47.147.64.0             m
:Broadcst=47.147.79.255:Subnet=255.255.240.0:MTU=1500:/
Router=47.147.64.1:NISdmain=bvwlab:NISservs=47.147.64.91:
#
```

NI2004 s Site,128,ASCII,1,0

Nortel-i2004-A m:

NI2004="Nortel-i2004-A,47.147.75.31:4100,1,5;47.147.77.143:4100,1,5.":

## Network Table

01006038760290 00 47.147.65.198 47.147.74.36 944600968 nbvws286

0100C04F662B6F 00 47.147.65.199 47.147.74.36 944600959 nbvws286



Comments? infodev@avaya.com

# Appendix E: Change CS 1000 IP addresses

This section contains the recommended sequence and tasks you need to change all the IP addresses on a CS 1000 system and associated applications.

Follow these steps to change the IP addresses of a CS 1000 system:

### Changing IP addresses of CS 1000

1. Create an inventory list of the following network components:
    - Record the IP address and network masks for NRS.
    - Record the IP address for devices that currently use the NRS to route calls
    - For Call Servers, create an inventory of all devices and include IP address and network masks information for the following:
        - IP Phones
        - Gateway Controllers
        - MC32S and MC32 media cards
    - For applications, create an inventory of all applications connected to the Call Servers. Include the IP address and network mask for the following:
        - CallPilot
        - Contact Center applications
        - Recorded Announcement (RAN) trunk interface
        - Application gateways
2. Document the new IP addresses of all devices.
3. Change the security domain IP addresses.

    For information about changing the security domain, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

    **Note:**

    If you change the IP address of a VxWorks-based device (Call Server, Gateway Controller, Media Card), you must configure the device as part of the security domain to update the new IP address and public key-IP address mapping.
4. Register Linux base elements under the new IP address if you use the same Fully Qualified Domain Name (FQDN). Registration must take place after you reboot the Linux server.

    **Note:**

    Check the DNS server and the /etc/hosts file on the Linux servers to ensure the new FQDN-to-IP address mapping is accurate.

If the FQDN of the Linux server changes, you must log on to the Linux server locally and configure the Linux server as part of the security domain. Security configuration ensures that all elements published from the member server are in sync with the new FQDN. For information about local logon to a Linux server, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*. For information about security configuration, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

5. If a Domain Name Service (DNS) server is used to resolve FQDNs in the security domain and the member server's FQDN changes, ensure you update the DNS server to use the member server's new FQDN. If DNS is not used and you are using a CS 1000 Linux-based server, UCM's internal DNS server is used.

   **Note:**

   For non-CS 1000 products, ensure the primary server has an entry for the new member FQDN in the local /etc/hosts file or the C:\WINDOWS\system32\drivers\etc\hosts file.

6. Change the IP address of the NRS server. For more information about changing the NRS server's IP address, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

   **Note:**

   The Signaling Servers (virtual trunk gateways) do not attempt to register to the NRS until both the Call Server IP address and Signaling Server IP addresses have been changed. (VTRK will not attempt to register to the NRS until the PBX link is up).

7. Devices that register to an NRS server must change the NRS IP address on the device. The devices attempt to register with the new IP address of NRS.

8. Change IP Phone IP addresses. For more information about changing IP Phone IP addresses, see *IP Phones Fundamentals, NN43001-368*.

   **Note:**

   The IP Phones attempt to register to the Signaling Server, but the Signaling Server (TPS) ignores them until the Signaling Server is registered to the Call Server (the PBX link is up).

9. To change the IP address of a Gateway Controller, complete the following steps:

   - Change the IP address configuration of Gateway Controllers that are registered to the Call Server.
   - Change the Gateway Controller TLAN IP address, mask, or gateway using Element Manager.
   - Change the Gateway Controller ELAN IP address, mask, or gateway and the Call Server IP address using Element Manager.

     The Gateway Controller retrieves the new configurations from the Call Server and reboots with the new configurations.

     The Gateway Controller registers to the Call Server when the Call Server is configured with the new Gateway Controller ELAN IP address.

     If the Gateway Controller ELAN IP address was changed, you must also change the Gateway Controller ELAN IP address in LD 97 on the Call Server for the configured superloop.

**Note:**

If the Gateway Controller is not registered to the Call Server prior to step 4 on page 419, you must use MGCSETUP to change the ELAN and Call Server IP addresses in LDB1.

10. To change the Call Server IP address, complete the following steps:

    a. Create an inventory list of all the servers configured in the corresponding CS 1000 system in Deployment Manager.

    b. Delete the corresponding CS 1000 system. For more info about adding and deleting CS 1000 systems, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

    c. Change the Call Server IP address.

       For information on changing the IP address on a VxWorks Call Server, see *Avaya Communication Server 1000E Installation and Commissioning, NN43041-310*.

       To change the IP on a Linux Call Server, you must change the ELAN IP of the Linux server. For more information see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

    d. Register Call Server in the security domain under the new IP address.

       **Note:**

       Skip this step if Call Server is co-resident with the Primary UCM server.

    e. Recreate the CS 1000 system. Use the inventory list you created at the beginning of this step and add the previously configured servers.

    f. Update the IP Telephony node information on the Element Manager IP Telephony Nodes page with the new Call Server IP address. See *Element Manager System Reference - Administration, NN43001-632* for details.

11. Change the Signaling Server IP address. For more information about changing the Signaling Server IP address, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

    - Validate the IP Phone registration.
    - Validate the Signaling Servers that have registered to the NRS.

12. Use the inventory list from 1 on page 419 to validate all devices that have registered to the NRS.

    **Note:**

    If a device does not register properly and loses connection to the CS 1000E:

    - Use a direct serial port connection and print the IP addresses and network masks of the device.
    - Validate the expected destination device's IP address and network mask with the inventory list from step 1.

13. Change the applications' IP addresses and validate that they have registered to the Call Server.

# Index


## Numerics

100BaseT full-duplex .....178
802.1Q .....201

## A

autonegotiate .....178

## C

CAC (Call Admission Control) .....152

## D

Delay variation .....213
DHCP .....200, 405
Dynamic Host Configuration Protocol .....200

## F

fall back threshold algorithm .....213
Fax services .....164
feedback .....213
filter connector .....178
full-duplex .....178

## G

G.711A .....213
G.711U .....213

## H

half-duplex 10BaseT .....178

## I

IPE Module Backplane I/O ribbon cable assemblies 178
ITG shell .....178

## J

jitter buffer .....213
Jitter Buffer .....153
jitter buffers .....155

## N

Network Management Systems .....62
Network modeling .....111
NMS .....62

## O

OM .....210
Operational Measurement .....210

## P

packet loss evaluation .....158
ping .....211

## R

Reduce packet errors .....157
RMON .....62, 120

## S

shell .....178
Sniffer .....57
SNMP .....62
Subnet configurations .....182

## T

tlanDuplexSet .....178
tlanSpeedSet .....178
traceroute .....211

## Z

Zone .....73