Meridian 1
Succession 1000
Succession 1000M
Succession 3.0 Software

Data Networking for Voice over IP

Document Number: 553-3001-160
Document Release: Standard 1.00
Date: October 2003

Produced in Canada

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

Revision history

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Data Networking Guidelines (553-3023-103).

Contents

About this document 9
Subject 9
Applicable systems 9
Intended audience 11
Conventions 12
Related information 13

Overview 15
Contents 15
Introduction 16
Network convergence 18
Network design 20
Quality of Service (QoS) 21
Network performance measurement and monitoring 22
Available tools 24
Achieving satisfactory voice quality 25

Network design assessment 27
Contents 27
Introduction 28
Network modeling 28
LAN and WAN platforms 34
Protocols in use 36

Link speeds 38
Link types 39
Link utilization assessment 41
Traffic flows in the network 43
Service level agreements 45
Summary 45

QoS mechanisms 47
Contents 47
Introduction 49
The QoS process 54
WAN QoS mechanisms 58
Layer 2 (Ethernet) QoS 68
Layer 3 QoS 74
Layer 4 (TCP/IP) classification 83
Policy management 84
VoIP call admission control 84

Network performance measurement 95
Contents 95
Introduction 97
Network performance measurement tools 106
Network availability 107
Bandwidth 108
Delay 125
Jitter 140
Packet loss 145
Network delay and packet loss evaluation example 149
Estimate voice quality 151
Does the intranet provide expected voice quality? 159

Server LAN design 161
Contents 161
Introduction 163
Ethernet requirements 167
IP address requirements 174
Redundant LAN design 182
Succession Call Server to remote Succession
Media Gateway requirements 189
Sample system layout 195
Configuration of the DHCP server 199
Contents 199
Overview 200
i2002 and i2004 Internet Telephones, and i2050 Software Phone 200
Configuring the DHCP server to support full DHCP mode 203
Operating the VoIP network 215
Contents 215
System management 216
Network monitoring 219
Network Management 225
Appendix A: Configuring the
BPS / Baystack 450 229
Contents 229
Creating telephony VLANs on the Business Policy Switch 230
QoS configuration for the BPS/Baystack 450 253
Baystack 450 802.1p user priority configuration 260
Appendix B: Configuring QoS on the
Passport 8600 261
Contents 261

DiffServ core network with BPS 2000 261

DiffServ core network with Baystack 450 264

QoS on the Passport 8600 265

Layer 3 QoS mechanisms 270

Appendix C: Optivity Policy Services 275

Contents 275

Policies 275

Appendix D: Port number tables 283

Contents 283

Introduction 283

Appendix E: Subnet mask conversion from CIDR to dotted decimal format 299

Overview 299

Appendix F: DHCP supplemental information . . . 301

Contents 301

Introduction to DHCP 302

IP acquisition sequence 307

Internet Telephone support for DHCP 312

Appendix G: Setup and configuration of DHCP servers 321

Contents 321

Configure a Windows NT 4 server with DHCP 322

Configure a Windows 2000 server with DHCP 328

Install ISC's DHCP Server 334

Configure ISC's DHCP Server 334

Install and configure a Solaris 2 server 340

List of terms 343

About this document

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

Subject

The purpose of this document is to ensure that the data network has been properly provisioned to support IP Telephony services.

Note on legacy products and releases

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

http://www.nortelnetworks.com/

Applicable systems

This document applies to the following systems:

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

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

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

System migration

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

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

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

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

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

Note the following:

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

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

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

Intended audience

This document is intended for network deployment personnel responsible for ensuring that the data network has been properly provisioned to support IP Telephony services.

This document assumes that the reader understands general data networking technology and has a fundamental understanding of IP networking technologies and protocols.

Conventions

Terminology

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

- Meridian 1
- Succession 1000
- Succession 1000M

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

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

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

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

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

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *IP Peer Networking* (553-3001-213)
- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)
- *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232)
- *Installing and Configuring OTM* (553-3001-280)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331)
- *Succession 1000 Element Manager: System Administration* (553-3001-332)
- *IP Trunk: Description, Installation, and Operation* (553-3001-363)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Telephones and Consoles: Description* (553-3001-367)
- *Internet Terminals: Description* (553-3001-368)
- *Software Input/Output: Maintenance* (553-3001-511)
- *Small System: Planning and Engineering* (553-3011-120)
- *Large System: Planning and Engineering* (553-3021-120)
- *Succession 1000 System: Planning and Engineering* (553-3031-120)
- *i2004 Internet Telephone User Guide*

Online

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

http://www.nortelnetworks.com/

CD-ROM

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

Overview

Contents

This section contains information on the following topics:

Introduction 16

Network convergence 18
Voice applications 19

Network design 20
Server LAN design 21
Configuring the DHCP server 21

Quality of Service (QoS) 21
QoS versus bandwidth 22

Network performance measurement and monitoring 22
Application requirements 23

Available tools 24

Achieving satisfactory voice quality 25

Introduction

This NTP discusses a number of areas which must be addressed when building a converged multi-media network. These include:

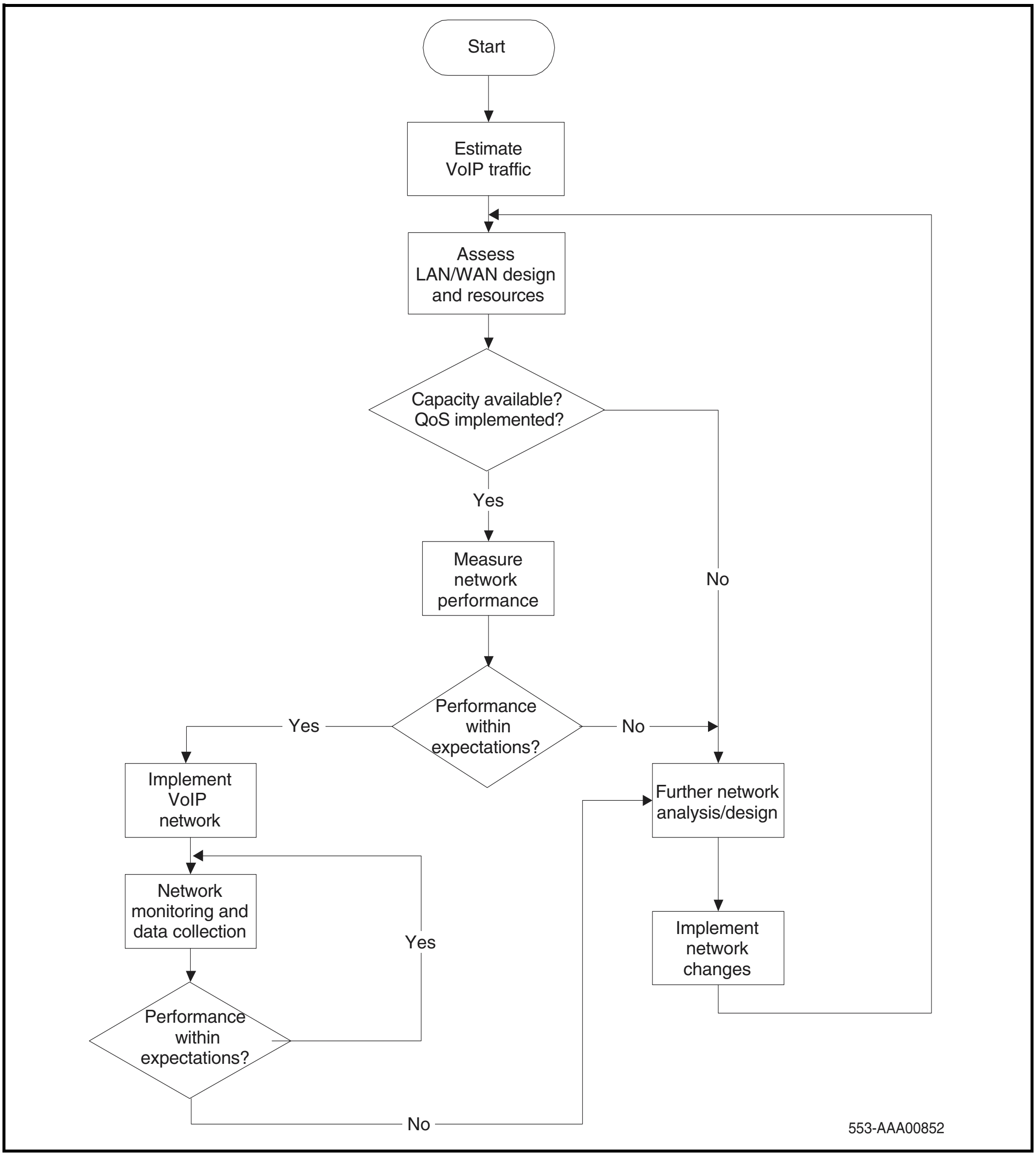
- network design
- performance
- Quality of Service (QoS)
- operations

Many considerations are important when creating and maintaining a converged network. It is important to gain a detailed understanding of the design of the existing data network before implementing 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 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 NTP.

Figure 1 on page 17 is a logical view of the steps necessary to assess a network for Voice over Internet Protocol (VoIP) readiness. This network assessment flow chart is used as a guideline for this NTP and the network engineering process.

Figure 1
Network assessment flow chart


Start
Estimate VoIP traffic
Assess LAN/WAN design and resources
Capacity available? QoS implemented?
Yes
No
Measure network performance
Performance within expectations?
Yes
No
Implement VoIP network
Further network analysis/design
Network monitoring and data collection
Yes
Implement network changes
Performance within expectations?
No
553-AAA00852

Network convergence

In the last several years, there has been a move toward network convergence. Network convergence is the transport of all services over the same network structure. Previously, there were separate, dedicated networks for different types of applications, such as voice, video, and data. Today, many of these applications are being merged into a single network to reduce operating costs and increase ease of operation.

A traditional enterprise may 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)
- multi-protocol network, including such varied protocol types as Internetwork Packet Exchange (IPX) and AppleTalk

Many enterprises look to converged networks to achieve cost and operational efficiency. A converged network mixes different types of traffic, each with different requirements. This creates difficulties that must be addressed. When different types of applications had their own dedicated networks, QoS technology played a smaller role. Dedicated network traffic was similar in behavior, and the networks were fine-tuned to achieve an application’s required 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. Such performance is obtained on a circuit-switched network. A best-effort data network has varying amounts of packet loss and variable delay usually caused by network congestion. A packet-based data network usually is the opposite of what is needed by a voice application.

Implementing QoS mechanisms helps to address this issue.

Voice applications

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

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

IP networks do not guarantee that bandwidth will be available 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 (see page 21), the following can occur:

- Voice packets experience variable, unpredictable amounts of delay.
- Voice packets are dropped when the network is congested.
- Voice packets can re-ordered by the network if the packets arrive out of sequence.

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

Network design

It is important to have a detailed understanding of the converged networks design. This can be done by answering the following questions:

- Is a physical network diagram available for the data and voice network?
  - Is a logical diagram for both networks available? The logical diagram can be provided by the SNMP Network Management System (NMS).
- What Local Area Network (LAN)/Wide Area Network (WAN) platforms are currently installed?
  - Do the currently installed platforms support some form of QoS?
- What types of links are in use?
  - Point-to-Point Protocol (PPP)
  - Frame Relay (FR)
  - Asynchronous Transfer Mode (ATM)
- What protocols are in use? What routing protocols are in use?
- What link speeds are in use on the LAN? What link speeds are in use on the WAN?
- What is the current utilization of those links?
  - What are the peak delays on the WAN links?
  - What is the current delay and packet loss?
- What is the current flow of data and voice traffic?

These are discussed more in the “Network design assessment” on page 27.

Server LAN design

Server LAN design for the system is discussed in the page 161. The topics covered include Layer 2 design, IP addressing, and server LAN redundancy.

Configuring the DHCP server

Nortel Networks' i200x Internet Telephones support automatic configuration using the Dynamic Host Configuration Protocol (DHCP). See page 199 for details on configuring the DHCP server.

Quality of Service (QoS)

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 is transmitted over a network, and has no assurances that the data will even be delivered at all.

Therefore, a means of providing guarantees is required. The purpose of QoS mechanisms is to 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 bandwidth available is only several hundred kbps. For example, data traffic could easily use all of the bandwidth available on link thereby causing voice quality problems. QoS mechanisms could be used to guarantee that network bandwidth is 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 on page 47.

QoS versus bandwidth

One approach to network engineering says that QoS is not needed; simply increasing bandwidth provides enough QoS for all applications. This theory also states that implementing QoS is complicated; adding bandwidth is easy. However, because of 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.

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 low latency. Latency is the length of time needed for information to travel through a network. High latency can significantly 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 elements:

- availability
- bandwidth
- delay
- jitter
- packet loss

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 95. “Operating the VoIP network” on page 215 also discuss the ongoing monitoring and management of measurement of the network.

Application requirements

Table 2 on page 23 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 2
Common application performance parameters

Application	Relative bandwidth demand	Sensitivity to		
		Delay	Jitter	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
E-mail	Low	Low	Low	High
File Transfer	Med	Low	Low	High

Available tools

Recommendation

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

For example:

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

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

Some of the Nortel Networks-recommended tools are highlighted throughout this document.

For a detailed list of many of the network administration tools available today, visit: http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#

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

Achieving satisfactory voice quality

A satisfactory level of perceived voice quality is achieved through the following:

- a properly-engineered network
- good network equipment and redundancy
- adequate bandwidth for peak usage
- use of QoS mechanisms
- ongoing monitoring and maintenance

If these elements are not present, VoIP performance suffers.

This document provides recommendations for the following:

- network design and configuration
- QoS mechanisms
- performance measurements
- operational monitoring and maintenance

Network design assessment

Contents

This section contains information on the following topics:

Introduction 28

Network modeling. 28

Physical and logical network diagrams 29

Sample IP network model 29

Typical network topology 30

Network Modeling tools 33

LAN and WAN platforms 34

Campus platforms. 34

Supported QoS mechanisms. 35

Bandwidth. 35

Security and QoS 36

Protocols in use 36

Routing protocols 36

LAN protocols 36

WAN protocols 37

Convergence 37

Mixing protocols 37

Link speeds 38

Link types 39

Point-to-point links (PPP). 39

Frame Relay (FR) 39

Asynchronous Transfer Mode (ATM) 40

Virtual Private Network (VPN) 40

Link utilization assessment 41
Assessing link utilization 41
Traffic flows in the network 43
Traceroute 43
Call Detail Record 44
Traffic study 44
Service level agreements 45
Summary 45

Introduction

It is important to gain a full understanding of the design of an existing data network before implementing a VoIP network. This section describes key issues to consider when creating a new converged voice and data network.

For example, it is very important to 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 that can be used to assess the VoIP network are described, as well as examples of logical connection diagrams for small, medium, and large campus networks.

Network modeling

Network analysis can be difficult or time-consuming if the intranet and the Succession 3.0 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 would 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 multi-site environment.

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

Sample IP network model

The Succession 1000, Succession 1000M, 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.

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

QoS mechanisms are recommended at 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.

If campus-distributed Succession Media Gateways 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.

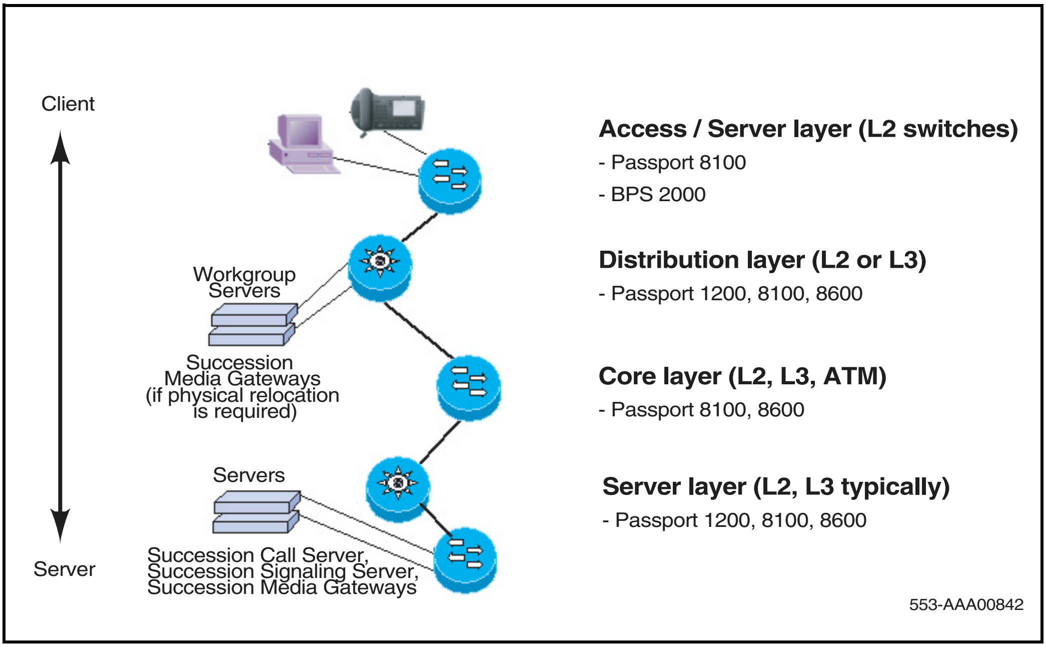
The following are planned based on the access and distribution layers' configuration:

- VLANs
- subnets
- QoS mechanisms for the Internet Telephones such as DiffServ and 802.1Q

Typical network topology

Figure 2 on page 30 provides a reference model for a campus network.

Figure 2
Campus network reference model


Client
Server
Workgroup Servers
Succession Media Gateways (if physical relocation is required)
Servers
Succession Call Server, Succession Signaling Server, Succession Media Gateways
Access / Server layer (L2 switches)
- Passport 8100
- BPS 2000
Distribution layer (L2 or L3)
- Passport 1200, 8100, 8600
Core layer (L2, L3, ATM)
- Passport 8100, 8600
Server layer (L2, L3 typically)
- Passport 1200, 8100, 8600
553-AAA00842

The following figures (Figure 3, Figure 4 on page 32, and Figure 5 on page 33) provide examples of logical connection diagrams for small, medium, and large campus networks. Other network designs can be used. The actual design that is implemented depends on many factors, including physical locations, size, and scalability.

Figure 3 illustrates an example of a small campus network design.

Figure 3
Small campus network example

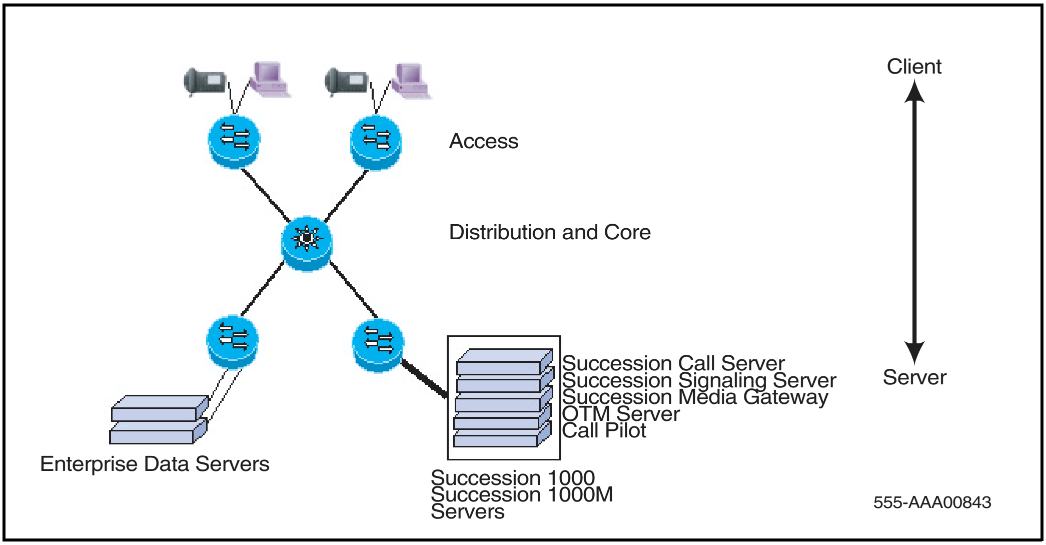


Figure 4 illustrates an example of a mid-size campus network design.

Figure 4
Mid-size campus network example

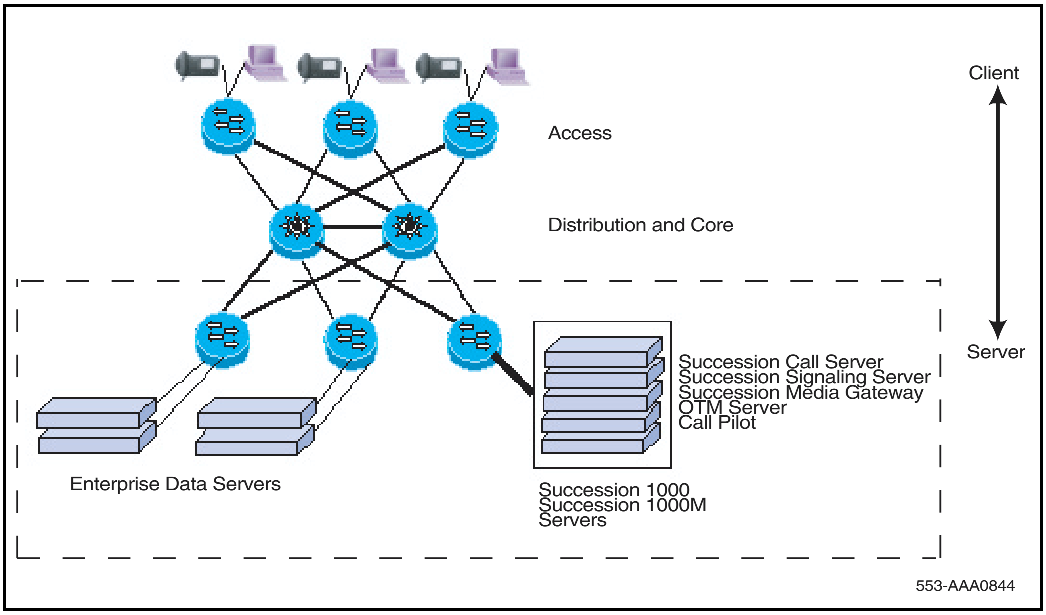
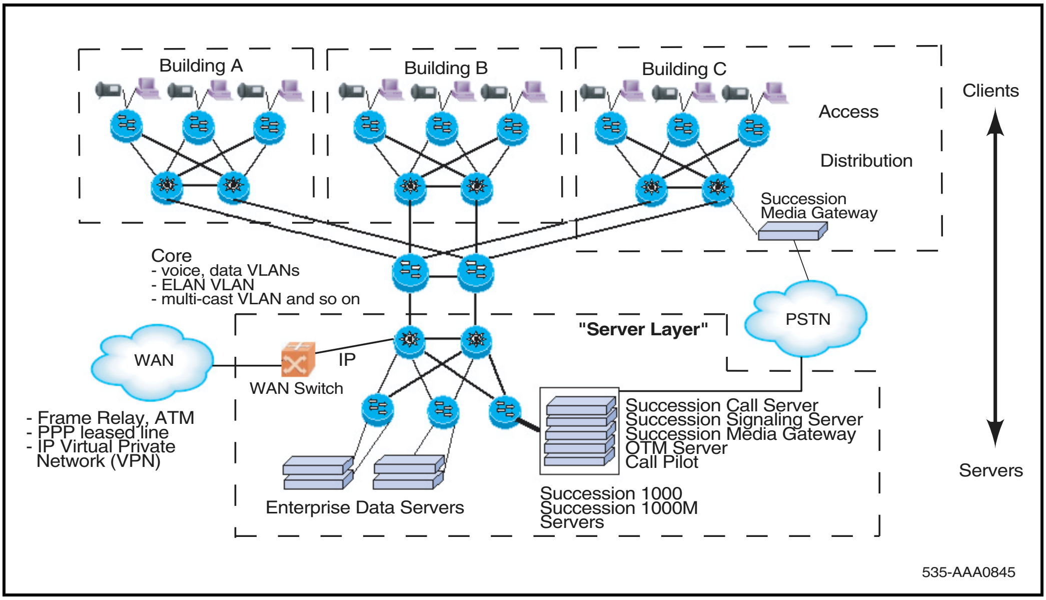


Figure 5 illustrates an example of a large campus network design.

Figure 5
Large campus network example



Recommendation

Nortel Networks recommends that a network be designed to accommodate a larger VoIP deployment than will be installed, and that network administrators monitor the network's data traffic on a regular basis.

Network Modeling tools

Contact your Nortel Networks sales representative if you require help determining a suitable Network Modeling solution.

LAN and WAN platforms

After determining the network topology, the next step is to 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, it is necessary to assess the network's bandwidth.

Campus platforms

It is important to document the platforms used in the campus. It is important to document 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 multi-gigabit Ethernet connections to a switched Layer 3 IP network.

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

Migrating 100 Mbps riser links to Gigabit Ethernet is suggested.

WARNING
All VoIP servers and Internet Telephones 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.

Supported QoS mechanisms

To ensure consistent voice quality, some form of QoS must be supported on the platforms that transport VoIP. There are several ways to provide QoS, including the following:

- bandwidth
- packet classification
- DiffServ
- fragmentation
- traffic shaping
- the use of the platforms queuing mechanisms

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

Bandwidth

It is important to note of the maximum packets per second forwarding rates of the platforms.

A LAN/Campus network’s elements usually consist of the following:

- 100 Mbps bandwidth to the desktop
- high performance closet switching
- devices such as the Business Policy Switch (BPS) connected to the core network
- multi-gigabit riser connections
- devices such as the Passport 8600 in the core

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

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.

Security and QoS

The following security features must be considered:

- firewalls
- Network Address Translation (NAT) (See "NAT" on page 349.)
- Secure Virtual Private Network (VPN) access through Secure Internet Protocol (IPSec) encryption. (See "IPSec" on page 349.)

Routers might use NAT and IPSec for remote network users who connect to the network through the public internet, using IPSec encryption. A firewall connection might also be in place. The network designer must consider the security policy in force and see if the ports required for VoIP can go through the firewall.

Protocols in use

When assessing 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 and/or RMON probes, and analyze the results.

Routing protocols

It is important to note the routing protocols used within the network as they have the potential to effect network availability.

LAN protocols

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

WAN protocols

Routing protocols in the WAN can be very important when considering how VoIP calls will be routed and how quickly fail-over occurs. When planning a VoIP network, be aware of what situations trigger a routing table update with respect to the routing protocol. This helps when predicting 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 re-converge 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 running over IP can set the frames with the “may fragment” bit to 1, which prevents fragmentation. As part of the overall assessment process, the network analysis on the LAN can determine if any applications have this bit setting.

Link speeds

Link speeds in a WAN environment are usually low compared to a LAN. When considering VoIP in a WAN environment, link speeds are an important consideration, as speeds under 1 Mbps are subject VoIP to serialization delay. This can impair deployment. When smaller VoIP packets travel over a network that typically has 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 also have several mechanisms available.

If the link speed and packet size are considered, the serialization delay introduced can be predicted. See "Serialization delay" on page 129 for more information.

Recommendation

Nortel Networks recommends beginning with an MTU size of 232 bytes for links under 1 Mbps, adjusting 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 Mbps of bandwidth going to the desk, with multi-Gigabit riser links. Since 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)

PPP links are direct point-to-point links. PPP links give the network operator the most control for QoS. They provide dedicated bandwidth. A meshed topology is more expensive with PPP links, but PPP links have great flexibility about where they terminate, once the network is in place.

Frame Relay (FR)

Frame Relay networks provide more flexibility when the requirements include a full meshed topology. They 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 set 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 re-transmitted.

It is important to 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 (ATM)

ATM transport can provide a Constant Bit Rate (CBR) service, dedicating a channel with a fixed bandwidth based on the application's needs.

Using ATM as a transport for VoIP adds overhead associated with ATM. A G.711 codec with 20 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 the frame to be segmented to fit into multiple cells. This adds an additional 10-15% 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 (VPN)

A Virtual Private Network (VPN) is a network that 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 VPN information, refer to Nortel Network's Contivity Solutions at http://www.nortelnetworks.com/solutions/ip_vpn/.

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 on utilization of a given WAN link.

Other methods of assessment include the use of imbedded Remote Monitoring (RMON) and external RMON probes installed for the purpose of gathering 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. This is done to minimize the maximum queuing delay that the VoIP traffic experiences over low-bandwidth connections.

Assessing link utilization

WAN links are the highest repeating expenses in the network and they often cause capacity problems in the network. 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 installing the network.

IMPORTANT!

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

To assess the link utilization, follow the steps in Procedure 1 on page 42.

Procedure 1
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 ICMP (Internet Control Messaging Protocol) on page 106.
3. Determine the current utilization of the WAN links. Note the reporting window that appears in the link utilization report. For example, the link's use can be averaged over a week, a day, or an hour.
4. Obtain the busy period (peak hour) use of the link.
5. Since 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 that capacity usage remains below pre-determined level.

   For example, a planning policy states that the use of a 56 Kbps 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 Kbps link would therefore be 28 Kbps, and for the T1, 1.2288 Mbps. 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 re-routed.
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 not only to a physical capacity, but also to 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 Kbps.

End of Procedure

Traffic flows in the network

Identify traffic flows in the network by using an existing NMS (Network Management System) or using 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 day, week, and month to determine the highest utilization periods.

Once traffic flows are identified, determine bandwidth requirements, using tools such as a VoIP bandwidth calculator. Ask your Nortel Networks representative for the VoIP bandwidth calculator spreadsheet. For more information, see "VoIP Bandwidth Demand Calculator" on page 115.

Available traffic tools

There are many tools available for assessing network traffic flows. Some of these include:

- Traceroute
- Call Detail Record
- Traffic study

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. It must instead throw away the packet and return to the originating IP address an ICMP "time exceeded" message. Traceroute uses this mechanism 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. Then Traceroute sends out a datagram with a TTL of 2. This 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 an UDP Port number unlikely to be in use at the destination (usually > 30,000). This causes the destination to return a “port unreachable” ICMP packet. This identifies 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 and day of week/month must be considered to ensure consistent voice quality.

For more information, refer to *Call Detail Recording: Description and Formats* (553-3001-350).

Traffic study

Traffic is a measurement of a specific resource's activity level. LD 02 has been reserved for scheduling and selecting 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
- queuing activity (Off-Hook Queuing and Callback Queuing) and the length of time users queue, on average

For more information on traffic studies, refer to:

- *Traffic Measurement: Formats and Output* (553-3001-450)
- LD 02 in *Software Input/Output: Administration* (553-3001-311)

Service level agreements

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

Whether you are a home user on a cable or DSL connection, or a large network customer using Frame Relay, you 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 you receive the CIR rate that you pay for when you lease a connection.

Exercise caution if service level agreements are not available.

Summary

It is crucial to fully understand the existing data network design before implementing a VoIP network. There are many considerations that are important when creating a new converged voice and data network. Network design tools are available to assist with this process.

QoS mechanisms

Contents

This section contains information on the following topics:

Introduction 49
Traffic mix 50
TCP traffic behavior 51
QoS problem locations 51
Campus networks 53
Wide Area Networks 53
The QoS process 54
Classification 54
Marking 55
Queuing 55
Weighted Random Early Detection (WRED) 56
Packet prioritization and schedulers for VoIP 56
WAN QoS mechanisms 58
Bandwidth demand 58
Bandwidth example 60
Fragmentation and interleaving 60
PPP fragmentation and interleaving 61
IP fragmentation 62
Packet reordering 64
Traffic Shaping 64
RTP header compression 66
PPP QoS 66
Frame Relay QoS 66
ATM QoS 67

Layer 2 (Ethernet) QoS . . . 68
MAC address . . . 68
IEEE 802.1Q . . . 68
VLAN ID. . . . 70
802.1p user priority bits . . . 71
802.1p configuration . . . 71
Port prioritization . . . 72
3-port switch port prioritization . . . 72
Layer 3 QoS . . . 74
IP address classification . . . 74
DiffServ for VoIP. . . . 75
Trust configuration. . . . 77
Voice signaling and media DSCPs . . . 77
Setting DSCP values . . . 78
Mapping DSCP to 802.1Q . . . 79
Example. . . . 80
OTM and Element Manager QoS configuration . . . 80
Layer 4 (TCP/IP) classification . . . 83
Port number classification . . . 83
Protocol ID classification. . . . 83
Meridian 1, Succession 1000, and Succession 1000M ports . . . 83
Policy management. . . . 84
Optivity Policy Services. . . . 84
VoIP call admission control . . . 84
VoIP bandwidth management zones . . . 86
Relationship between zones and subnets . . . 90
VoIP network voice engineering considerations . . . 91
Determining interzone and intrazone bandwidth values . . . 91
Codec selection . . . 93

Introduction

This chapter describes the mechanisms required to design a QoS-managed VoIP network with satisfactory voice quality.

Today's corporate intranets evolved to support data services that found a "best effort" IP delivery mechanism sufficient. Standard intranets are designed to support a set of QoS objectives dictated by these data services.

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, maintaining 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 will be 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 could use most of the available bandwidth this would cause voice packet loss and therefore, poor voice quality.

Recommendation

Nortel Networks strongly recommends implementing suitable QoS mechanisms on any IP network carrying VoIP traffic.

This section outlines QoS mechanisms that work in conjunction with the Succession 3.0 node. This section also discusses the intranet-wide consequences if the mechanisms are implemented.

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

- TLAN connections
- VoIP traffic between Internet Telephones
- VoIP traffic between Internet Telephones and Voice Gateway Media Cards on the TLAN

Traffic mix

Before implementing QoS mechanisms in the network, 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 is designed to deliver only VoIP traffic, and all traffic flows are of equal priority, then there is no 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 planning 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 will be 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. There are two consequences, as follows:

- WAN link inefficiency
- VoIP traffic streams are unfairly affected

The solution to this problem is Weighted Random Early Detection queueing (WRED) as described on page 56.

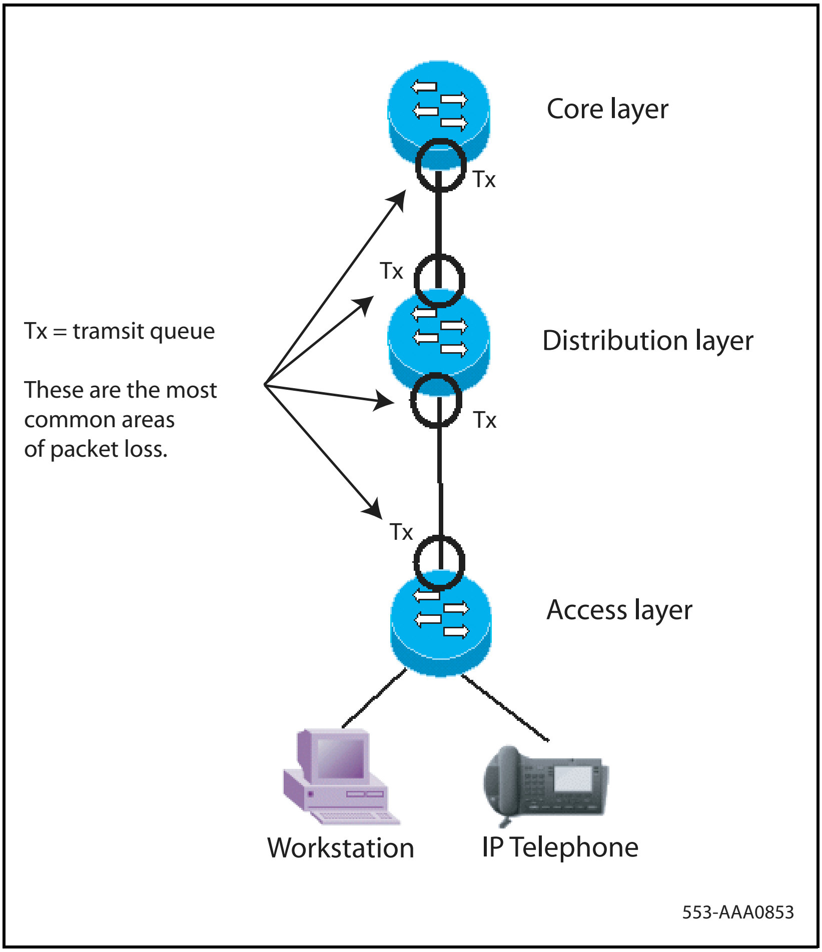
QoS problem locations

Figure 6 on page 52 identifies typical network congestion areas.

Voice traffic competes for limited bandwidth on the uplinks. These uplinks are shown in Figure 6 on page 52.

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 6
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 queuing 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/or 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 re-mark 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.

WAN require more sophisticated QoS mechanisms such as:

- fragmentation
- interleaving
- ATM
- Frame Relay

For more information, refer to “WAN QoS mechanisms” on page 58.

The QoS process

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

1. classification
2. marking
3. queueing (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. This means that 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 Protocol (RSVP).

Classification

The following can classify and mark their VoIP packets:

- Succession Signaling Server - classifies its packets as signaling packets
- Voice Gateway Media Card - classifies its packets as voice or signaling packets
- Internet Telephones - classify their packets as voice or signaling packets

> ***Note:*** To classify Succession Signaling Server and Voice Gateway Media Card packets at Layer 2 (802.1p) and/or Layer 3 (DiffServ), implement QoS mechanisms on the Succession Signaling Server and Voice Gateway Media Card and the Layer 2 switch ports to which they are attached. Internet Telephones with firmware 1.31 (or later) can classify voice and signaling packets at Layer 2 (802.1p) and/or Layer 3 (DiffServ).

Classification can be implemented on Layer 2 or Layer 3 switches. Consult the switch's documentation for information on configuring classification.

Policy management also provides other methods of classifying and marking packets, based on identifiers such as the originating IP address of the packet. For more information on Policy Management, see "Policy management" on page 84.

Packets can also be pre-marked with default 802.1p and DiffServ CodePoint (DSCP) values. The Layer 2/Layer 3/Policy switches can be configured to trust that the packets have been marked correctly.

Marking

Nortel Networks Internet Telephones, upon power-up, contact the Telephony Proxy Server (TPS) that controls them. The TPS then instructs the Internet Telephones to mark all packets with a default, yet configurable (through Element Manager) DSCP and/or 802.1Q/802.1p tag.

The control packets are marked for each of the following:

- Succession Signaling Server
- Voice Gateway Media Cards
- H.323 Gateway
- H.323 Gatekeeper

Queuing

Queueing delay is a major contributor to delay, especially on highly-utilized and low-bandwidth WAN links ("Queuing delay" on page 132). Routers that are QoS-aware and support priority queuing can help reduce queueing delay of voice packets when these packets are treated with preference over other packets.

Weighted Random Early Detection (WRED)

The global synchronization situation described in "TCP traffic behavior" on page 51 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 dropping of packets from long-lived TCP sessions and minimize the dropping of voice packets. Check the configuration guidelines with the router vendor for performance ramifications when enabling 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 which adversely affect voice quality.

> ***Note:*** 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, leaving the second highest priority queue for the remaining user traffic.

Recommendation

Nortel Networks recommends that voice traffic be placed 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 could be combined with other high-priority network-controlled traffic. Because the queuing delay is small for Ethernet interfaces, this should have very little impact on voice quality.

Most Layer 2 switches use a strict-priority scheduler. A strict-priority scheduler schedules all packets in a higher-priority queue before servicing 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 set to limit the maximum amount of bandwidth that the VoIP traffic can consume. This threshold is also called “rate limiting”.

Recommendation

Nortel Networks recommends that a strict priority be used 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.

> ***Note:*** Other vendors often refer to “priority queueing” when describing their 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 100% weight (highest priority). This queue is where the voice packets with DSCPs marked with ‘EF' (Expedited forwarding) and 'CS5' (Class Selector 5) are placed by default, when QoS is enabled on an interface.

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

WAN QoS mechanisms

There are many items 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

One of the main attractions of VoIP is the ability to use an existing WAN data network to save on inter-office toll calls. However, offices often connect over low-bandwidth WAN connections, so special considerations must be made when adding 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 being used for the VoIP call. This reduces the data traffic throughput to, perhaps, an unacceptable level. Adding VoIP to the existing WAN data network might require an increase in the WAN bandwidth.

VoIP bandwidth is dependent on the following:

- type of codec used
- if Voice Activity Detection (VAD) is used. VAD is also known as Silence Suppression.
- packetization rate (voice sample size)
- IP/UDP/RTP encapsulations
- if RTP Header Compression is 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 kbps (5-octet FR) to 16.8 kbps (42-octet 802.3 LAN) for each VoIP call.

    Note: 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 kbps. Due to the potential use of 20% of link capacity for "zero-bit stuffing", a safe assumption for link capacity is 102 kbps. For design purposes, assume a maximum utilization of 70% (in this example, 90 kbps).

This bandwidth has been sufficient for the current data requirements. The company believes that it only needs 70-80 kbps 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. If all 4 calls were simultaneously active, this would require 108.8 kbps (using a G.729 codec, 20 ms voice sample, and PPP overhead/frame) of the available 90 kbps of the 128 kbps 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 kbps link is the minimum speed to provide 109 kbps for four G.729 VoIP calls, 80 kbps 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 Mbps) connections. There are several different protocols that can be used to fragment packets.

For Frame Relay connections, the FRF.12 standard can be used for fragmenting packets. ATM provides fragmentation since 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.

Consult the router's documentation for information on 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 two reasons:

1. Layer 3 fragmentation applies only to the specific protocol being used. For example, Internet Protocol's (IP) MTU (Maximum Transmission Unit, in bytes) affects only IP traffic. It has no effect on IPX, AppleTalk, or other protocols.
2. Some applications do not function because they set the "Do not Fragment" bit. This prevents the application's packets from being transmitted.

PPP fragmentation and interleaving

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

For example, a voice (small) 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 for a time, 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 will be sent before the rest of the data packet.

IP fragmentation

All routers support IP fragmentation. IP fragmentation 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 considerable amount of time to transmit over a low-bandwidth connection.

CAUTION
When determining the fragment size for a packet, ensure that the fragment size is not smaller than the voice packet. Fragment only the larger data packets, not the voice packets.

For example, over a 64 kbps link, a 1500 byte data packet takes 188 ms to transmit. If the WAN connection is Frame Relay (FR), this same queuing 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 is ever transmitted. Jitter of 188 ms is created, which greatly exceeds the normal jitter buffer settings of 2 to 3 voice sample sizes (40 – 90 ms). This results in at least one packet, and usually many packets, arriving too late to be used.

Over bandwidth-limited connections (<1 Mbps), if Layer 2 (ATM, FRF.12, or PPP) fragmentation is not used, 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 will have a larger MTU size than a lower bandwidth connection.

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

Recommendation

Nortel Networks recommends PPP as the preferred method for packet fragmentation. Use IP fragmentation only if the router does not support a DLL fragmentation protocol, such as PPP or FRF.12.

Table 3 provides the recommended maximum MTU sizes for different connection speeds when using IP fragmentation. These choices result in a maximum delay of 8 ms.

Note: These values also apply to Layer 2 fragmentation techniques.

Table 3
Recommended MTU sizes for various connection speeds

	Connection Rate (in kbps)				
	56	**64**	**128**	**256**	**512**
Maximum MTU size (in bytes)	56	64	128	256	512

Recommendation

Nortel Networks recommends PPP as the preferred method 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

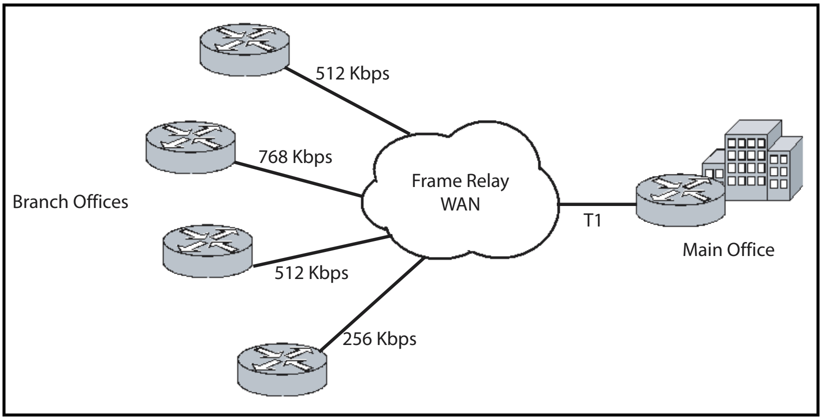
In some cases, there can be multiple paths for a VoIP packet to take when traveling from source to destination. If all VoIP packets do not take the same path, packets can arrive out-of-order. This can cause voice quality issues, even though packet reordering often has little or no adverse affect on data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

For example, if two locations are connected using two Frame Relay Permanent Virtual Circuits (PVCs), it is necessary to 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. Another approach is to 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, terminating at Branch Office locations with a single high-speed link into a hub location. See Figure 7.

Figure 7
Traffic shaping



In this example, the Branch Office 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 Branch Office sites. Without traffic shaping, the network can randomly drop packets. The resulting packet loss is detrimental to voice quality.

Traffic shaping prevents this from happening. Through the use of traffic shaping, it is possible to determine which packets are dropped due to congestion and which packets receive priority.

Traffic shaping works by queuing 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 any packets as Discard Eligible. This cannot be tolerated when running real-time applications such as voice.

When running traditional data applications over Frame Relay, the network allows bursting over a certain Time Interval (Tc). If the data burst exceeds the contract during that time interval, 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 is occurring in the upstream or downstream direction. Upon receiving this feedback, the DTE should throttle back to the Committed Burst (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 our 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 down to a size of 2 to 4 bytes.

This results in significant bandwidth savings across low bandwidth WAN links. It is important to note current WAN platform CPU levels before implementing 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.

Implementing QoS mechanisms over a PPP WAN link may involve the use of the following:

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

Frame Relay QoS

Nortel Networks recommends 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. It can be beneficial to use partially meshed PVCs, depending on traffic patterns.

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

ATM QoS

Two methods of ensuring VoIP QoS on ATM links are available:

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

Nortel Networks recommends 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 source IP address or Diffserv CodePoint. VoIP bandwidth management on the Succession 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 queuing 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 Networks Internet Telephone can be recognized because each Nortel Networks Internet Telephones has a unique set of MAC addresses. When the Layer 2 switch recognizes the Internet Telephone packet's MAC address, it marks the packets with the appropriate 802.1p value. Then the Layer 2 switch 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 additional bytes to the Ethernet packet header. See Figure 8 on page 69.

The 802.1Q extensions contain two important fields – the 802.1p field and the VLAN ID field. Table on page 69 lists the 802.1Q field names and their definitions.

Figure 8
Ethernet 802.1Q extensions

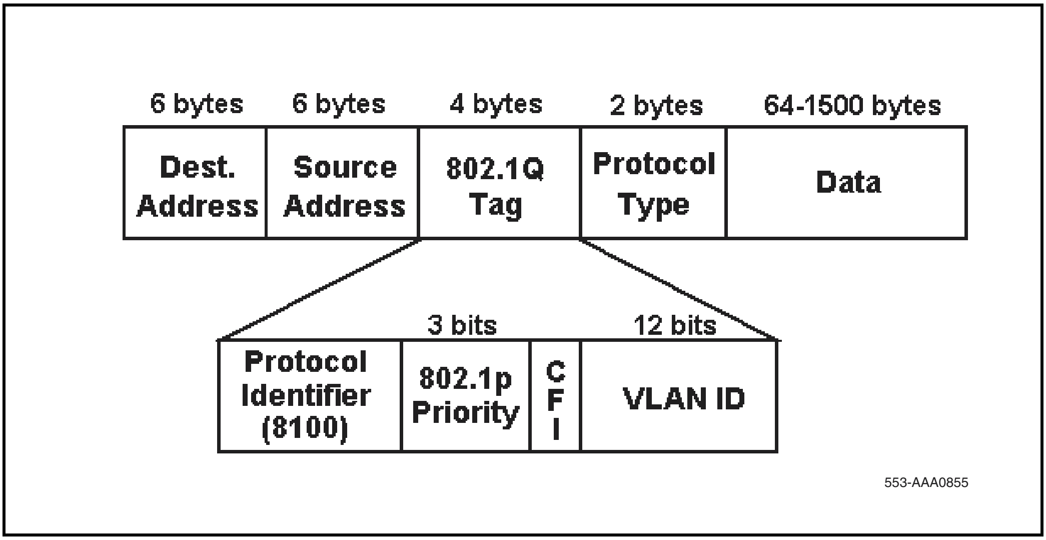


Table 4
IEEE 802.1Q field definitions

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 0-7 representing 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.

> ***Note:*** The routers must be compatible. Routers must support VLANs on their physical ports.

VLANs have obvious 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.

> ***Note:*** When 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 all receives consistent QoS treatment.

> ***Note:*** A VLAN can only provide QoS on Layer 2 switches that support the 802.1Q (VLAN) standard. Once the packets leave the Layer 2 switch, and encounter routers or WAN switches, DiffServ should be used to provide end-to-end QoS. Nortel Networks Internet Telephones also mark the DSCP, so when voice packets encounter routers, the routers can be configured to prioritize the packets based on their DSCP value.

The i200x Internet Telephones 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 i200x Internet Telephone firmware tags the ethernet frames with both the telephone's VLAN ID and the 802.1p priority specified in Element Manager. The recommended 802.1p priority is 6.

The i2050 Software Phone 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 to provide eight Classes of Service (CoS). 802.1p-capable L2/L3 switches use these Classes of Service to prioritize packets, and then place them in different queues. This provides service differentiation.

802.1p configuration

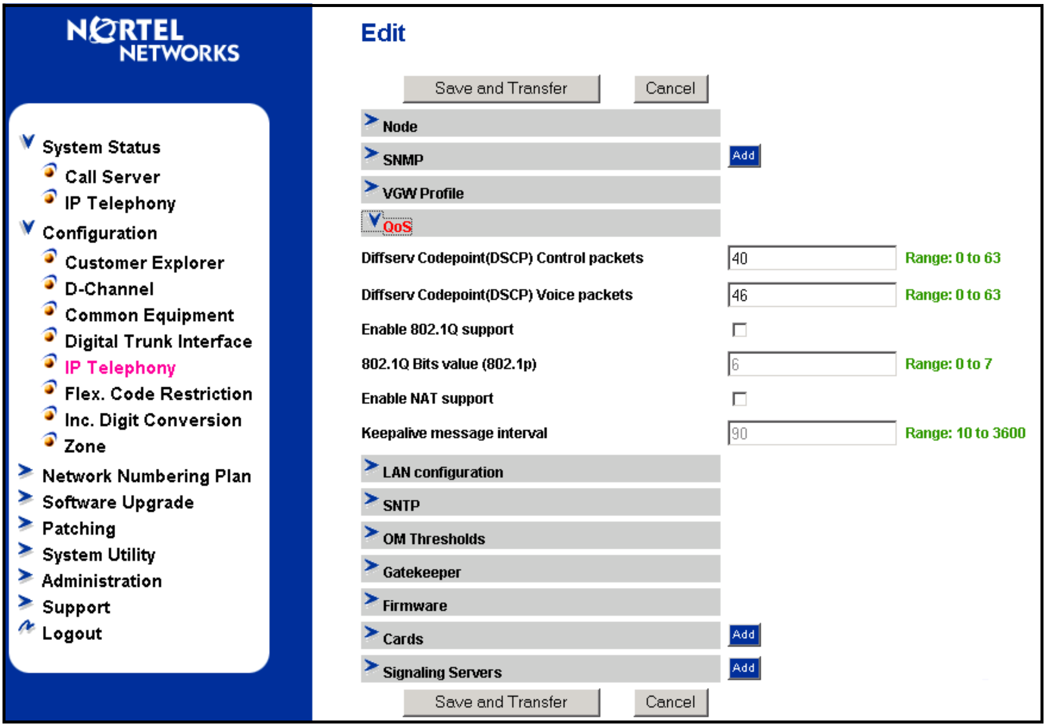
The 802.1p priority bits are configured in Element Manager.

Configure the following:

- Enable 802.1Q Support {0 = disabled, 1 = enabled}
- 802.1Q Bits value (802.1p) = {Internet Telephone priority = 0 to 7}

See Figure 9 on page 72.

Figure 9
Priority bit configuration in Element Manager



Diffserv Codepoint(DSCP) Control packets 40 Range: 0 to 63

Diffserv Codepoint(DSCP) Voice packets 46 Range: 0 to 63

Enable 802.1Q support □

802.1Q Bits value (802.1p) 6 Range: 0 to 7

Enable NAT support □

Keepalive message interval 90 Range: 10 to 3600

Port prioritization

A Layer 2 switch port can be configured to prioritize all packets entering it. This could be done in cases where Internet Telephones connect to a Layer 2 switch port that is not shared with other devices.

3-port switch port prioritization

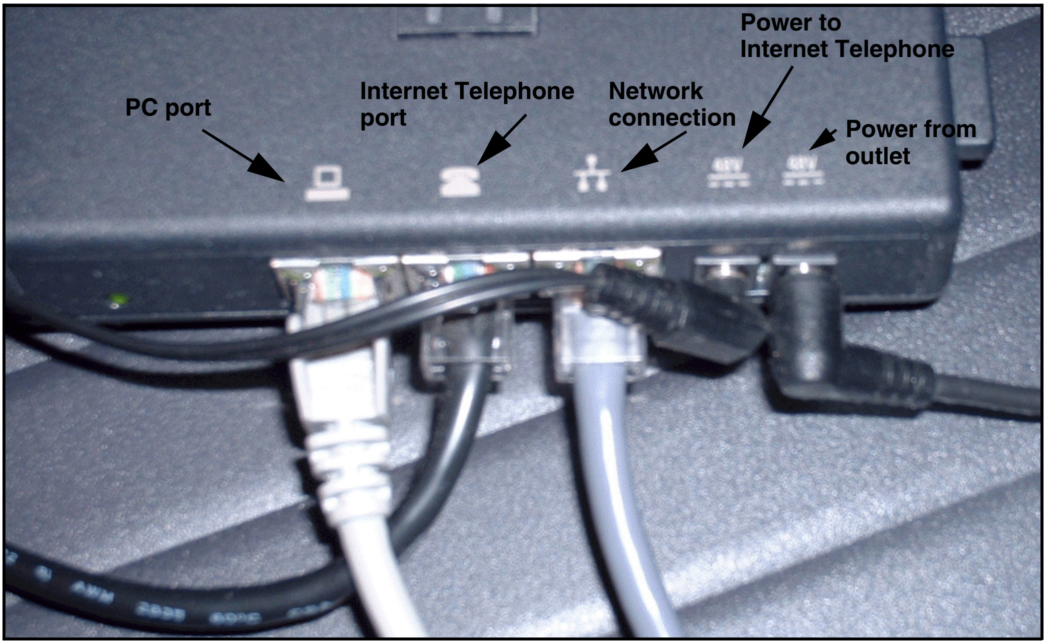
The i2004 Internet Telephone has an optional external 3-port Layer 2 switch module that is inserted into the bottom of the phone. See Figure 10 on page 73.

The i2002 Internet Telephone has a built-in 3-port switch. The internal port is used by the 2002 Internet Telephone. 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 Internet Telephone to share a single Ethernet connection. All packets entering the port connected to the Internet Telephone are given a higher priority than packets entering the port connected to the PC. This ensures that all voice packets are sent ahead of any data packets. This has little effect on the data packets because the Internet Telephone packets are small and use little bandwidth.

> ***Note:*** When using the optional external 3-port switch module, the Internet Telephone must be plugged into the correct port for the voice packets to receive proper treatment. See Figure 10 on page 73.

Figure 10
3-port switch



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

Recommendation

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. Newer Layer 3 IP devices (routers and Layer 3 switches) can classify Internet Telephone 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 these two fields must be coordinated across the entire IP data network. Do not change them arbitrarily.

IP address classification

A Nortel Networks Internet Telephone obtains its 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 set aside exclusively for Internet Telephones. The Layer 3 switch/router can then prioritize the packets based on this range of IP addresses. It marks the voice packets from those designated IP addresses with the recommended DSCP.

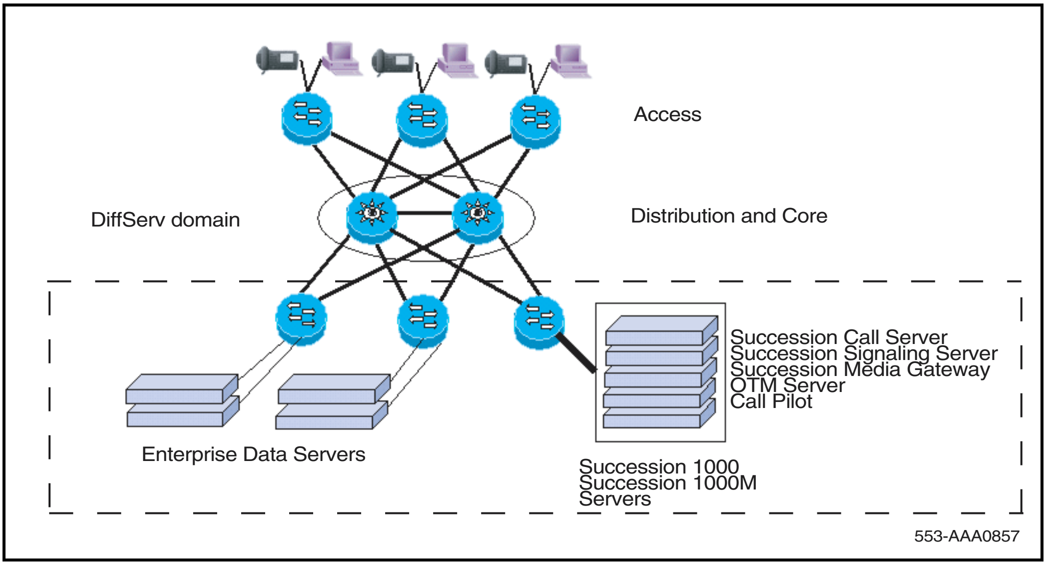
This method does not differentiate between voice media and signaling packets. Only a single DSCP is used for both. However, if additional filters are applied to sort the different packet types, the voice media and signaling packets can be marked with different DSCPs.

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 11 shows the architecture of DiffServ-based QoS.

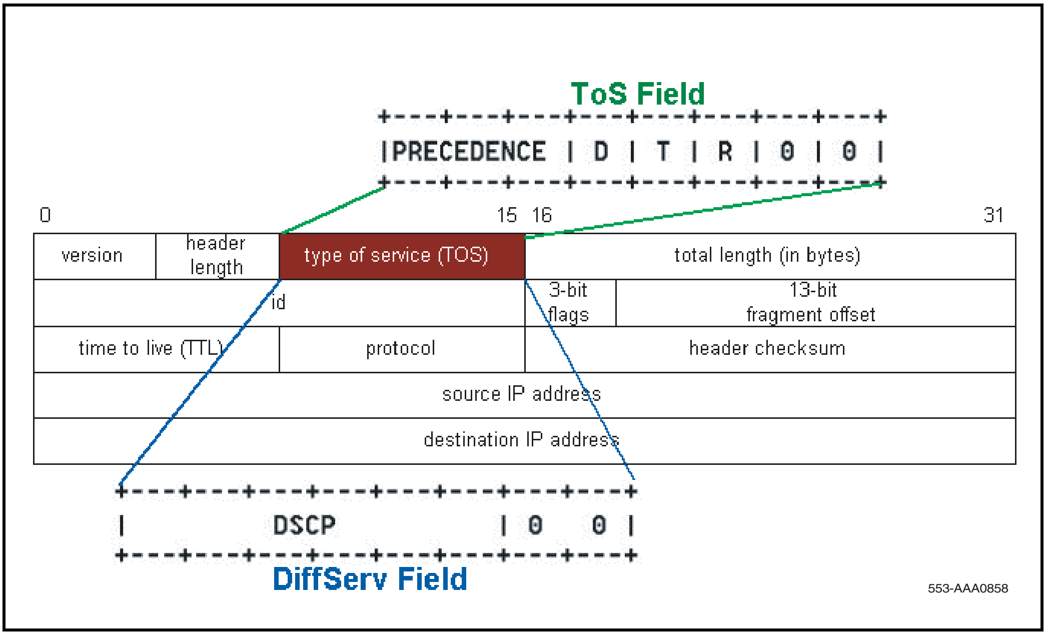
Figure 11
DiffServ-based QoS architecture



The DiffServ CodePoint (DSCP) is a 6-bit value contained in the second byte of the IPv4 header. See Figure 12 on page 76. 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) which was formerly known as the Type of Service (ToS) Field. Some routers use the older ToS terminology instead of the newer DiffServ terminology. However, in either case, the six most significant bits in this field are the DSCP value. See Figure 12.

Figure 12
IPv4 header showing DSCP location



Note: The 8-bit value, rather than the 6-bit value, is seen if using a network analyzer to look at the DiffServ byte.

Trust configuration

DiffServ edge routers and switch interfaces can be configured to trust or distrust any previously-marked DSCP or 802.1p-tagged packet. Voice packets entering 'untrusted' interfaces are re-marked to a DSCP/802.1p value of 0 (best effort), unless filters are set up 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 re-marked and the pre-marked voice packets are prioritized based on their DSCP and 802.1p values.

A router can use the DSCP to queue pre-marked Internet Telephone packets if they have arrived from a trusted source.

For example, a Layer 3 switch can have Ethernet ports assigned just to Internet Telephones. These ports can be configured to trust that the Internet Telephones have 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 Mbps) connection, considerable queuing delay can occur. This queuing 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 packets and voice signaling packets must be separated into different queues. By marking the voice media packets 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.

> *Note:* It is important to categorize signaling packets so they are not discarded by the network. The Internet Telephone contains a watchdog timer that resets the Internet Telephone if signaling packets are not seen within a certain amount of time. Lost signaling packets can cause the Internet Telephones 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 packets and voice signaling packets. This is necessary to minimize jitter that was introduced by the signaling packets to the voice media packets. This 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 Succession Signaling Server, Voice Gateway Media Cards, and the i2002 and i2004 Internet Telephones.

Table 5 on page 79 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

> ***Note:*** If using 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 Networks standard DSCP for signaling is decimal 40.

The Nortel Networks standard DSCP for voice is decimal 46, based on six bits of an 8-bit field. Two bits are unused.

The DSCP is programmed through Element Manager.

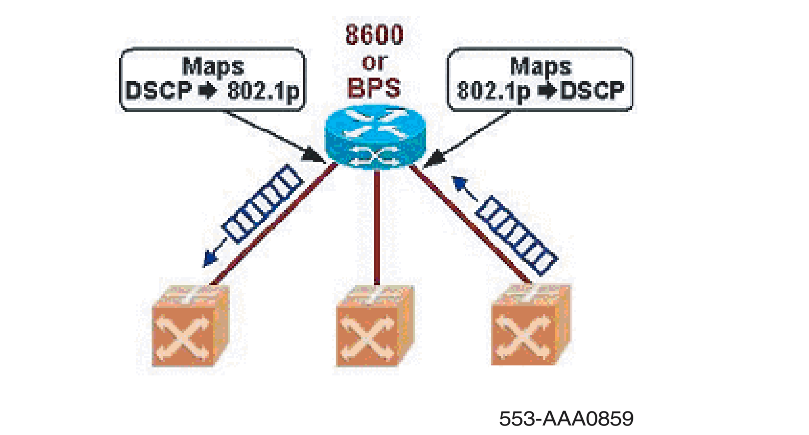
For an example of Layer 3 QoS configuration, see Appendix B on page 261.

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 Figure 13 on page 80. This extends the IP QoS to Layer 2 QoS for the downstream L2 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 has configured a different 802.1p tag for the Internet Telephone’s 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.

Figure 13
Mapping DSCP to 802.1p



Example

Using Optivity Telephony Manager (OTM), a network administrator can configure the i2004 Internet Telephones 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 pre-marked packets entering ports configured as 'core ports'. The Passport 8600 places these packets into the highest priority queue by default. Its scheduler for this queue has been pre-configured with a Packet Transmit Opportunity (PTO) or queue weight of 100%. This configuration provides the necessary behavior required for Internet Telephone packets to achieve the required QoS.

OTM and Element Manager QoS configuration

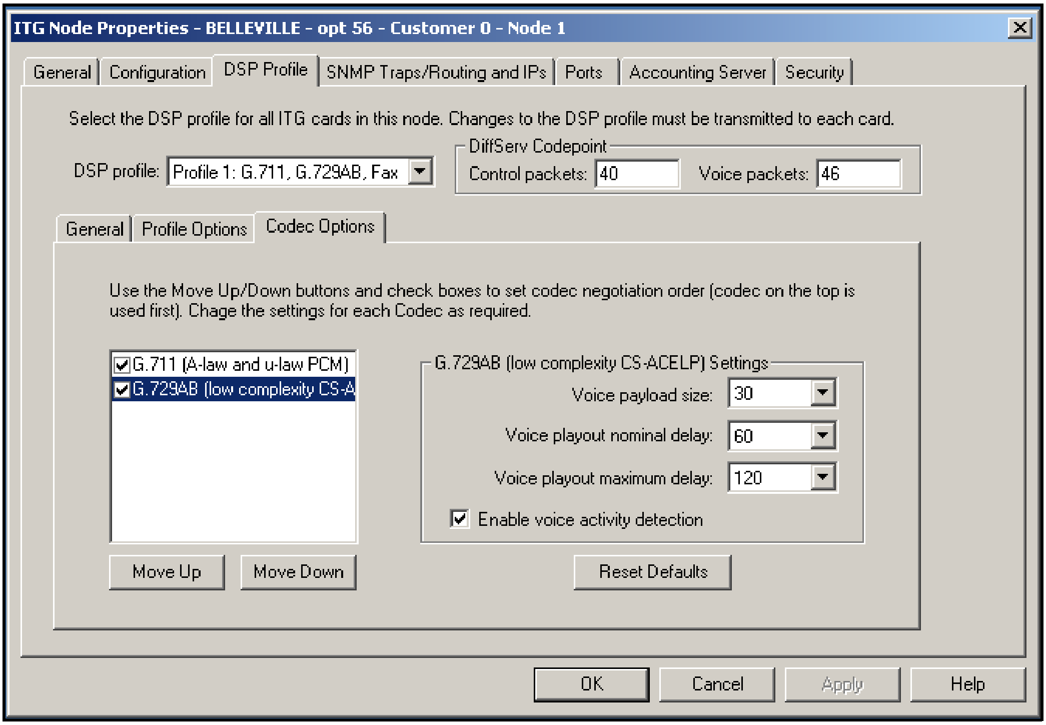
QoS configuration is done using OTM or Element Manager.

- Meridian 1 systems equipped with IP Trunk and IP Line must use OTM.
- Succession 1000 and Succession 1000M systems must use Element Manager.

Adhering to Nortel Networks standards, the DSCP bits for VoIP control packets are set to ‘CS5’, decimal value of 40. The voice packets are set to the Expedited Forwarding 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 Mbps), the control and voice packets marked with different DSCP values should be separated into different queues; otherwise, the voice packets experience significant queuing delays. Figure 14 on page 81 shows the DSCP configuration through OTM.

Figure 14
Voice Gateway Media Card DiffServ CodePoint (DSCP) configuration through OTM



ITG Node Properties - BELLEVILLE - opt 56 - Customer 0 - Node 1

Select the DSP profile for all ITG cards in this node. Changes to the DSP profile must be transmitted to each card.

DSP profile: Profile 1: G.711, G.729AB, Fax

DiffServ Codepoint
Control packets: 40
Voice packets: 46

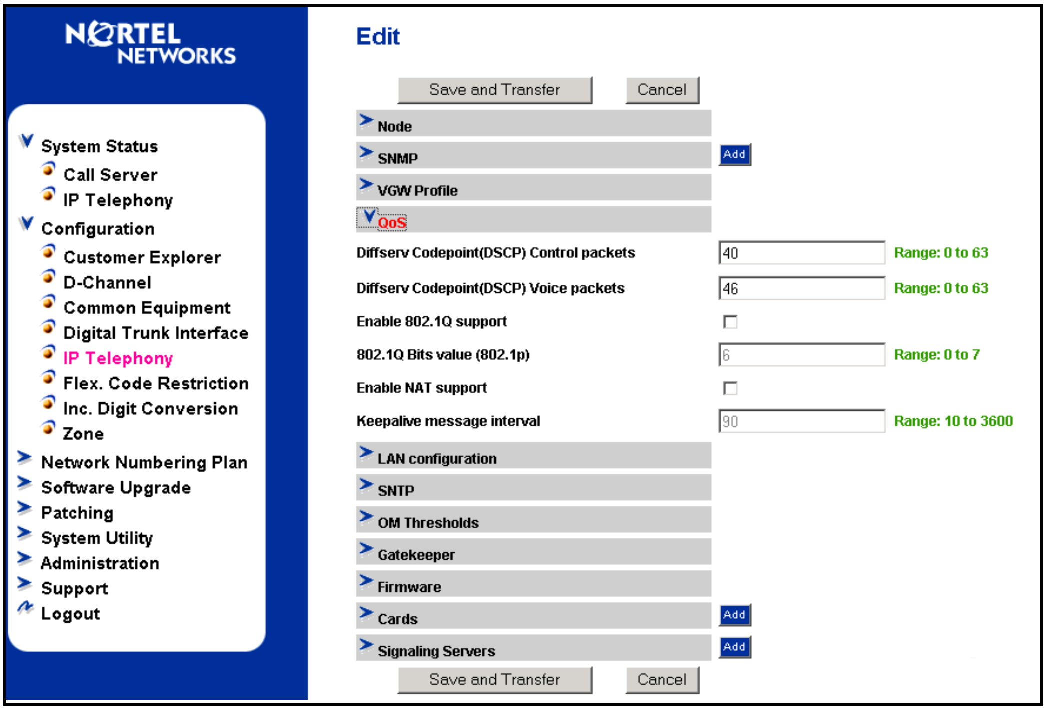
Use the Move Up/Down buttons and check boxes to set codec negotiation order (codec on the top is used first). Chage the settings for each Codec as required.

☑ G.711 (A-law and u-law PCM)
☑ G.729AB (low complexity CS-A

G.729AB (low complexity CS-ACELP) Settings
Voice payload size: 30
Voice playout nominal delay: 60
Voice playout maximum delay: 120
☑ Enable voice activity detection

Figure 15 shows the DCSP configuration through Element Manager.

Figure 15
Voice Gateway Media Card DSCP configuration through Element Manager



Diffserv Codepoint(DSCP) Control packets	40	Range: 0 to 63
Diffserv Codepoint(DSCP) Voice packets	46	Range: 0 to 63
Enable 802.1Q support	□	
802.1Q Bits value (802.1p)	6	Range: 0 to 7
Enable NAT support	□	
Keepalive message interval	90	Range: 10 to 3600

Layer 4 (TCP/IP) classification

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

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

Port number classification

UDP port numbers used by Internet Telephone RTP packets are dynamically assigned. This makes it difficult to classify packets by port number. However, if a specific range of port numbers is assigned to Internet Telephones, then the router recognizes that the packet has come from a port number assigned to Internet Telephones, and prioritizes the packet as a voice packet.

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

Protocol ID classification

The Real-time Transport Protocol (RTP) is used by many multimedia applications such as real-time fax and video, as well as voice. Prioritizing packets according to the protocol used, therefore, cannot be used to accurately prioritize the voice packets.

Meridian 1, Succession 1000, and Succession 1000M ports

See Appendix D: “Port number tables” on page 283 for more information.

Policy management

Prioritization of traffic can also be implemented through policy management. Nortel Networks supports this option through Optivity Policy Services software. See “Policy Management” on page 226 and “Policies” on page 275.

Optivity Policy Services

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

See “Optivity Policy Services” on page 275 for configuration examples.

Refer to the following website for more information on Optivity Policy Services: http://www.nortelnetworks.com/solutions/net_mang/

VoIP call admission control

The Meridian 1, Succession 1000, and Succession 1000M systems provide a means of IP network-based call admission control. Network-based call admission control is implemented using bandwidth management zones. Bandwidth management is considered a QoS mechanism because it provides a means of guaranteeing that Succession VoIP traffic will not use more network bandwidth than is 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.

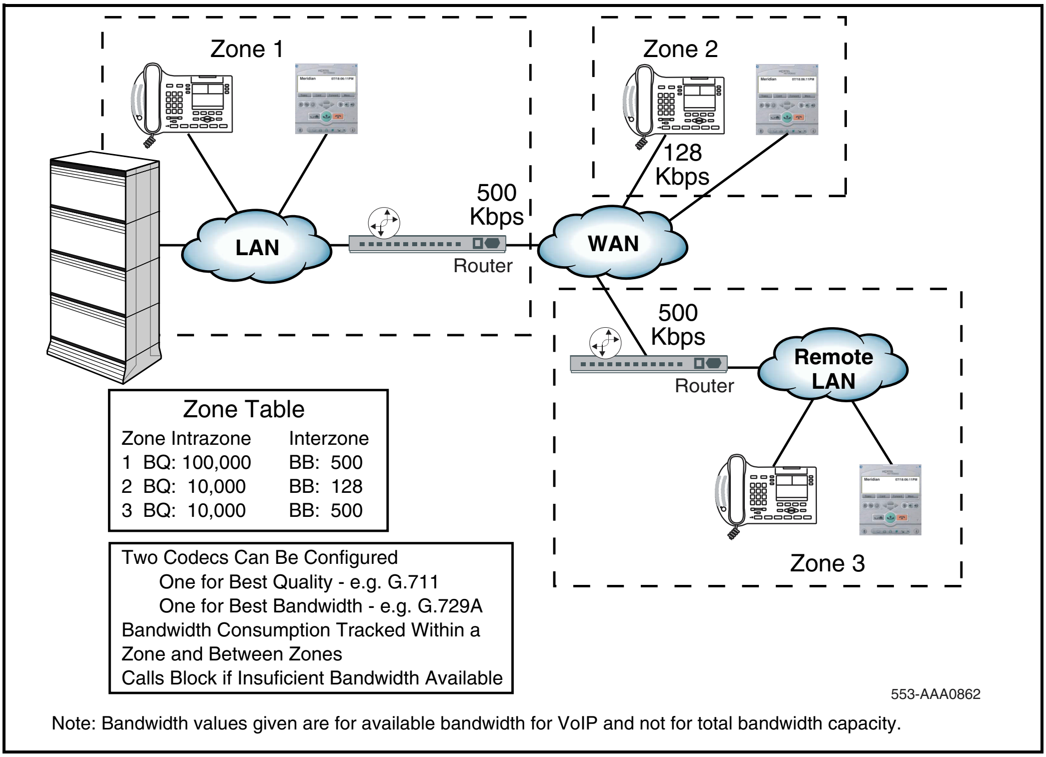
Interzone and intrazone bandwidth availability is calculated dynamically by the Succession Call Server on a per-call basis. A call is blocked if there is insufficient bandwidth available.

For example, if a CCS-type approach to VoIP network voice engineering is used, an administrator has to 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 (see Figure 16 on page 86).

Alternatively, through the use of bandwidth management zones, an administrator could simply enter the amount of bandwidth actually available for voice on the IP network into the Succession Call Server. The amount of bandwidth is ensured using other QoS mechanisms such as priority, as well as the type of voice CODEC that is used. The Succession Call Server then ensures that the VoIP call volume entering or leaving a zone will not exceed the IP network bandwidth available. This enables users to avoid quality degradation because of insufficient bandwidth for active connections.

Call admission control applies equally well to a single distributed system with centralized call control or multiple systems as in the case of a main site with numerous Branch Offices connected with VoIP.

Figure 16
Bandwidth management example



Zone Table

Zone	Intrazone	Interzone
1	BQ: 100,000	BB: 500
2	BQ: 10,000	BB: 128
3	BQ: 10,000	BB: 500

Two Codecs Can Be Configured
One for Best Quality - e.g. G.711
One for Best Bandwidth - e.g. G.729A
Bandwidth Consumption Tracked Within a Zone and Between Zones
Calls Block if Insuficient Bandwidth Available

Note: Bandwidth values given are for available bandwidth for VoIP and not for total bandwidth capacity.

VoIP bandwidth management zones

Bandwidth management zones divide Internet Telephones and Voice Gateway Media Cards into logical groupings (zones) to determine codec selection and bandwidth management. Zones are configured after the QoS-managed IP network has been designed.

Each Internet Telephone and Voice Gateway Media Card port is assigned a zone number in which it resides.

Virtual Trunk routes also allow configuration of a zone. A single Succession Call Server considers calls out a Virtual Trunk to be terminated on that Virtual Trunk. Therefore, Virtual Trunks and Internet Telephones should not be in the same zone. Zones allocated to Virtual Trunk routes are primarily used for intrasystem codec selection, as a result, Virtual Trunk zone bandwidth should be set to the maximum value of 1Gbps (1,000,000 Kbps). Bandwidth is already managed within the Internet Telephone zone.

As calls are made, the Succession 3.0 Software chooses a codec to be used for the call, based on the zone configuration. The software also tracks bandwidth usage within each zone and between zones. When making an interzone call, the lowest bandwidth codec between the zones is always chosen.

Zones are network wide, therefore zone numbers must not be duplicated. Branch Office zones should be configured on the Main Office system. The Branch Office zones would only contain equipment located at the Branch Office.

Each codec has specific parameters that must be configured, such as packetization delay and voice activity detect. These parameters are configured on the Succession Signaling Server using Element Manager. For further information, see “Element Manager” on page 217.

Zone properties are defined in LD 117. Up to 256 zones can be configured. The systems use the zones for bandwidth management. New calls are blocked when the bandwidth limit is reached.

Each zone has four parameters. The prompt lists the parameters as p1, p2, p3, p4, and p5:

- p1 - The total bandwidth available for intrazone calls.
- p2 - The preferred strategy for the choice of codec for intrazone calls (that is, preserve best quality or best bandwidth).
- p3 - The total bandwidth available for interzone calls.
- p4 - The preferred strategy for the choice of the codec for interzone calls.
- p5 - The zone resource type; the type is either shared or private.

The Succession Call Server uses the values shown in Table 6 on page 88 when calculating the bandwidth each call uses in a zone. The Succession Call Server uses the values in the columns labeled "TLAN Bandwidth". It looks up these values and subtracts them from the available zone bandwidth to determine if a zone has sufficient bandwidth for the call.

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 (Kbps)**	**Average bandwidth (Kbps)**	**Peak bandwidth (Kbps)**	**Average bandwidth (Kbps)**
G.711 (64 Kbps)	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 Kbps)	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 Kbps)	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 Kbps)	30	24	Off	54.40	54.40	17.07	17.07
G.723.1 (5.3 Kbps)	30	24	Off	54.40	54.40	17.07	17.07

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. These are often excluded from bandwidth calculations but must be included to give a true indication of the bandwidth used. The Succession Call Server assumes a half-duplex Ethernet connection (again, to cover the worse case), so the bandwidth values shown are twice what is normally listed for a full-duplex link.

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, such as Frame Relay, is added to the base value to determine the total bandwidth used. The values shown are for a duplex link, so if the WAN facility is half-duplex, the values should be doubled.

The Succession Call Server cannot determine whether the LAN/WAN connection is half- or full-duplex. Therefore, the Succession Call Server assumes the worse case, and subtracts the bandwidth consumed on a half-duplex link by the codec and voice payload combination from the available zone bandwidth.

This should be considered when entering a zone's intra- and inter-bandwidth values in LD 117. If the zone has full-duplex links, then the bandwidth entered should be doubled. For example, with a 100BaseT full-duplex LAN, the intrazone bandwidth can be configured to be 200 000.

> ***Note:*** The Succession Call Server is unaware of the particulars of the WAN facility and always uses the values shown in the "TLAN Bandwidth" columns.

If no IP voice zones are configured, zone 0 operates as a default zone with no restrictions on bandwidth usage. If no IP voice zones are configured in LD 117, zone 0 can be configured for IPTN in LD 14, and for virtual line in LD 11 as a default zone. However, if any additional zones are required, zone 0 must be first configured in LD 117 if it is referenced by any Internet Telephone or ITG Physical TNs (IPTN). If zone 0 is not configured first, then all calls in zone 0 are labeled as soon as another zone is configured in LD 117.

CAUTION
When moving an Internet Telephone, the Administrator should check and change, if necessary, the telephone's zone assignment in LD 11. See *Software Input/Output: Administration* (553-3001-311).

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

Relationship between zones and subnets

Internet Telephones 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 Internet Telephones 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 router(s) with sufficient bandwidth. The Internet Telephones and gateway channels spread across them could all reside in a single zone. However, if there is a WAN facility with limited bandwidth 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 Internet Telephone is present at the remote location. It can be convenient to allocate zones for users with similar connection speeds. In that case, set both the interzone and intrazone codec to Best Bandwidth.

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 refer to:

- "Bandwidth" on page 108
- The Capacity Engineering section in *Large System: Planning and Engineering* (553-3021-120)

Determining interzone and intrazone bandwidth values

In the following example, it is assumed that voice traffic engineering, capacity planning, and bandwidth demand per link have all been calculated, and the maximum number of calls allowed in each bandwidth zone, and between zones has been determined. In this example, 125 calls within the zone, and 8 calls between zones, are assumed.

To determine intrazone bandwidth, follow the steps in Procedure 2 on page 91.

Procedure 2
Determining intrazone bandwidth

1. For each bandwidth zone, determine the maximum number of simultaneous calls to be allowed within the zone.
2. Choose the bandwidth per call value from Table 6 on page 88, based on the codec and options configured for Best Quality (BQ).

   For example, if G.711, 20 ms, VAD Off is selected for BQ, the Call Server will calculate 190.40 Kbps of bandwidth use for each intrazone call.

3 Calculate the intrazone bandwidth setting by multiplying the BQ bandwidth per call value (as calculated in kbps in step 2) by the maximum number of calls to be allowed within the zone. Round up to the next whole number, if necessary.

In this example, if the maximum number of intrazone calls is 125, then 190.40 kbps/call * 125 calls = 23,800 kbps.
CAC will then allow up to 125 calls in the zone. Use this value for intrazone bandwidth when defining the zone.

End of Procedure

To determine interzone bandwidth, follow the steps in Procedure 3.

Procedure 3
Determining interzone bandwidth

1 For each bandwidth zone, determine the maximum number of calls to be allowed between zones.

2 Choose the bandwidth per call value from Table 6 on page 88, based on the codec and options configured for Best Bandwidth (BB).

For example, if G.729A, 30 ms, VAD off is selected for BB, the Call Server will calculate 57.60 Kbps of bandwidth use for each interzone call.

3 Calculate the interzone bandwidth setting by multiplying the BB bandwidth per call value (as calculated in kbps in step 2) by the maximum number of calls to be allowed between zones. Round up the value to the next whole number, if necessary.

In this example, if the maximum number of interzone calls is 8, then 57.60 kbps/call * 8 calls = 460.8 kbps. Round 460.8 kbps to 461 kbps.
CAC will then allow up to 8 calls between zones. Use this value for interzone bandwidth when defining the zone.

End of Procedure

Note: If a network link is a full-duplex link, enter twice the bandwidth into the bandwidth zones configuration. For example, a 512 Kbps full-duplex link has same the amount of bandwidth as a 1024 Kbps half duplex link (full-duplex bandwidth = half-duplex / 2).

Codec selection

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

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 Networks CallPilot**,** introduces another stage of compression and decompression.
- Conferences can double the number of IP links.
- ITG Trunks can add additional stages of compression and decompression.

  Note: Nortel Networks 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 are different.

Network performance measurement

Contents

This section contains information on the following topics:

Introduction 97

Performance criteria 97

Network performance evaluation overview 99

Set QoS expectations 100

Network performance measurement tools. 106

Network availability 107

Bandwidth 108

Available Bandwidth 108

Guaranteed Bandwidth 108

Queueing. 109

Calculating per call bandwidth use. 109

Calculating VoIP traffic requirements. 109

Calculating LAN traffic. 110

WAN traffic calculations. 113

VoIP Bandwidth Demand Calculator 115

Silence Suppression engineering considerations 116

Estimate network loading caused by VoIP traffic 116

Route Link Traffic estimation 121

Enough capacity 123

Insufficient link capacity 124

Other intranet resource considerations 124

Delay 125

Effects of delay on voice quality 128

Components of delay 129

Propagation delay 129

Serialization delay 129

Queuing delay 132

Routing and hop count 133

VoIP system delay. 133

Other delay components 133

Measuring end-to-end network delay 134

Sample PING output: 135

Assessment of sample PING output 135

Adjusting PING measurements 136

One-way and round-trip 136

Adjustment due to IP Line processing 136

Other measurement considerations 137

Reducing delays 137

Reducing hop count 138

Recording routes 139

Routing issues 139

Jitter 140

Jitter buffers 142

Late packets 142

Adjusting jitter buffer size 143

Packet loss. 145

Physical medium loss. 145

Congestion loss 145

Measuring end-to-end packet loss 147

Packet Loss Concealment 147

Reducing packet loss 148

Network delay and packet loss evaluation example 149

Estimate voice quality. 151

Sample scenarios 156

Scenario 1 156

Scenario 2 157

Scenario 3 158

Does the intranet provide expected voice quality? 159

Introduction

To create a VoIP-grade network, certain QoS standards for basic network elements must be met. Several QoS parameters can be measured and monitored to determine if desired service levels have been obtained. These parameters comprise the following:

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

These QoS parameters and mechanisms affect the application's or end-user's Quality of Experience (QoE). These QoS parameters apply to any IP network carrying VoIP traffic, including LANs, campus-wide networks, and WANs.

Performance criteria

This section illustrates criteria for achieving excellent voice quality. The network should meet these 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 Telephone must be located to minimize the number of hops to the network backbone or WAN.

  Note: To ensure good voice quality, an end-to-end delay of <= 50 ms is recommended on the IP network. This does not include the built-in delay of the Voice Gateway Media Card and Internet Telephone.

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

Note: For high-quality voice transmission, the long-term average packet loss between the Internet Telephones and the Voice Gateway Media Card TLAN interface must be < 1%, and the short-term packet loss must not exceed 5% in any 10-second interval.

Recommendation

To achieve excellent voice quality, Nortel Networks recommends using 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). See "Succession Call Server to Succession Media Gateway Packet Delay Variation jitter buffer" on page 193.
- packet loss less than 0.5% (approaching 0%)
- maximum jitter buffer setting for Internet Telephone as low as possible (maximum 100 ms)

Packet loss on the ELAN interface can cause:

- communication problems between the Succession Call Server and the Voice Gateway Media Cards
- lost SNMP alarms
- incorrect status information on the OTM console
- other signaling-related problems

Note: Since 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 interface, the packet loss must be < 1%.

Network performance evaluation overview

There are two main objectives when dealing with the QoS issue in an IP network:

1. to predict the expected QoS
2. to evaluate the QoS after integrating VoIP traffic into the intranet

The process for either case is similar; one is with, and the other is without, VoIP traffic. The differences are discussed in this section.

In the process, it is assumed that the PING program is available on a PC, or some network management tool is available to collect delay and loss data and access the LAN that connects to the router to the intranet.

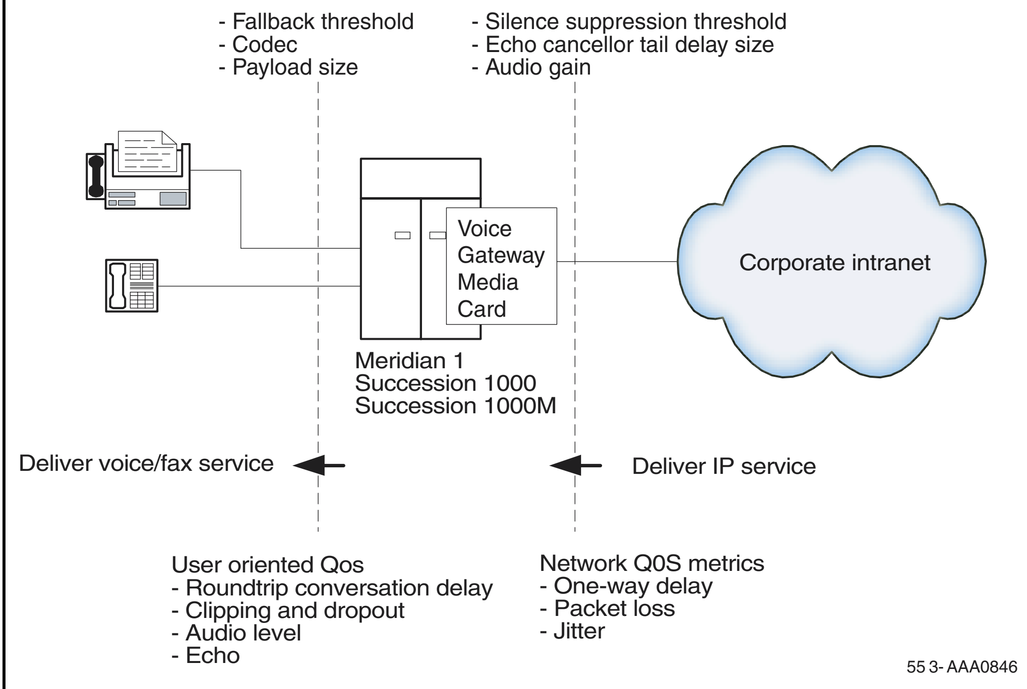
1. Use PING or an equivalent tool to collect round-trip delay (in ms) and loss (in%) data.
2. Divide the delay by 2 to approximate one-way delay. Add 93 ms to adjust for ITG processing and buffering time.
3. Use a QoS chart, or Table 20 on page 154, to predict the QoS categories: excellent, good, fair or poor.
4. If a customer wants to manage the QoS in a more detailed fashion, re-balance the values of delay compared to loss by adjusting system parameters, such as preferred codec, payload size, and routing algorithm, to move resulting QoS among different categories.
5. If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

Set QoS expectations

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

In the context of a Meridian 1, Succession 1000, and Succession 1000M system, Figure 17 on page 100 shows the relationship between users and services.

Figure 17
QoS parameters



From Figure 17 on page 100, it can be seen that there are two interfaces to consider.

- 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 set 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 which takes on one of these four settings: excellent, good, fair, and poor, indicating the quality of voice service. IP Trunk 3.0 (or later) periodically calculates the prevailing QoS level per site pair, based on its measurement of the following:

- one-way delay
- packet loss
- codec

Recommendation

Nortel Networks recommends that G.711 codec be used over high-bandwidth connections and used any time that call quality is the top priority. In call quality is the top 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 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 set to G.729A or G.729AB between zones (interzone).

Codec details are then configured on the Succession Signaling Server through OTM or Element Manager.

The computation (used to create Figure 18 on page 103, Figure 19 on page 104, and Figure 20 on page 105) is derived from ITU-T G.107 Transmission Rating Model.

Figure 18 on page 103, Figure 19 on page 104, and Figure 20 on page 105 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(u-law) delivers the best quality for a given intranet QoS, followed by G.729AB and then G.723.1 (6.4 kbp/s) and lastly G.723.1 (5.3 kbp/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 the human ear is; quality starts to degrade when packet loss exceeds 4%. Nortel Networks recommends that fax services be supported with IP Trunk 3.0 (or later) operating in either 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.

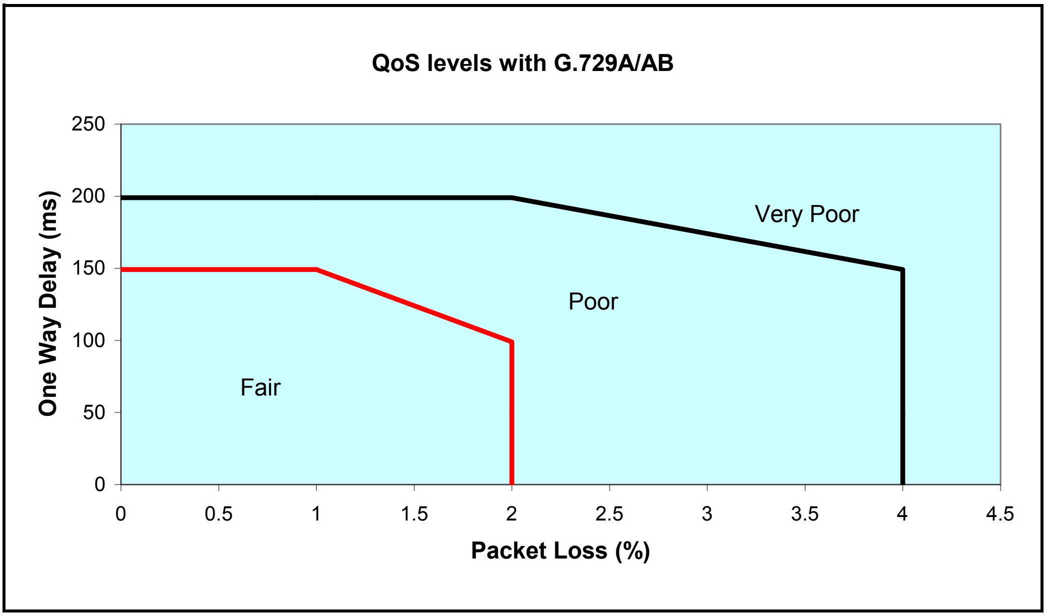
G.729AB codec

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.729 AB codec has the same requirements as the G.711 codec.

Figure 18 illustrates the QoS levels with a G.729A/AB codec.

Figure 18
QoS levels with G.729A/AB codec

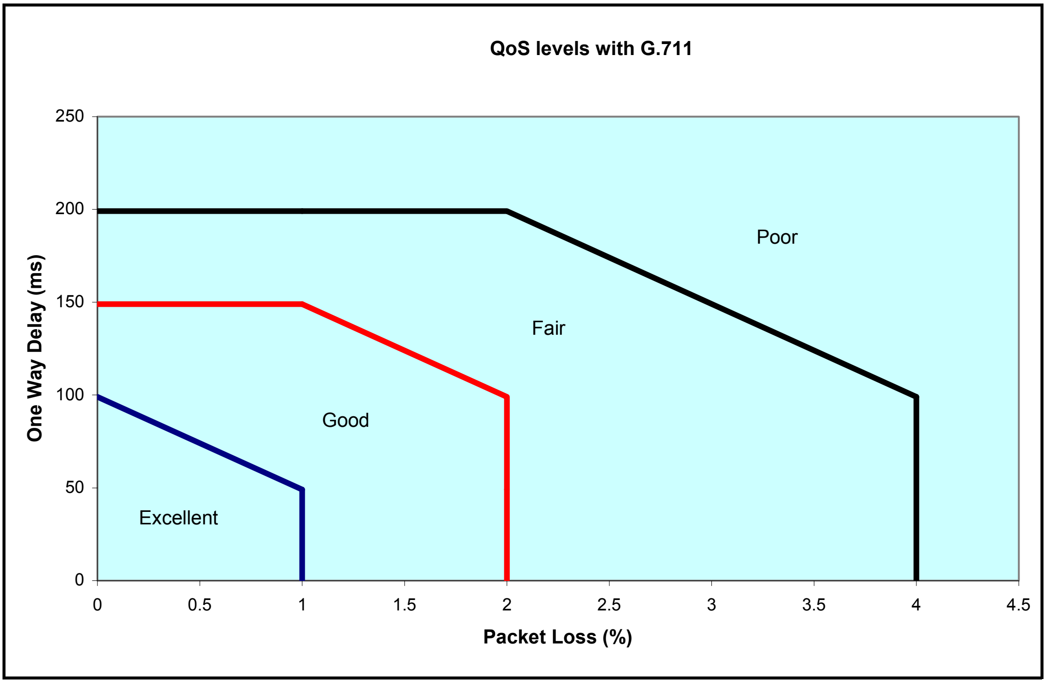


G.711 codec

G.711 is the recommended codec.

Figure 19 illustrates the QoS levels with a G.711 codec.

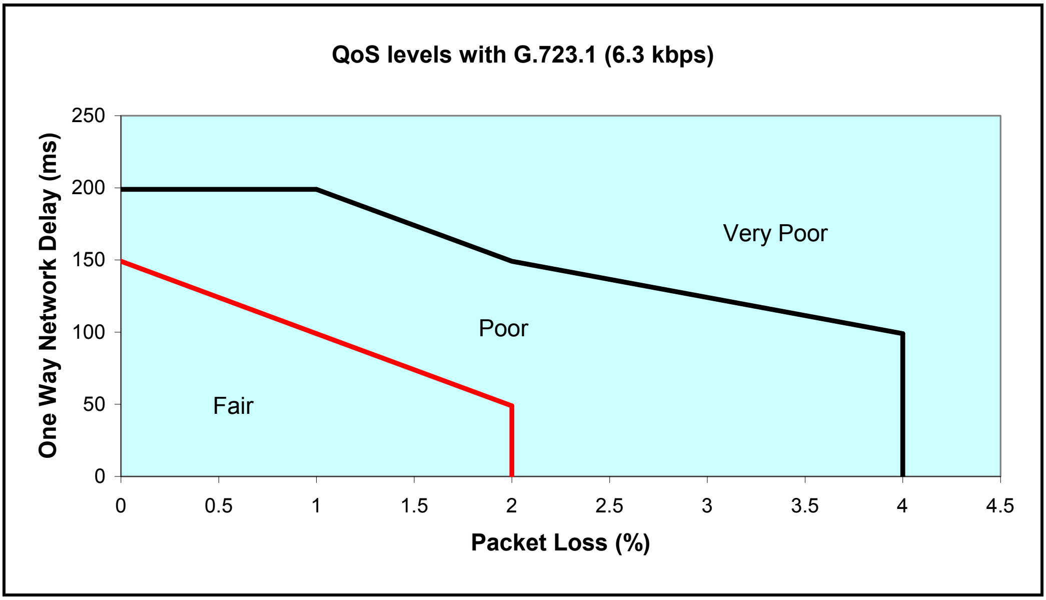
Figure 19
QoS level with G.711 codec



G.723 codec

Figure 19 illustrates the QoS levels with a G.723 codec.

Figure 20
QoS level with G.723 codec



Network performance measurement tools

PING and Traceroute are standard IP tools that are usually included with a network host's TCP/IP stack. A survey of QoS measurement tools and packages, including commercial ones, can be found in the home page of the Cooperative Association for Internet Data Analysis (CAIDA) at http://www.caida.org. These include delay monitoring tools that include features like the timestamping, plotting, and computation of standard deviation.

The following measuring tools are based on the ICMP (Internet Control Messaging Protocol):

- 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. They 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. In addition, these programs 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.

Network availability

Network availability has the most significant effect on QoE. 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

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.

It is necessary to engineer a survivable network to provide guaranteed network availability.

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 bandwidth available 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's SLA is met.

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 transmitting port's queue, 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 will be discarded because the queue is too full. Network delay is reduced, as voice packets are transmitted first. This minimizes delay, jitter, and loss. Perceived voice quality is greatly improved.

Calculating per call bandwidth use

Calculating VoIP traffic requirements

It is necessary to forecast the hundreds of call seconds for each hour (CCS) of traffic that the Succession 1000M, Succession 1000, and Meridian 1 systems processes through the IP Line network. CCS traffic generated by an Internet Telephone is similar to that of a digital telephone. The following procedures calculate the bandwidth required to support given amounts of traffic.

The procedures require the:

1 CCS/CCS rating of Internet Telephone

Note: For more information, refer to *Large System: Planning and Engineering* (553-3021-120).

2 number of Internet Telephones

3 number of subnets/servers accessed by the Internet Telephones

Note: Base all traffic data on busy hour requirements.

The result of the calculation provides estimated values for the following:

1 total LAN bandwidth requirement

2 WAN bandwidth requirement for each subnet or server/router

It is necessary to 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 re-routing 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. 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 and it is used to describe the total traffic volume of one hour. Network designers use these measurements to track network traffic patterns.

Follow Procedure 4 on page 111 to calculate the LAN traffic.

Procedure 4
Calculating LAN traffic

1 Total subnet traffic is the sum of (measured in Erlangs):

- number of Internet Telephones x (CCS ÷ CCS rating)
- voice gateways on Voice Gateway Media Card
- WAN connection

Note: Each source of traffic has a different CCS rating. Calculate the subnet traffic for each source of traffic and add the amounts to get the total.

2 Use the number of Erlangs to calculate the equivalent number of lines by using the calculator at the following website:

http://www.erlang.com/calculator/erlb

Note: Assume a blocking factor of 1% (0.010).

3 Find the LAN bandwidth usage (Kbps) in Table 6 on page 88, based on the Codec used for the traffic source.

4 Calculate the bandwidth of a subnet using the following calculation:

Bandwidth for each subnet equals the total number of lines multiplied by the LAN bandwidth usage:

Subnet bandwidth = Total number of lines × LAN bandwidth usage

5 Repeat step 1 to step 4 for each subnet.

6 To calculate the total LAN traffic, add the total bandwidth for each subnet calculation.

End of Procedure

LAN engineering example

The following is an example of calculating LAN bandwidth assuming half-duplex links.

Using G.729AB 30 msec, LAN bandwidth usage is 57.6 Kbps.

Formula is
Number of Erlangs = Number of Internet Telephones × (CCS ÷ 36)

1 Subnet A: 28 Internet Telephones, average 6 CCS ÷ Internet Telephone

Subnet A total Erlangs = 28 × 6 ÷ 36 = 4.66
Subnet A bandwidth = 4.66 × 57.6Kbps = 268.4 Kbps

2 Subnet B: 72 Internet Telephones, average 5 CCS ÷ Internet Telephone

Subnet B total Erlangs = 72 × 5 ÷ 36 = 10
Subnet B bandwidth = 10 × 57.6 = 576 Kbps

3 Subnet C: 12 Internet Telephones, average 6 CCS ÷ Internet Telephone

Subnet C total Erlangs = 12 × 6 ÷ 36 = 2
Subnet C bandwidth = 2 × 57.6 = 115.2 Kbps

4 Calculate the LAN Bandwidth by finding the sum of all subnet bandwidths:

LAN Bandwidth = 268.4 + 576 + 115.2 = 959.6 Kbps

WAN traffic calculations

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 Kbps on the LAN is equal to a 64 Kbps 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.

Procedure 5
Calculating WAN traffic

1. Total subnet traffic = Number of Internet Telephones x CCS/Internet Telephone.
2. Convert to Erlangs:

   Total CCS / 36 (on the half-duplex LAN)
3. Find WAN bandwidth usage (Kbps) from the “WAN Base Bandwidth” columns of Table 6 on page 88.
4. 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)

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

End of Procedure

WAN engineering example

The following is an example of calculating the WAN bandwidth.

1 Subnet A: 36 Internet Telephones, average 6 CCS/Internet Telephone

- Total Erlangs = 36 x 6/36 = 6
- For G.729AB 50 msec, WAN bandwidth usage is 14.4 Kbps.
- Subnet A WAN bandwidth = 14.4 x 6 = 86.4Kbps
- Subnet A WAN bandwidth with 30% peaking
  = 86.4 x 1.3
  = 112.32 Kbps

2 Subnet B: 72 Internet Telephones, average 5 CCS/Internet Telephone

- Total Erlangs = 72 x 5/36 = 10
- Subnet B WAN bandwidth = 14.4 x 10 = 144 Kbps
- Subnet B WAN bandwidth with 30% peaking
  = 144 x 1.3
  = 187.2 Kbps

3 Subnet C: 12 Internet Telephones, average 6 CCS/Internet Telephone

- Total Erlangs = 12 x 6/36 = 2
- Subnet C WAN bandwidth = 14.43 x 2 = 28.8 Kbps
- Subnet C WAN bandwidth with 30% peaking
  = 28.8 x 1.3
  = 37.44 Kbps

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 Kbps.
- Subnet B WAN bandwidth with ATM overhead
  = 187.2 x 1.2
  = 224.64 Kbps
- Subnet C WAN bandwidth with ATM overhead
  = 37.44 x 1.2
  = 44.93 Kbps

Note: Bandwidth values can vary slightly depending on the transport type.

——————————— ***End of Example*** ———————————

VoIP Bandwidth Demand Calculator

The VoIP Bandwidth Demand Calculator is an 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 Networks representative for the VoIP Bandwidth Demand Calculator spreadsheet. Use these parameters 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 in instantaneous bandwidth savings. 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 Kbps of bandwidth but the average bandwidth used for the entire call would be approximately 23 Kbps.

To calculate the average bandwidth, perform the following calculation:

Codec bandwidth from Table 6 on page 88 multiplied by 0.6.

When voice services with multi-channel 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 are generated due to the simultaneous voice-traffic bursts on multiple channels on the same links.

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 steps in Procedure 6 on page 117.

Before bandwidth estimation can begin, obtain the following network data:

- A network topology and routing diagram.
- A list of the sites where the Succession 3.0 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 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.

Procedure 6
Performing the bandwidth assessment procedure

1. Estimate the amount of traffic processed by the Meridian 1, or Succession 1000, or Succession 1000M system through the IP Line network. See *Capacity Engineering (*553-3001-149) / *Large System: Planning and Engineering* (553-3021-120).
2. Assess if the existing corporate intranet can adequately support voice services. See “Network design assessment” on page 27.
3. Organize the IP Line network into “zones” representing different topographical areas of the network that are separated according to bandwidth considerations. See “VoIP call admission control” on page 84.
4. Ensure that appropriate QoS measures are implemented across the network to prioritize voice packets over data traffic.

End of Procedure

To illustrate this process, the following multi-node engineering example is provided.

Table 7 summarizes traffic flow of a 4-node Succession 3.0 network.

Table 7
Example: Traffic flow in a 4-node Succession 3.0 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 8 on page 118 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 8
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 following example illustrates the calculation procedure for Santa Clara and Richardson. 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 using the following formula: (60/36)*11.2 = 18.7 kbit/s. Augmenting 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:

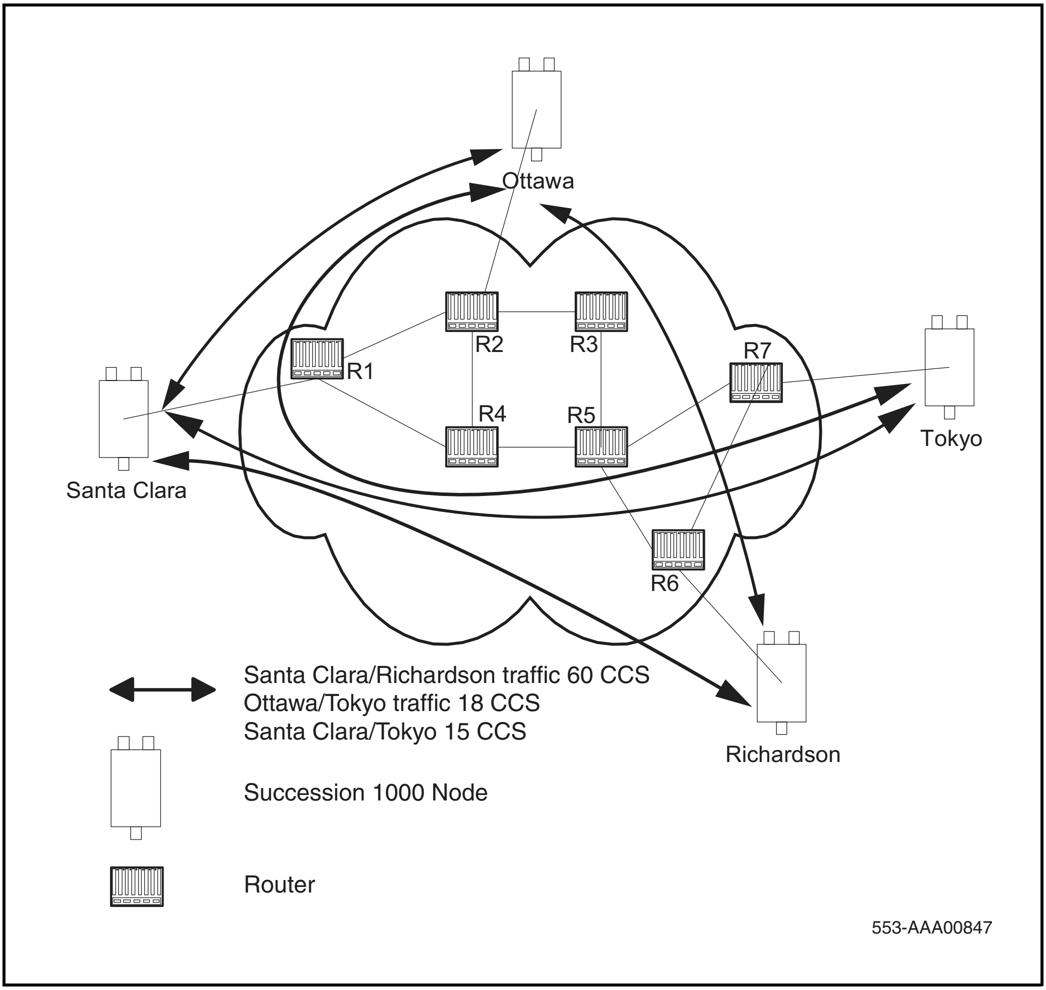
(40/36)*11.2 + (14/36)*33.6 = 25.51 kbit/s

Where 14 CCS is the larger of two fax traffic parcels (14 CCS as compared to. 6 CCS). After adjusting for peaking, the incremental data rate on WAN for this route is 33.2 kbit/s. 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 as compared to 14 CCS) will not compensate for higher bandwidth requirement of a fax as compared to voice call (33.7 kbit/s as compared to 11.2 kbit/s) in this example.

This section deals with nodal traffic calculation in both LAN and WAN. It indicates the incremental bandwidth requirement to handle voice on data networks.

At this point, enough information has been obtained to “load” the VoIP traffic on the intranet. Figure 21 on page 120 illustrates how this is done on an individual link.

Figure 21
Calculate network load with VoIP traffic



Suppose the intranet has a topology as shown in Figure 21 on page 120 and a prediction on the amount of traffic on a specific link, R4-R5, is required. From the *Large System: Planning and Engineering* (553-3021-120) NTP and Traceroute measurements, the R4-R5 link is expected to 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. The summation of the three flows yields 93 CCS or 24 kbit/s as the incremental traffic that R4-R5 will need to support.

To complete this exercise, total the traffic flow for every site pair to calculate the load at each endpoint.

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 can be 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 syntax:

```
Richardson3% traceroute -g santa_clara_itg4 richardson3
```

The Traceroute program identifies the intranet links that transmit VoIP traffic. For example, if Traceroute of four site pairs yield the results shown in Table 9 on page 122, then the load of VoIP traffic per link can be computed as shown in Table 10 on page 122.

Table 9
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 10
Route link traffic estimation

Links	Traffic from:
R1-R4	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R4-R5	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R5-R6	Santa Clara/Richardson +Richardson/Ottawa
R1-R2	Santa Clara/Ottawa + Tokyo/Ottawa
R5-R7	Santa Clara/Tokyo + Ottawa/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Enough capacity

For each link, Table 11 compares the available link capacity to the additional IP Trunk 3.0 (or later) load. For example, on link R4-R5, there is plenty of available capacity (492 kbit/s) to accommodate the additional 24 kbit/s of VoIP traffic.

Table 11
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/Richard son + Ottawa/ Tokyo + Santa Clara/Tokyo	31.4	Yes

Some network management systems have network planning modules that compute network flows in the manner just described. These modules provide more detailed and accurate analysis, as they can take into account actual node, link, and routing information. They also help assess network resilience by conducting link and node failure analysis. By simulating failures and re-loading network and re-computed routes, the modules indicate where the network might be out of capacity during failures.

Insufficient link capacity

If there is 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 link's bandwidth.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources are less frequent. For a more 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 an application's data to reach its intended destination. Delay causes significant QoE issues with voice and video applications. Other applications, such as Fax transmissions, simply time-out and fail with excessive delay.

Some applications can compensate for specified amounts of delay, but once that amount is exceeded, the 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 causes 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. Depends on link speed (a fixed, constant value for each link).
- Propagation delay — The 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 milliseconds (ms). Delay becomes annoying at the following levels:

- for G.711 codec, 250 ms
- for G.729AB codec, 150 ms

Figure 22 on page 126 shows the mechanisms that cause delay, and the technologies to counter it.

Figure 22
Sources of packet delay

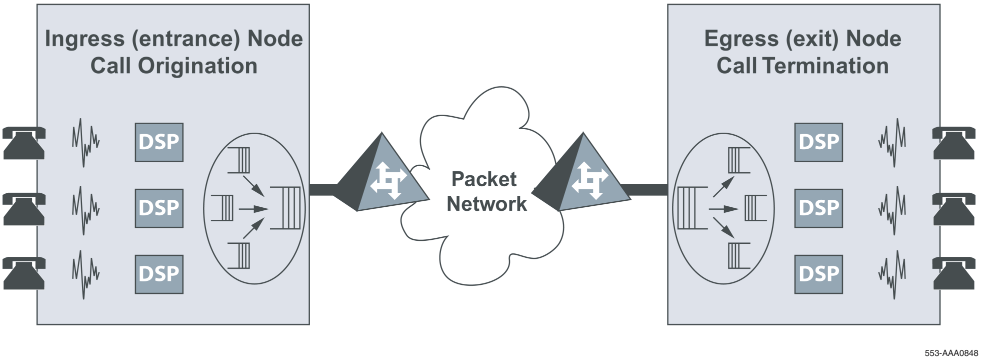


Table 12 lists the network elements where delay occurs, and the characteristics of that delay.

Table 12
Delay characteristics of voice traffic (Part 1 of 2)

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

Table 12
Delay characteristics of voice traffic (Part 2 of 2)

Packet action	Network element	Delay type
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

Note: Table 12 does not account for enhanced applications, such as packet encryption, tunnelling, and Virtual Private Networks (VPNs), which adds delay due to the buffering of the extra payload, additional Digital Signal Processing (DSP), and from repacketization. These contributions to extra delay 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 be longer than 150 ms for good quality voice over landline 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 resulting in poorer 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.

To better understand the effects of delay on voice quality, refer to Figure 17 on page 100, Figure 18 on page 103, and Figure 19 on page 104.

Components of delay

End-to-end delay is caused by many components. The major components of delay are as follows:

- Propagation delay
- Serialization delay
- Queuing 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 trans-oceanic 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:

The following calculation is used to measure serialization delay in ms.

8 * (IP packet size in bytes) / (link bandwidth in kbit/s)

Table 13 shows the serialization delay (in ms) for different packet sizes and link speeds.

Table 13
Serialization delay characteristics (in ms) for different packet sizes and link speeds

Link speed in Kbps	Packet size									
	40 bytes	**80 bytes**	**88 bytes**	**136 bytes**	**184 bytes**	**232 bytes**	**280 bytes**	**520 bytes**	**1 Kbyte**	**1.48 Kbytes**
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 14 shows what 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 14
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

Queuing delay

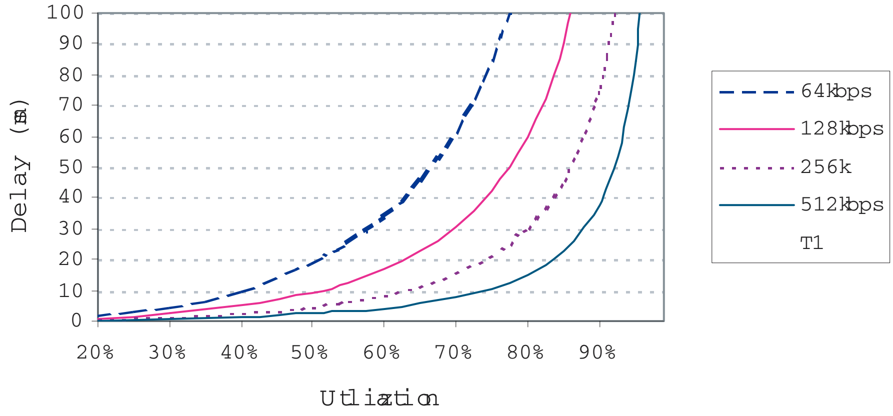
Queueing delay is the time it takes for a packet to wait in transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queueing time in ms is estimated by the following formula:

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 generally is between 250 and 500 bytes. Figure 23 displays the average queueing delay of the network based on a 300-byte average packet size.

Figure 23
Queuing delay of various links



553-AAA0850

As can be seen in Figure 23 on page 132, 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 de-packetize 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 terminating 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, generally considered minor, are as follows.

- **Router processing delay**
  The time it takes to forward a packet from one link to another on the router is the transit or router processing delay. 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 is just one or two milliseconds.

Measuring end-to-end network delay

End-to-end delay and error characteristics of the intranet must be measured so the technician can set realistic QoS expectations for intranet voice services.

The basic tool used in IP Line 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. IP Trunk 3.0 (or later) allows the 8-bit DiffServ/TOS field to be set to any value specified by the IP network administrator for QoS management purposes. For example, if a decimal value of 36 is entered in OTM 2.0, this is interpreted as TOS Precedence = Priority and Reliability = High. If PING measurements are made on an intranet that uses prioritization based on the TOS field, the rtt measured will be higher than the actual delay of voice packets when the -v option is not used. See “Queueing” on page 109.

> ***Note:*** Ensure that the ITG network DiffServ bytes are set to their intended operational values before taking measurements.

To ensure the delay sample results are representative of the IPLine_Node1 (see “Sample PING output:” on page 135):

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
```

Note: PING results can vary.

Assessment of sample PING output

Note: The round-trip time (rtt) is indicated by the time field.

The rtt from the PING output varies. It is from repeated sampling of rtt that a delay characteristic of the intranet can be obtained. To obtain a delay distribution, the PING tool can be embedded in a script that controls the frequency of the PING probes, timestamps and stores the samples in a raw data file. The file can then be analyzed later using a spreadsheet or another application. The technician can also check if the intranet's network management software has any 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 5 on page 33). 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's peak hour. For a complete assessment of the intranet's delay characteristics, obtain PING measurements over a period of at least one week.

Adjusting PING measurements

One-way and round-trip

PING statistics are based on round-trip measurements, while the QoS metrics in the Transmission Rating model are one-way. Divide the delay and packet error PING statistics in half to ensure the comparison is valid.

Adjustment due to IP Line processing

The PING measurements are taken from PING host to PING host. The Transmission Rating QoS metrics are from end-user to end-user, and 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.

> ***Note:*** 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.

Other measurement considerations

The PING statistics described above measure the intranet prior to IP Trunk 3.0 (or later) installation, which means that the measurement does not take into consideration the expected load created by the IP Trunk 3.0 (or later) users.

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 the section "Estimate network loading caused by VoIP traffic" on page 116.

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. This reduces the serialization delay of the packet, but also reduces the utilization of the link and the queueing delay. Before upgrading a link, the technician must check both routers connected to the link to be upgraded and ensure compliance with router configuration guidelines.
- Implementing QoS mechanisms.

To determine the links for upgrading, list all the 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 most used links and the slowest links. Estimate the link delay of suspect links using the Traceroute results.

Example: A 256 Kbps link from router1 to router 2 has a high utilization. The following is a Traceroute output that 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 about 40 ms; the one-way link delay is about 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of this link's delay is due to queueing.

Reducing hop count

Consider the current network topology and whether a more efficient design which reduces hop count can be implemented. Reducing hops reduces the fixed and variable IP packet delay and improves the Voice over IP QoS. It may also simplify the 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 the 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
```

The Traceroute program 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, as illustrated in the following command:

```
ipline_node1% traceroute -g subnetA ipline_node1
```

Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation might overlook a substantially better route. A high delay variation can be caused by routing instability, misconfigured 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 these routing anomalies. Then routing implementation and policies can be audited and corrected.

Jitter

Jitter 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 for packet flow (the absolute fastest time for a voice packet to pass through the network), and a variation as well. The variation in the delay is jitter. Jitter is also known as variable delay.

The primary cause of jitter (variable delay) is contention (competing 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 results, 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 Internet Telephones 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 higher levels of jitter, within a limited range, during periods of higher 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. This is due to the differences in delay created by 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. Since 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 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 a 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 Mbps), the larger data packets introduce queuing delay to the smaller voice packets waiting to be queued 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 (queuing delay).

Jitter buffers

When voice and data packets share a high-speed connection (> 1 Mbps), the variable queuing delay (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. This is done 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.

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 msec
- the jitter buffer is set to a nominal (or average) value of 40 msec
- then the maximum value is 2 x 40 + 50 = 130 msec

Therefore, any packet with a one-way delay of greater than 130 msec 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.

The jitter buffer setting is configured on the voice gateway channels of the Voice Gateway Media Card and are sent out to Internet Telephones. The jitter buffer size is set when you configure the DSP Profiles:

- in the OTM IP Line 3.1 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 milliseconds. The default jitter buffer value is 50 milliseconds. 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 set in the DSP Profile tab. As each call is set up, the jitter buffer for each device is set to the nearest whole number increment of the selected codec frame size.

For example, if the jitter buffer is configured as the default 50 msec in the DSP Profiles, but a 20 msec codec is used, the jitter buffer is set to 60 msec, which is the nearest whole number increment.

50 msec / 20 msec = 2.5
2.5 rounded up to the nearest whole number increment is 3
3 x 20 msec = 60 msec

If the jitter buffer is configured as zero, the depth of the jitter buffer is set to the smallest value the device can support. In practice, the optimum depth of the jitter queue is different for each call. For 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 poorer 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 originating 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 set the set the jitter buffer size smaller than 2s.

The Internet Telephone firmware must also be configured for jitter buffers. However, instead of specifying the jitter buffer size in msec, it is configured with the number of frames to be held in the jitter buffer, such as 1, 2, or 3.

Recommendation

To achieve maximum voice quality, Nortel Networks recommends that Internet Telephone 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.

Packet loss

Loss is defined as 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 landline connections have very low loss, measured in Bit Error Rate (BER). Wireless connections, such as satellite, mobile, or fixed wireless networks, have a high BER. The BER can vary due to the following:

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

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

Congestion loss

Congestion loss is made up 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 bandwidth available 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). RED deliberately drops packets once 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.

> ***Note:*** 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 re-transmitted. Flow rates are not adjusted by devices that communicate through UDP.

Without discard priorities, it would be necessary to 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 sub-queues, determined by their assigned discard priority. For example, if a product supports three discard priorities, then the product's queue provides three sub-queues, 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 which can result in choppy or unintelligible speech.

Packet loss occurs in the following situations:

- during network congestion
- mis-configured LAN settings
- mis-configured clock settings
- bit errors in the network

Recommendation

To achieve maximum voice quality, Nortel Networks 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

The PING program also reports whether the ICMP packet successfully completed its round trip. Use the same PING host setup to measure end-to-end error, and in making delay measurement, 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 running PING over a greater 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 more natural. The best algorithms can repair a 20-40 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's 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 are where the packet loss is high because packets get dropped, as the packets 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 means that the router is constantly performing processing-intensive tasks, which impede the router from forwarding packets. Determine the CPU utilization threshold and check if any suspect router conforms to it. The router may need to be re-configured or upgraded.

- Saturation — Routers can be overworked when configured with too many high capacity links and too many 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. Do a similar calculation for packet loss without adjustment.

Adding a standard deviation to the mean of both delay and loss is for planning purposes. A customer might want to know whether traffic fluctuation in their intranet reduces the user's QoS.

Table 15 on page 150 provides a sample measurement of network delay and packet loss for the G.729A codec between various nodes.

Table 15
Sample measurement results for G.729A codec

Destination pair	Measured one-way delay (ms)		Measured packet loss (%)		Expected QoS level (See page 154)	
	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.

Since the algorithm implemented in IP Trunk 3.0 (or later) calculates only mean and not standard deviation, it confirms the “excellent” rating (if the objective is set for excellent, it will not fallback to alternate facilities), but the customer has up to a 50% chance of experiencing a service level inferior to an “excellent” level.

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. Refer to two ITU-T recommendations (ITU-T E.107 and E.108) for more information on the E-Model and its application.

A simplified version of the E-Model is applied to IP Trunk 3.0 (or later) 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:

$$\mathbf{R = 94 - lc - ld - lp}$$

where:
lc = codec impairment (see Table 16 on page 152)

ld = delay impairment (see Table 17 on page 152)

lp = packet loss impairment (see Table 18 on page 153)

Note: This model already takes into account some characteristics of the Internet Telephone, and therefore the impairment factors are not identical to those shown in the ITU-T standards.

Refer to Table 19 on page 153 for the translation of R values into user satisfaction levels.

Table 16
Impairment factors of codecs

Codec	Codec Impairment (Ic) (msec frames)
G.711	0
G.729A/AB	11 - 20 or 30
G.729A/AB	16 - 40 or 50
G.723.1 (5.3 Kbps)	19
G.723.1 (6.3 Kbps)	15

Table 17
Impairment factors due to network delay

Network delay* (msec)	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 18
Impairment factors due to packet loss

Packet loss (%)	Packet Lose Impairment (Ip)
0	0
1	4
2	8
4	15
8	25

Table 19
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 20 to estimate the IP Trunk 3.0 (or later) QoS level based on QoS measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10ms respectively. The techniques used to determine and apply the information in this table are Nortel Networks proprietary.

Table 20
IP Trunk 3.0 (or later) QoS levels (Part 1 of 2)

Network delay (ms)	Packet loss (%)	QoS level		
		G.711 20	**G.729A/AB 30**	**G.723.1 (6.3 Kbps) 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
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

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.

Table 20
IP Trunk 3.0 (or later) QoS levels (Part 2 of 2)

Network delay (ms)	Packet loss (%)	QoS level		
		G.711 20	G.729A/AB 30	G.723.1 (6.3 Kbps) 30
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

Scenario 1

A local LAN has the following characteristics:

- G.711 codec
- 20 msec network delay
- 0.5% packet loss

To calculate R = 94 - lc - ld - lp, use Table 16 on page 152, Table 17 on page 152, and Table 18 on page 153:

- G.711 codec: lc = 0
- 20 msec network delay: ld = 0
- 0.5% packet loss: lp = 2

Then:

R = 94 - 0 - 0 - 2

R = 92

Using Table 20 on page 154, a value of 92 means the users are very satisfied.

Scenario 2

A campus network has the following characteristics:

- G.711 codec
- 50 msecs delay
- 1.0% packet loss

To calculate R = 94 - lc - ld - lp, use Table 16 on page 152, Table 17 on page 152, and Table 18 on page 153:

- G.711 codec: lc = 0
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 4

Then:

R = 94 - 0 - 5 - 4

R = 85

Using Table 20 on page 154, a value of 85 means that the users are satisfied.

Scenario 3

A WAN has the following characteristics:

- G.729 codec
- 30 msec network delay
- 2% packet loss

To calculate R = 94 - lc - ld - lp, use Table 16 on page 152, Table 17 on page 152, and Table 18 on page 153:

- G.711 codec: lc = 11
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 8

Then:

R = 94 - 11 - 5 - 8

R = 70

Using Table 20 on page 154, a value of 70 means some users are dissatisfied.

Does the intranet provide expected voice quality?

At the end of this 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 15 on page 150, 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. Often this involves a link upgrade, a 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 that 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.

Recommendation

Nortel Networks recommends a minimum R-value of 70.

Server LAN design

Contents

This section contains information on the following topics:

Introduction 163

ELAN and TLAN subnets 164

ELAN subnet 164

TLAN subnet 166

Ethernet requirements 167

General LAN considerations 167

TLAN Ethernet connections 168

ELAN Ethernet connections 168

Network Interface Card (NIC) names 168

ELAN/TLAN half- and full-duplex operation 170

Spanning Tree options on Layer 2 switches 171

How to avoid system interruption 171

Duplex mismatch 171

I/O filter connector 172

IP address requirements 174

General requirements for a node’s IP addressing 174

Succession Call Server IP address requirements 176

Succession Signaling Server IP address requirements 176

Gatekeeper IP address requirements 177

Voice Gateway Media Card IP address requirements 177

ELAN and TLAN subnet configuration examples 178

Selecting public or private IP addresses 180

Private IP addresses 180

Public IP addresses 180

- ELAN and TLAN interfaces on a single subnet 181
- Multiple nodes on the same ELAN and TLAN subnets 182

Redundant LAN design 182

Succession Call Server to remote Succession Media Gateway requirements. 189

- Succession Call Server to Succession Media Gateway connection requirements 190
- Bandwidth planning 191
- Monitoring network behavior QoS 192
- Succession Call Server to Succession Media Gateway Packet Delay Variation jitter buffer 193

Sample system layout 195

Introduction

This chapter describes the requirements for creating and maintaining a robust, redundant network.

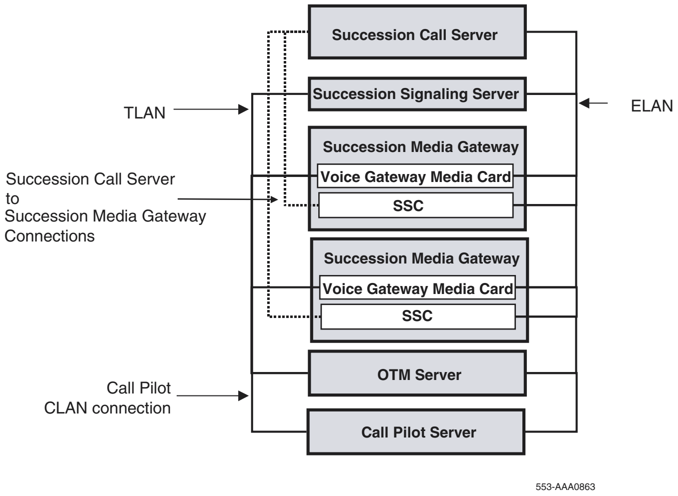
The system requires two separate sub-networks to operate. In order to differentiate the two sub-nets and the corresponding interface on each device, they where named:

- ELAN
- TLAN

Figure 24 illustrates the logical elements of basic system connectivity in a Succession 1000 network.

Figure 24
Example: Succession 1000 logical connectivity

- **Logical** server connectivity.



Note: Every device, with the exception of the Succession Call Server, has an ELAN and a TLAN interface. The Succession Call Server has a single ELAN interface and up to four Succession Call Server-to-Succession Media Gateway interfaces. The Succession System Controller (SSC) in the Succession Media Gateway has a single Succession Call Server-to-Succession Media Gateway connection and an ELAN interface.

VoIP Desktop Clients on a QoS-managed IP network are usually separate from the core system's ELAN and TLAN subnets.

ELAN and TLAN subnets

ELAN subnet

The ELAN is an isolated 10BaseT management LAN required for management traffic and signaling traffic between the Succession Call Server, the Succession Signaling Server, as well as the Succession System Controllers (SSCs) and Voice Gateway Media Cards in the Succession Media Gateways. All core signaling is done over the ELAN.

The Succession Media Gateway ELAN connections include the Succession Media Gateway SSC ELAN connection and the Voice Gateway Media Cards ELAN connection. Other cards could also require ELAN connections.

All ELAN connections must be in an isolated broadcast domain. Connect all ELAN connections to an isolated ELAN or a Virtual LAN (VLAN). This reduces the risk of network outage due to broadcast storms.

For maximum redundancy, connect the following to a backup Layer 2 switch:

- the Succession Media Gateway designated as the alternate Succession Call Server
- the redundant Succession Signaling Server

For more information on survivability, see "Redundant LAN design" on page 182.

Connect the ELAN network interface cards (NICs) from other applications, such as CallPilot and Symposium Call Center, to the ELAN subnet.

Recommendation

Nortel Networks recommends that the Optivity Telephony Manager (OTM) server/Element Manager workstation be deployed on the ELAN when managing a single system. Refer to *Optivity Telephony Manager: Installation and Configuration* (553-3001-230) for information on connecting the OTM server to the ELAN.

The ELAN subnet carries management and signaling data. The ELAN subnet connects the Succession Call Server, Succession Media Gateway SSCs, Succession Signaling Server(s), and Voice Gateway Media Card(s). The ELAN is not usually routed, but in special cases, such as remote access, limited access can be implemented.

The management workstation is usually on the ELAN subnet to achieve the highest degree of system security. The ELAN subnet can be isolated or non-routable. If a single management workstation is required to manage multiple systems, then the management workstation can be deployed on the TLAN subnet or elsewhere on the enterprise network. Remote access to the ELAN subnet should be restricted to the management workstation.

TLAN subnet

The TLAN is a 100BaseT full-duplex LAN that connects all Voice Gateway Media Cards and Succession Signaling Servers within an IP Telephony node. An IP Telephony node is defined as a logical grouping of Voice Gateway Media Cards and Succession Signaling Servers.

Recommendation

Nortel Networks recommends that the TLAN subnet carry only Succession-specific traffic and be separated from customer traffic by a Layer 3 switch. Deploy the Internet Telephones on the client side of the (the enterprise IP customer’s IP network).

A single IP telephony node cannot be a member of more than one subnet/VLAN. However, a VLAN can have more that one IP Telephony node as a member.

Succession Call Server to Succession Media Gateway connections can also be made on the TLAN.

Recommendation

Nortel Networks recommends using a point-to-point cross-over cable to connect the Succession Call Server to the Succession Media Gateway.

For reliable performance and more security, isolate the TLAN subnet from other subnets in the network.

Recommendation

Nortel Networks recommends that customers configure the TLAN subnet as a separate subnet.

The TLAN can share a subnet/VLAN with other applications' Customer LAN (CLAN) connections, such as CallPilot and Symposium, to simplify core network implementation. Nortel Networks recommends that this subnet still be isolated.

WARNING
The ELAN and TLAN NICs must be connected to Layer 2 switches. Shared-media hubs are not supported, as they are typically unreliable and are low bandwidth devices which can cause unpredictable voice quality.

Port prioritization is recommended for all TLAN connections. For detailed information on port prioritization, see the chapter. The TLAN primarily carries VoIP traffic. It connects the Succession Signaling Server and Voice Gateway Media Card(s) within a single node. The CLAN network interfaces from applications such as CallPilot is also be connected to the TLAN subnet.

Ethernet requirements

Careful consideration must be given to the Layer 2 infrastructure that the system is connected to. This section discusses issues that must be considered when designing the server LAN which connects a system to the IP network.

General LAN considerations

Passive Ethernet hubs are not supported. Use Layer 2 Ethernet switches for both the ELAN and TLAN. Ideally, managed switches should be used.

The general requirements are as follows:

- no foreign broadcast coming from other subnets
- no BootP relay agent requirement (only on ELAN subnets router interface)
- no Network Address Translation (NAT) between Internet Telephone and IP Telephony node

- the TLAN cable between the ITG-P Line Card and the Layer 2 switch must be 50 meters or less
- disable Spanning Tree on the Layer 2 switch ports connected to the ELAN and TLAN ports of the Meridian 1, Succession 1000, and Succession 1000M components

TLAN Ethernet connections

The TLAN must connect to a 10/100BaseT switch. The uplink from the TLAN to the router should be at least 100 Mbps. If the uplink is 100 Mbps, then the maximum number of IP trunk cards allowed on the switch is subject to the limits described in *Large System: Planning and Engineering* (553-3021-120).

ELAN Ethernet connections

The ELAN is 10BaseT Ethernet. Very little traffic is generated by the IP Trunk 3.0 (or later) node on this network. Cards generate this traffic when the cards are looking for the Active Leader after a reset and when SNMP traps are emitted due to IP trunk card events and errors.

The ELAN can also carry functional signaling traffic for Symposium Call Center Server (SCCS), Small Symposium Call Center (SSCC), or CallPilot multimedia message server. The ELAN can be configured on a Layer 2 switch to maximize data throughput.

Network Interface Card (NIC) names

The devices in the system have different network interface card names depending on whether is it is on the TLAN or on the ELAN subnets. Table 21 on page 169 shows the network interface card names for the Voice Gateway Media Cards (Succession Media Card and ITG-P Line Card), the Succession Signaling Server, Succession System Controller (SSC), and Call Processor Pentium (CPP).

Table 21
Network Interface Card Names

Device Type	TLAN/ELAN	Network Interface Card Name
Succession Media Card	ELAN	ixpMac1
	TLAN	ixpMac0
ITG-P Line Card	ELAN	lnIsa0
	TLAN	lnPci1
Succession Signaling Server	ELAN	fei0
	TLAN	fei1
SSC	ELAN	qu0
	TLAN	not applicable
CPP	ELAN	fei0
	TLAN	not applicable
	HSP (high speed pipe for redundant CPUs)	fei1

ELAN/TLAN half- and full-duplex operation

The ELAN NIC on the Voice Gateway Media Card operates at half-duplex only and is limited to 10BaseT operation due to filtering on the Small Systems back planes.

The TLAN NIC on Voice Gateway Media Card operates at half-duplex or full-duplex and can run at 10BaseT or 100BaseT.

It is recommended that any network equipment connected to the ELAN or TLAN NICs be set to Auto Sense / Auto Negotiate 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 even with 24 busy channels, VAD disabled, and G.711 codec with 10ms 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 that typically exhibit as lost packets and CRC errors. The Voice Gateway Media Card cannot be hard-coded for 100BaseT/full-duplex operation, and as a result the card's TLAN NIC operates in Auto Negotiate mode. Duplex mismatches and lost packets occur if the TLAN NIC interface is not configured properly.

⚠ **CAUTION**

Duplex mismatches occur in the LAN environment when one side is set to Auto Negotiate and the other is hard configured.

The Auto Negotiate side adapts only to the speed setting of the fixed side. For duplex operations, the Auto Negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

Spanning Tree options on Layer 2 switches

Nortel Networks recommends disabling the Spanning Tree option on the Layer 2 switch ports that connect to the TLAN and ELAN interfaces on the Meridian 1, Succession 1000, and Succession 1000M systems.

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 unplugged/plugged-in, can interfere with the Master Election Process in the Meridian 1, Succession 1000, and Succession 1000M system devices. In most cases the Master Election Process recovers from this after a slight delay. However, to reduce the potential of unforeseen complications in this scenario, it is recommended that the Spanning Tree option on these ports be disabled or the Port Fast option enabled.

How to avoid system interruption

Duplex mismatch

Duplex mismatches can occur in the LAN environment when one side is set to auto-negotiate and the other is hard-configured. The auto-negotiate side adapts to the fixed-side settings, including speed. For duplex operations, the auto-negotiate 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 in order to avoid duplex mismatch problems.

⚠ **WARNING**
Configure the ports on Layer 2 or Layer 3 switching equipment as **auto-negotiate**.

If one side is manually configured, and the other side is configured as auto-negotiate, the following situation occurs.

The auto-negotiate side sets itself to the manually configured side's speed, but always sets itself to half-duplex transmission. If the manually-configured side is full-duplex transmission, then a mismatch occurs and voice quality is unsatisfactory.

Recommendation

Nortel Networks recommends that network equipment connected to the ELAN or TLAN Layer 2 switches be set to Auto-Negotiate.

I/O filter connector

The other major TLAN NIC operation problem arises from the standard I/O filter connector in IPE modules on Meridian 1 Large Systems and Succession 1000M Large Systems.

Use the following guidelines to avoid system interruption stemming 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 TLAN UTP cabling must meet the UTP Cat-5 termination and impedance uniformity standards.
- The TLAN UTP cabling must not exceed 50 meters for the ITG-Pentium 24-port trunk card.

The TLAN interface can auto-negotiate to 100BaseT full-duplex. To ensure the TLAN can be used for VoIP, 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 TLAN UTP cabling to 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 in to the ITG> shell. In the shell, use the commands **tlanDuplexSet** and **tlanSpeedSet** to set the TLAN NIC to operate at half-duplex 10BaseT.

With standard PCM encoding (G.711 codec), a two-way conversation channel has a rate of 128 kbit/s (64 kbit/s in each direction). The same conversation on WAN, such as T1, only requires a 64 kbit/s channel, because a WAN channel is a full-duplex channel.

When simplex/duplex Ethernet links terminate on the ports of an Ethernet switch such as a Baystack 450, the fully duplex Ethernet up-link to the router/WAN can be loaded to 60% on each direction of the link.

IP address requirements

This section describes the IP address requirements for each node, for each card, and for each Internet Telephone.

A node is a group of ITG-P Line Cards and Succession Media Cards within a given Meridian 1, Succession 1000, and Succession 1000M system. Each card within a node has two IP addresses: for the Telephony LAN (TLAN) NIC and for the Meridian 1, Succession 1000, and Succession 1000M Embedded LAN (ELAN) NIC. Each node has one Node IP address on the TLAN subnet, that is dynamically assigned to the connection server on the node Master. The Internet Telephone uses the Node IP address during the registration process.

All ELAN addresses for all nodes must be on one subnet. All ELAN addresses must be on the same subnet as the Meridian 1, Succession 1000, and Succession 1000M Core ELAN. All TLAN addresses must be in the same subnet for a given node.

General requirements for a node's IP addressing

The following is a list of IP addresses that must be assigned to configure a node:

- IP address for every TLAN interface of every Voice Gateway Media Card and Succession Signaling Server.
- IP address for every ELAN interface of every Voice Gateway Media Card and Succession Signaling Server.
- Voice LAN (TLAN) Node IP address. (This address is shared among all the cards.) This alias IP address appears dynamically on the TLAN port of one card in the node, the Leader or node Master.
- On the Succession 1000 and Succession 1000M systems, an IP address for the Signaling Server ELAN NIC and Succession Signaling Server TLAN NIC.

In addition to the IP addresses that must be assigned, additional network information must be entered:

- Management LAN (ELAN) gateway IP address
- Management LAN (ELAN) subnet mask
- Voice LAN (TLAN) subnet mask
- VLAN gateway IP address

CAUTION
You must use separate subnets with the Voice Gateway Media Card for ELAN and TLAN.

The default setting of separate ELAN and TLAN subnets offers the benefit of protecting the ELAN from general LAN traffic, including broadcast and multicast storms. It may also protect the Succession Call Server from unauthorized access from the customer's enterprise network.

Recommendation

Nortel Networks recommends using separate dedicated VLANs and subnets for the ELAN and TLAN, separated by a router/Layer 3 switch.

If it is necessary to use a single subnet for the ELAN and TLAN, refer to “ELAN and TLAN interfaces on a single subnet” on page 181.

CAUTION
To provide backward compatibility, the user interface permits you to choose whether to use separate subnets. It is, however, mandatory to use separate subnets.

Table 22
IP Address Requirements

For the IP address requirements for the...	See...
Succession Call Server	page 176
Succession Signaling Server	page 176
Gatekeeper	page 177
Voice Gateway Media	page 177

Succession Call Server IP address requirements

The Succession Call Server IP address is the IP address of the Succession Call Server on the Embedded LAN (ELAN) subnet. The Succession Call Server ELAN NIC's IP address must correspond to the Active ELNK IP address configured in LD 117. It must be in the same subnet as the IP Line node.

- one IP address for the Succession Call Server's ELAN connection
- two IP addresses for each daughterboard link on Succession 1000M Small System:
  - one IP address is on the Succession Call Server
  - the other IP address is on the Succession Media Gateway SSC

Succession Signaling Server IP address requirements

The Succession Signaling Server is a TLAN network interface and an ELAN network interface.

- one IP address for the Succession Signaling Server's ELAN connection
- one IP address for the Succession Signaling Server's TLAN connection

The IP address is configured from the Succession Signaling Server installation CD-ROM menu. Follower Succession Signaling Servers are configured using Element Manager running on the Leader Succession Signaling Server. For more information about the Succession Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Gatekeeper IP address requirements

The Gatekeeper software can be run on a Succession Signaling Server in stand-alone mode with no other applications or it can optionally run in co-resident mode along with other Succession Signaling Server applications such as the Line TPS and H.323 Gateway.

In the case of a co-resident gatekeeper, the Succession Signaling Server IP address requirements apply:

- one IP address for the Succession Signaling Server's ELAN connection
- one IP address for the Succession Signaling Server's TLAN connection

In the case of a standalone gatekeeper, only a single TLAN ethernet connection is required. A node IP address and a TLAN IP address must be configured on the standalone gatekeeper.

An ELAN ethernet connection 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.

The Gatekeeper IP address is the TLAN IP address of the Succession Signaling Server.

The ELAN, TLAN, and Gatekeeper IP addresses are configured from the Succession Signaling Server installation CD-ROM menu. Follower Succession Signaling Servers are configured using Element Manager running on the Leader Succession Signaling Server.

Voice Gateway Media Card IP address requirements

You must provide an IP address for an ELAN and TLAN port. All cards must be on the same ELAN subnet, which is the same subnet that the system is connected to. All cards in a node must be on the same TLAN subnet.

The ELAN IP 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 or OTM.

You must use separate subnets for the IP Telephony node. Each Voice Gateway Media Card configuration requires the following:

- Management (ELAN NIC) IP address
- Voice (TLAN NIC) IP address
- Management MAC address
- Voice LAN gateway IP address

ELAN and TLAN subnet configuration examples

The following restrictions apply:

- The Leader 0 and Leader 1 cards must co-reside on a single TLAN subnet with the Node IP Address.
- Follower cards can reside on separate TLAN subnets.
- All devices must co-reside on the same ELAN subnet as their respective Succession 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 IP	10.0.0.136
ELAN GW	10.0.0.129
ELAN Subnet Mask	255.255.255.128
TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57

TLAN GW	10.0.0.1
TLAN Subnet Mask	255.255.255.0

The ELAN range of addresses – 10.0.0.129 to 10.0.0.255 – overlaps the TLAN range of addresses – 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 when adding a Succession Media Card 32-port trunk card to an existing ITG Trunk 2.x node that consists of ITG 24-port trunk cards and ITG 8-port trunk cards.

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 IP	10.0.0.136
ELAN GW	10.0.0.129
ELAN Subnet Mask	255.255.255.128

TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57
TLAN GW	10.0.0.1
TLAN Subnet Mask	255.255.255.128.

The TLAN subnet has a range of addresses from 10.0.0.1 to 10.0.0.127. The ELAN 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 fulfills the requirement that subnets do not overlap.

Selecting public or private IP addresses

Consider a number of factors to determine if the TLAN and ELAN subnets will use private (internal IP addresses) or public IP addresses.

Private IP addresses

Private IP addresses are internal 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 set up 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 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 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 re-numbering an existing private IP address autonomous domain. NAT allows private IP addresses to be accessed selectively over the internet.

> ***Note:*** Do not NAT the TLAN subnet.

Public IP addresses

Public IP addresses can be used for the TLAN and ELAN, but consume limited resources.

This has the same result as the private IP address solution, but the ELAN subnet is accessible from the internet without NAT.

ELAN and TLAN interfaces on a single subnet

IP Trunk 3.0 (or later) supports the use of a single ethernet interface (the ELAN interface). The Succession 1000 system does not have this option.

Single subnet configuration implies the configuration and use of just one Ethernet interface, namely the ELAN interface, over which all voice and management traffic is routed. Single subnet configuration can also mean configuring both the TLAN and ELAN interfaces to be in the same subnet. Neither configuration is supported. The configuration of the ELAN and TLAN NICs must be done such that both interfaces are used and the assigned IP addresses are in different subnets. Similarly, all traffic would be routed out of the ELAN ethernet interface.

Separate or dual subnet configuration implies the configuration of both the TLAN and ELAN interfaces. All management traffic is routed out the ELAN NIC, while all telephony traffic is routed out the TLAN NIC.

> ***Note:*** When using separate subnets as recommended, the Network Activity LEDs provide valuable maintenance information for the Ethernet voice interface. When using an ITG-Pentium 24-port trunk card in a single subnet configuration, all traffic uses the ELAN. This eliminates the use of the Ethernet voice (TLAN) port.

Although not recommended, the “single subnet” option for voice and management could be used in the following situations:

- The combined voice and management traffic on the ELAN 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):

1. Several IP Trunk 3.0 (or later) nodes belonging to the same customer and related to the same Nortel Networks PBX can be configured to route calls with different codecs depending on the digits dialed or the NCOS of the originating telephone. It can also be configured to limit the maximum number of IP Trunk 3.0 (or later) calls to a particular destination node. The traffic engineering considerations on the TLAN should determine how many different IP Trunk 3.0 (or later) nodes can be configured on the same LAN segment.
2. Layer 2 (10BaseT or 100Base TX) switching equipment or ATM infrastructure can support a Virtual LAN (VLAN) segment that is distributed across a campus or larger corporate network. In this case, some or all of the ITG destination nodes can be on the same subnet.
3. In test labs, training centers, and trade shows, it is common for destination nodes to be located on the same LAN segment and subnet.

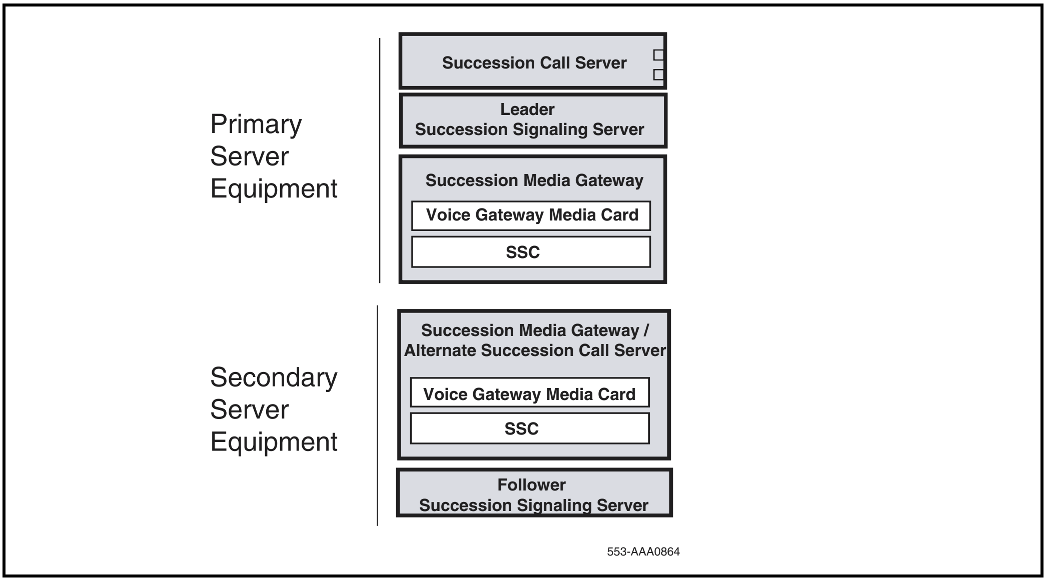
Do not place other IP devices, from Nortel Networks or another vendor, on the same TLAN subnet as the IP Trunk 3.0 (or later) nodes.

Redundant LAN design

A redundant network is defined as a network that has one or more backup systems or elements available for processing or transmission in case of system or element failure.

To begin planning for redundancy, group equipment into primary and secondary groupings, as shown in Figure 25 on page 183.

Figure 25
Primary and secondary groupings


Primary Server Equipment
Succession Call Server
Leader Succession Signaling Server
Succession Media Gateway
Voice Gateway Media Card
SSC
Secondary Server Equipment
Succession Media Gateway / Alternate Succession Call Server
Voice Gateway Media Card
SSC
Follower Succession Signaling Server
553-AAA0864

To provide a redundant core network, follow these recommendations:

- Connect ELAN and TLAN connections for the primary core components (Succession Call Server, Leader Succession Signaling Server, and Succession Media Gateway) to the primary Layer 2 switch.
- Connect ELAN and TLAN connections for the secondary core components (Alternate Succession Call Server, Follower (secondary) Succession Signaling Server, and Succession Media Gateway) 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 Open Shortest Path First (OSPF) (recommended) protocol or Spanning Tree Protocol (STP), to multiple Layer 3 switches.

  Note: Spanning Tree Protocol (STP) convergence can cause Layer 2 switch ports to be disabled for up to 60 seconds. This can affect the entire system. In some cases, STP needs to be disabled on the switch ports directly connecting the system.

- If using a high availability, chassis-based system (for example, Passport 8100), then designate one card as the primary Layer 2 switch and another card as the secondary Layer 2 switch. Then group the ELAN and the TLAN with port-based VLANs.

  Note: Use of a single highly-available Nortel Networks Passport 8600 switch can provide a "five nines" network.

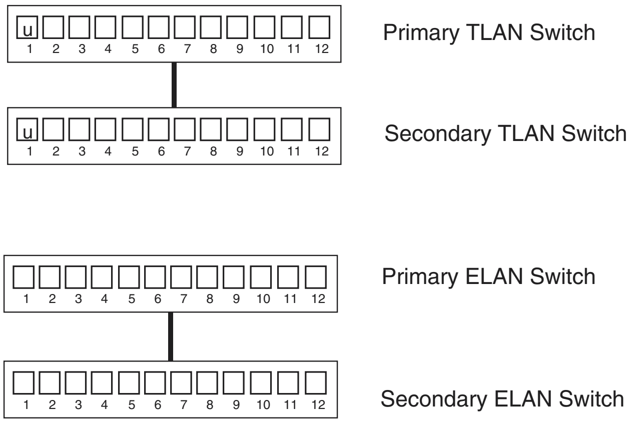
Figures 26 through 29 illustrate a network architecture that divides the core components into primary and secondary groups. Each group is connected to its own Layer 2 switch. Both the ELAN and TLAN connections are made to the group's respective Layer 2 switch. VLANs can be used to reduce the number of switches required to obtain a redundant core network.

Figure 26 on page 185 and Figure 27 on page 186 provide examples of a redundant core network that does not utilize VLANs on the Layer 2 switch infrastructure.

CAUTION
The primary and secondary TLAN must be on the same subnet and in the same broadcast domain.

The primary and secondary ELAN must be on the same subnet and in the same broadcast domain.

Figure 26
Redundant core network – no VLAN on Layer 2 switch infrastructure



Important:
The primary and secondary TLAN must be in the same sub-net and broadcast domain.

The primary and secondary ELAN must be in the same sub-net and broadcast domain.

553-AAA0865

Figure 27
Redundant core network – no VLAN on Layer 2 switch infrastructure detailed core system connections

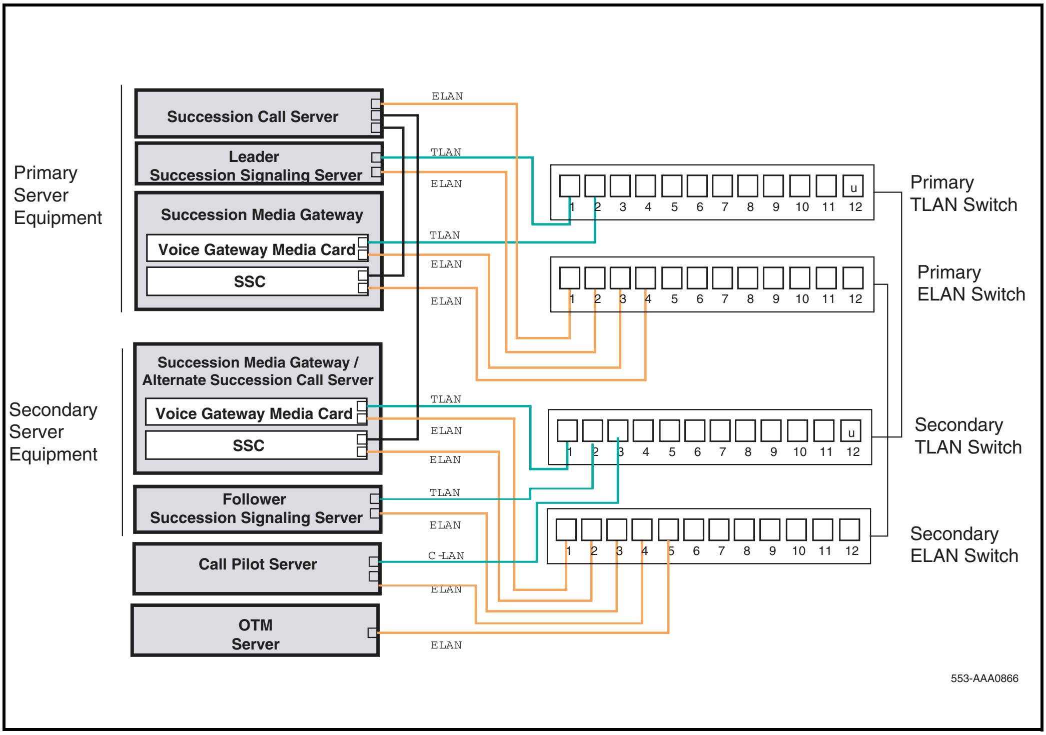


Figure 28 shows Layer 2 switch port provisioning when utilizing VLANs in the core system.

Figure 28
Redundant core network – Layer 2 switch port provisioning when using VLANs in the core system

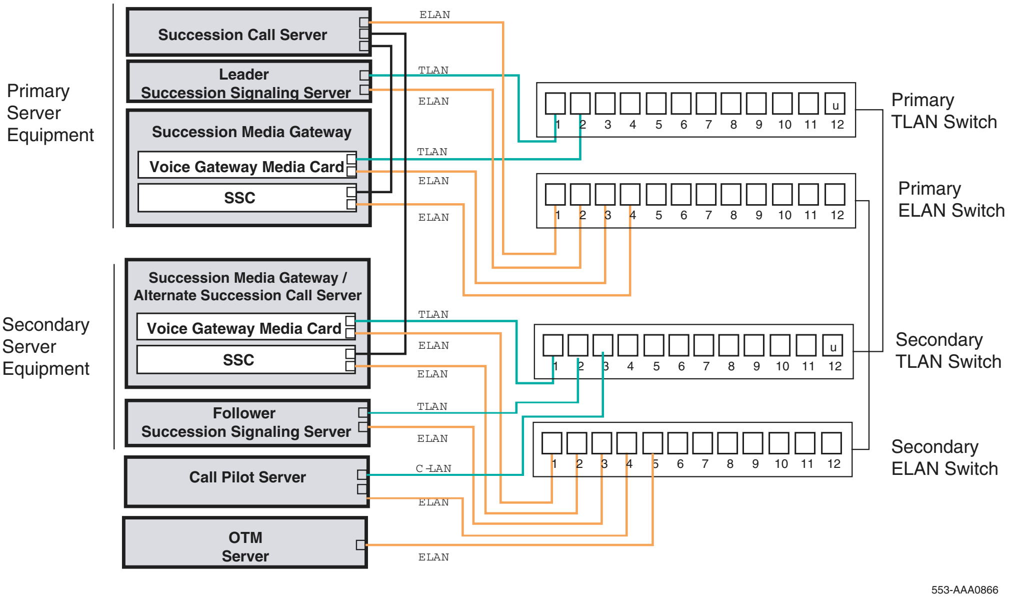
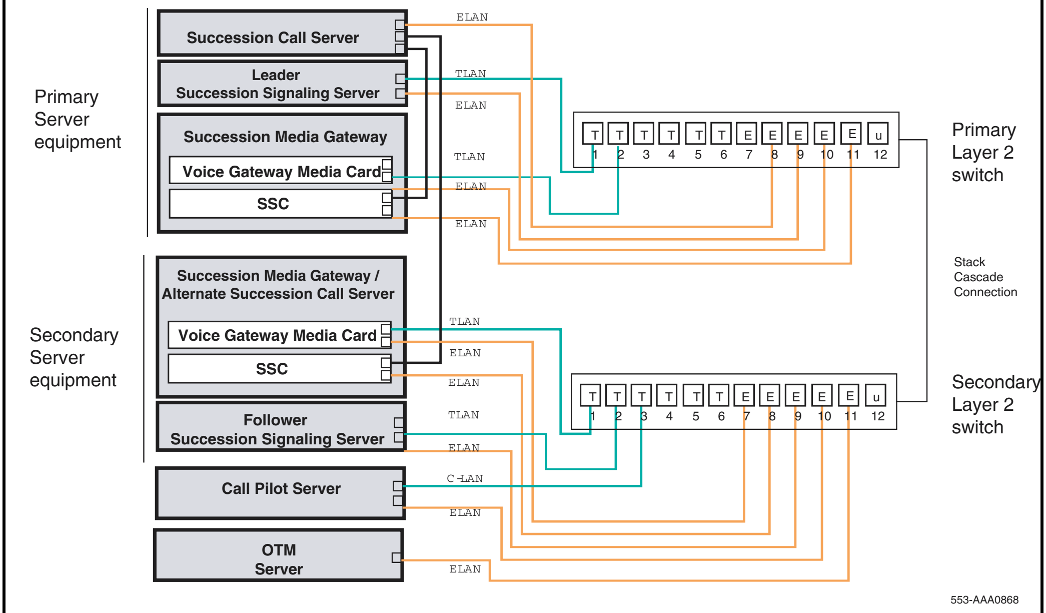


Figure 29 shows detailed core system connections in a redundant core system utilizing VLANs.

Figure 29
Redundant core network – Layer 2 switch infrastructure detailed core system connections utilizing VLANs



Succession Call Server to remote Succession Media Gateway requirements

The Succession Call Server-to-Succession Media Gateway connection exists on a segment of the TLAN. The connection links the Succession Call Server IP daughterboards to the Media Gateways SSC daughterboards. This segment is logically separate from the TLAN that connects the Voice Gateway Media Cards and the Succession Signaling Servers, although both TLANs can exist on the same LAN segment.

The Succession Call Server-to-Succession Media Gateway connections have strict requirements, due to the packetization format used over the links. Each packet contains data from multiple users. This format is efficient, though no echo cancellation is possible. To avoid echo, network delay must be very low.

WARNING
Configure the ports on Layer 2 or Layer 3 switching equipment as **auto-negotiate**.

If one side is manually configured, and the other side is configured as auto-negotiate, the following situation occurs.

The auto-negotiate side sets itself to the manually configured side's speed, but always sets itself to Half-duplex transmission. If the manually-configured side is Full-duplex transmission, then a mismatch occurs, and voice quality is unsatisfactory.

The Succession Call Server/Succession Media Gateway LAN connects the Succession Call Server to each Succession Media Gateway Succession System Controller (SSC) (see Figure 24 on page 163). In many cases, the Succession Call Server/Succession Media Gateway LAN is implemented using point-to point cabling (crossover cable) and non-routable IP addresses, but it can also operate through a Layer 2 switch.

Succession Call Server to Succession Media Gateway connection requirements

For excellent voice quality, the following requirements apply to the 100BaseTx connection between the Succession Call Server and the Succession Media Gateway SSCs:

- 100BaseT Layer 2 (or Layer 3) switch that supports full-duplex connection. Software-based routers are not supported in Succession Call Server-to-Succession Media Gateway connections.

  Note: The ports on Layer 2 (or Layer 3) switching equipment must be set to auto-negotiate ENABLED.

- packet loss < 0.5% (0% loss recommended)
- 100 Mbps full-duplex link (minimum)
  - — bandwidth usage on an idle system is negligible
  - — peak bandwidth under high voice traffic conditions (Internet Telephone to trunk calls) – 21 Mbps
- network delay – Round Trip Delay (RTD) with PDV jitter buffer set to maximum: < 5 msec
- network delay – Round Trip Delay (RTD) with PDV jitter buffer set to minimum: < 12 msec
- support of Port Priority Queuing (recommended, but not required)
- support of VLAN configuration (recommended, but not required)

Bandwidth planning

The Succession 1000 System and the Succession 1000M Small Systems are designed for non-blocking transmission between the Succession Call Server and the Succession Media Gateways. The throughput of the network must be guaranteed.

Under high traffic conditions, a peak bandwidth of 10 Mbps is used for voice traffic that requires Succession Media Gateway services, such as trunk services. See Table 23.

> ***Note:*** A minimum 100 Mbps full-duplex link is required.

If there is no traffic flow, there are negligible bandwidth requirements. Only active channels use bandwidth.

Table 23
Bandwidth Consumption/100BaseTx

Number of active conversations	Voice bandwidth (Mbps)	Signaling bandwidth (Mbps)	Total bandwidth (Mbps)
o	0	0.11	0.11
16	5.25	0.5	5.75
32	6.27	0.5	6.77
64	8.32	0.5	8.82
128	12.4	0.5	12.9
256	20.6	0.5	21.1

Note: For voice traffic that requires Succession Media Gateway services.

Monitoring network behavior QoS

Behavioral characteristics of the network depend on factors like Round Trip Delay (RTD), Packet Delay Variation (PDV) jitter buffers, queuing delay in the intermediate nodes, packet loss, and available bandwidth. The service level of each IP link is measured and maintained on the Succession Call Server.

If using cross-over cables to connect to the Succession Call Server and Succession Media Gateway, verify the active link.

Information on latency and packet loss is collected from the hardware and processed.

Based on system-configured thresholds, the level of service is compiled and reported by the **PRT QOS <cab#>** command in LD 117. See *Software Input/Output: Maintenance* (553-3001-511).

Data Network Ratings (Excellent, Good, Fair, Poor) along with the actual parameter values for network delay are displayed in Table 24.

Table 24
Campus data network voice quality measurements

Voice QoS Rating	Network Round Trip Delay (PDV Max 7.8 ms)	Network Round Trip Delay (PDV Min 0.5 ms)	Network Packet Loss
Excellent	<5 ms	<12 ms	<0.5%
Good	5 – 25 ms	12 – 32 ms	0.5 – 1%
Fair	25 – 45 ms	32 – 52 ms	1 – 1.5 ms
Poor	>45 ms	>52 ms	>1.5%

The values in Table 24 assume that there is no echo cancellation mechanism and no particular mechanism for recovering lost packets.

Succession Call Server to Succession Media Gateway Packet Delay Variation jitter buffer

The Succession Call Server to Succession Media Gateway connection Packet Delay Variation (PDV) jitter buffer ensures a constant voice playback rate, even when there is variation in the voice packet arrival rate. The PDV jitter buffer is also used to re-sequence out-of-order voice packets, and is integral to the IP-based clock recovery scheme.

The PDV jitter buffer delay is adjustable and should be as short as possible. The minimum and maximum values for excellent voice quality are given in Table 24 on page 192.

Insufficient jitter buffer delay causes a degradation in voice in the form of clicks or pops during a voice call. Insufficient delay is indicated when the QoS monitor reports buffer underflows.

If this happens, increase the size of the PDV buffer. Maximize the PDV buffer to minimize round trip delay. The goal is to operate with as smallest possible buffer. When increasing the buffer delay, increment in 0.5 msec steps until the QoS monitor no longer reports buffer underflows.

CAUTION
Excessive delay causes a degradation in voice quality in the form of additional echo.

> ***Note:*** Echo cancellers must be installed where the IP network interfaces with a TDM network that uses a 2-wire device, such as an analog loop device.

The command **PRT PDV <cab#>** in LD 117 displays both the current size of the PDV buffer and the number of PDV underflows.

In addition, a warning message is printed when a parameter threshold (or combination of thresholds) is reached. These thresholds are not user configurable.

In LD 117, the command **CHG PDV <port#> <delay>** is used to set Packet Delay Variation (PDV buffer size) on a per link basis. The **<delay>** parameter can accept values from 0.5 ms to 8 ms. This value should be initially tested at default settings. Increase the **<delay>** parameter value by 0.5 ms increments if an unacceptable level of voice quality is experienced ("pops and clicks"). Decrease this value if echo is experienced. The goal is to operate with the smallest jitter buffer possible.

The PDV jitter buffer size for each IP connection is configured at the Call Server and is automatically downloaded to the Succession Media Gateways.

Sample system layout

Figure 30 on page 195 shows a sample system layout for the Succession 1000.

Figure 30
Succession 1000 sample system layout

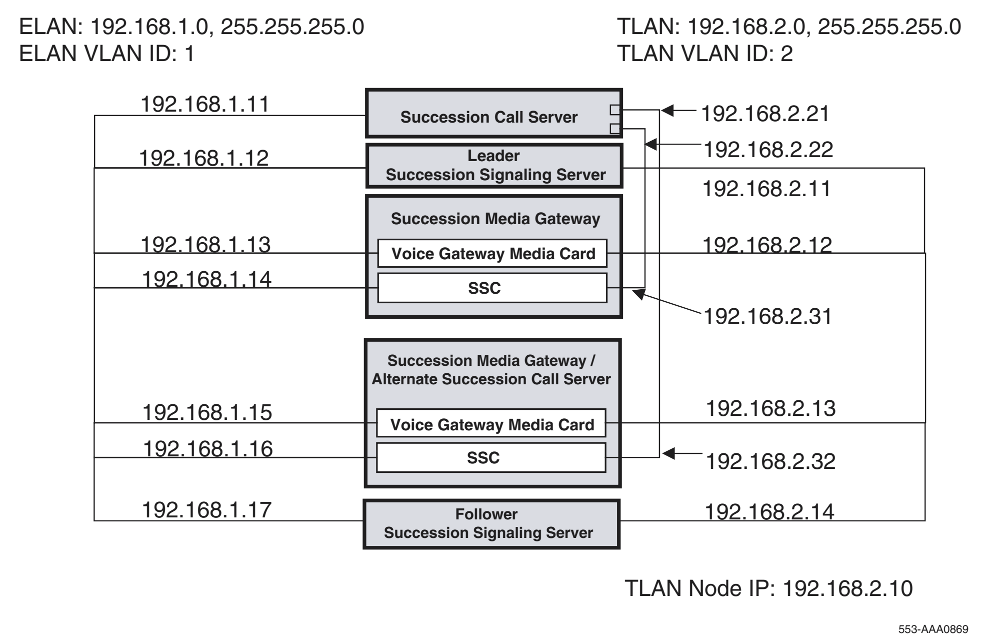


Table 25 on page 196 defines the addresses and connections.

Table 25
Sample system addresses and connections (Part 1 of 2)

Primary Gatekeeper IP	192.168.2.11	Secondary Gatekeeper IP Failsafe Gatekeeper IP	192.168.2.14 _____________	
SNMP NMS address	<ip address>			
System description	Succession 1000 core server network example			
ELAN VLAN ID	1	TLAN VLAN ID	2	
ELAN subnet	192.168.1.0	TLAN subnet	192.168.2.0	
ELAN mask	255.255.255.0	TLAN mask	255.255.255.0	
ELAN Gateway router	192.168.1.1	TLAN router	192.168.2.1	
Succession Call Server ELAN IP	192.168.1.11			
Succession Media Gateway #1 ELAN IP	192.168.1.14	Succession Media Gateway #3 ELAN IP	N/A	
Succession Media Gateway #2 ELAN IP	192.168.1.16	Succession Media Gateway #4 ELAN IP	N/A	

Table 25
Sample system addresses and connections (Part 2 of 2)

<table>
<tr><th colspan="2">Succession Call Server to Succession Media Gateway connection number</th><th>Succession Call Server IP D/B (IPM) IP address</th><th>Succession Media Gateway IP D/B (IPR) IP address</th><th>Succession Media Gateway IP D/B (IPR) MAC address</th></tr>
<tr><td colspan="2">1</td><td>192.168.2.21</td><td>192.168.2.31</td><td>00:90:cf:01:02:03</td></tr>
<tr><td colspan="2">2</td><td>192.168.2.22</td><td>192.168.2.32</td><td>00:90:cf:04:05:06</td></tr>
<tr><td colspan="2">3</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">4</td><td></td><td></td><td></td></tr>
<tr><td>Node number</td><td>1</td><td>Node IP address</td><td>192.168.2.10</td><td></td></tr>
<tr><td>Type</td><td>Card TN</td><td>ELAN MAC address</td><td>ELAN IP address</td><td>TLAN IP address</td></tr>
<tr><td>Primary Succession Signaling Server</td><td>N/A</td><td>00:60:aa:bb:cc:dd</td><td>192.168.1.12</td><td>192.168.2.11</td></tr>
<tr><td>Secondary Succession Signaling Server</td><td>N/A</td><td>00:60:ee:ff:aa:bb</td><td>192.168.117</td><td>192.168.2.14</td></tr>
<tr><td>Voice Gateway Media Card</td><td>11</td><td>00:60:aa:bb:cc”11</td><td>192.168.1.13</td><td>192.168.2.12</td></tr>
<tr><td>Voice Gateway Media Card</td><td>31</td><td>00:60:aa:bb:cc:22</td><td>192.168.1.15</td><td>192.168.2.13</td></tr>
</table>

Configuration of the DHCP server

Contents

This section contains information on the following topics:

Overview 200

i2002 and i2004 Internet Telephones, and i2050 Software Phone 200

Partial DHCP mode 201

Full DHCP mode 201

802.1Q configuration of Internet Telephones 203

Configuring the DHCP server to support full DHCP mode 203

Internet Telephone class identifier 203

Requested network configuration parameters 204

Format for Nortel Networks Internet Telephone DHCP Class Identifier option 206

Format for Nortel Networks Internet Telephone DHCP encapsulated vendor-specific option. 206

Format of the option 207

Configuration string examples. 211

Format for Nortel Networks Internet Telephone DHCP site-specific option 213

Format of the option 213

Overview

This chapter provides general guidelines on how to configure a host with a Dynamic Host Configuration Protocol (DHCP) server to support the i2002 and i2004 Internet Telephones, and i2050 Software Phone.

> ***Note 1:*** If not familiar with DHCP, Nortel Networks recommends reading 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. A convenient source for RFCs is http://www.ietf.org/.
>
> ***Note 2:*** For a general overview of DHCP server technology, refer to Appendix F: “DHCP supplemental information” on page 301.

i2002 and i2004 Internet Telephones, and i2050 Software Phone

The i2002 and i2004 Internet Telephones, and the i2050 Software Phone are Voice over Internet Protocol (VoIP) telephones that function as a telephone to the Meridian 1, Succession 1000, and Succession 1000M systems. The Internet Telephone encodes voice as binary data and packetizes the data for transmission over an IP Network to the Voice Gateway Media Card or to another Internet Telephone.

The Nortel Networks Internet Telephone can act as a DHCP client in one of two modes:

- partial DHCP mode
- full DHCP mode

Partial DHCP mode

When the Internet Telephone is configured to operate in partial DHCP mode, the DHCP server needs no special configuration to support Internet Telephones. The Internet Telephone receives the following network configuration parameters from the DHCP server:

- IP address configuration for the Internet Telephone
- subnet mask for the Internet Telephone IP address
- default gateway for the Internet Telephone LAN segment

Full DHCP mode

In full DHCP mode, the DHCP server requires special configuration. The Internet Telephone obtains network configuration parameters and Connect Server configuration parameters from specially-configured DHCP servers.

The following configuration parameters are provided for the primary and secondary Connect Servers:

- Connect Server IP address. For IP Line 3.1, the Connect Server IP address is the IP Telephony node IP address.
- port number of 4100
- command value of 1 that identifies the request to the Connect Server as originating from an Internet Telephone
- A retry count typically equal to 10

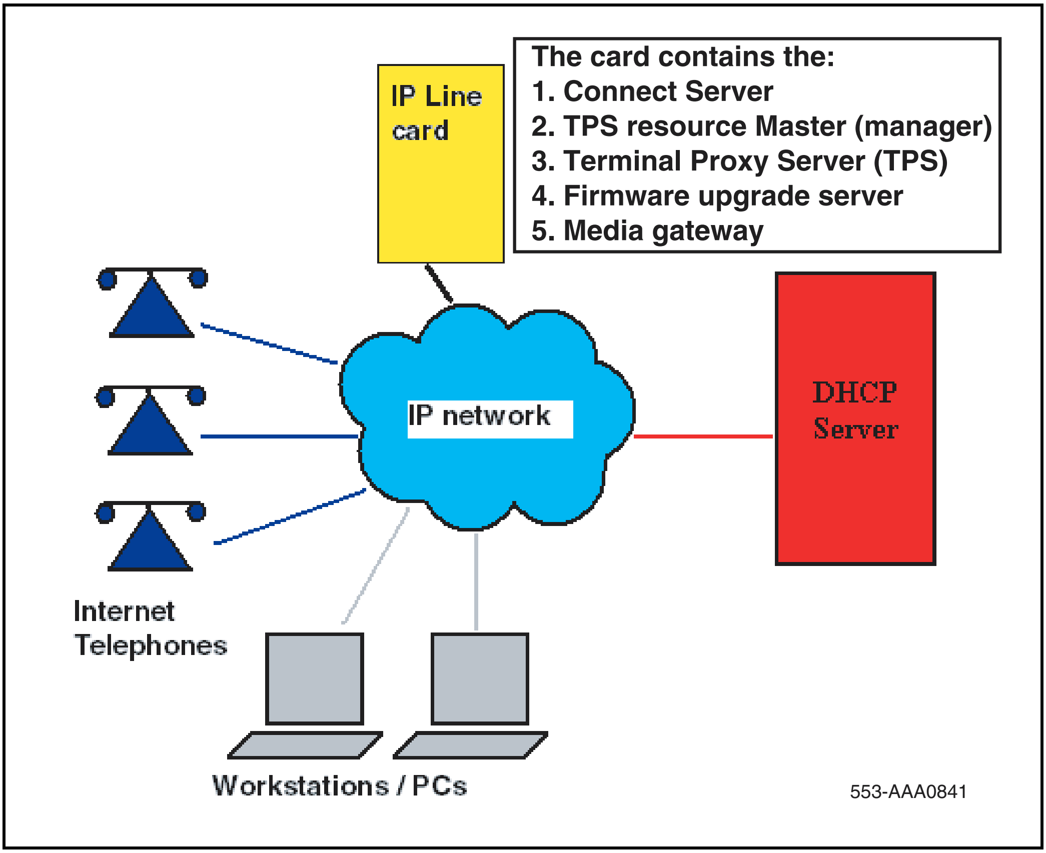
All the configuration parameters for the Internet Telephone can be entered manually. Each Internet Telephone requires the network configuration parameters, Connect Server parameters, IP Telephony node ID, and Virtual TN. If there are a number of Internet Telephones to configure, manual configuration is time consuming and error prone.

Using full or partial DHCP to automatically configure the Internet Telephones is more efficient and flexible. This ensures that current information is used.

Note 1: The IP Telephony node ID and Virtual TN must always be configured manually even in full DHCP mode.

Note 2: In partial DHCP mode the Connect Server parameters, node ID and Virtual TN must be entered manually.

Figure 31
DHCP block diagram



802.1Q configuration of Internet Telephones

The 802.1Q VLAN support is configured from the user display interface of the i2002 and i2004 Internet Telephones. This configuration takes place during the initial configuration procedure of the Internet Telephone.

For the 802.1Q configuration procedures of the Internet Telephones, see *Internet Terminals: Description* (553-3001-368).

Configuring the DHCP server to support full DHCP mode

The DHCP capability feature of the Internet Telephone enables the telephone to receive network configuration parameters and specific Connect Server parameters. This section describes the Internet Telephone's unique class identifier and requested network configuration and Connect Server parameters for automatic configuration.

Internet Telephone class identifier

The Internet Telephone is designed with a unique class identifier that the DHCP server can use to identify it. All Nortel Networks Internet Telephones use the same text string, “Nortel-i2004-A”. The ASCII string is sent inside the Class Identifier option of the Internet Telephone's DHCP messages.

The DHCP server also includes this string in its responses to the Internet Telephone DHCP client. This makes it possible to notify the Internet Telephone that the server is Internet Telephone-aware, and that it is safe to accept the server's offer. This string appears in the beginning of a list of specific Voice Gateway Media Card information that the Internet Telephone DHCP client requests.

When the DHCP server is configured to recognize the Internet Telephone as a special class, the DHCP server can treat the Internet Telephone differently than other DHCP clients. DHCP host configuration parameters can then be grouped by class and only information relevant to the Internet Telephone DHCP client, such as the Connect Server parameters, is supplied.

The administrator can design the network according to the client's class, if necessary, making maintenance easier. Depending on the capabilities and limitations of the DHCP server used and the design of the network, some of these advanced functions are not available.

Requested network configuration parameters

Nortel Networks Internet Telephones, using full DHCP mode, can be configured automatically by an Internet Telephone-aware DHCP server by requesting a list of Connect Server configuration parameters. The Internet Telephone uses DHCP, an industry standard protocol, to request and receive the information.

The Internet Telephones operating 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 26 lists the network configuration parameters requested by the Internet Telephone 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 26.

Table 26
Internet telephone network configuration requirements (Part 1 of 2)

Parameter request (Option Code 55)	DHCP option code
Subnet mask – the client IP subnet mask	1
Router/gateway(s) – the IP address of the client’s default gateway (not required in DHCPOFFER in Internet Telephone Firmware 1.25 and later for compatibility with Novell DHCP server)	3
Lease time – implementation varies according to DHCP server	51

Table 26
Internet telephone network configuration requirements (Part 2 of 2)

Parameter request (Option Code 55)	DHCP option code
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 26 are standard DHCP options and have pre-defined 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 Internet Telephone.

This non-standard information includes the unique string identifying the Internet Telephone and the Connect Server parameters for the primary and secondary servers. The Internet Telephone 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 is, or encapsulated in a Vendor Encapsulated option with option code 43. The method used depends on the DHCP server's capabilities and what options are already in use by other vendors.

The Internet Telephone rejects any DHCP Offers/Acks that do not contain the following:

- A router option. The Internet Telephone requires a default gateway (router).
- A subnet mask option.
- Either a vendor-specific option (see Note 1) or a site-specific option (see Note 2 on page 206).

Note 1: The vendor-specific option 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 Internet Telephone-specific string. If using a Windows NT DHCP Server, select the Site Specific option to accommodate the Internet Telephone-specific string.

Note 2: 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 Nortel Networks Internet Telephone DHCP Class Identifier option

All Nortel Networks Internet Telephones fill in the Class ID option of the DHCP Discovery and Request messages with the null-terminated, ASCII-encoded string Nortel-i2004-A, where A identifies the version number of the information format of the Internet Telephone.

The Class Identifier Nortel-i2004-A must be unique in the DHCP server domain.

Format for Nortel Networks Internet Telephone DHCP encapsulated vendor-specific option

The following definition describes the Nortel-specific, encapsulated vendor-specific option for the i2002 and i2004 Internet Telephones, and i2050 Software Phone. This option must be encapsulated in a DHCP vendor-specific option (refer to RFC 1533) and returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the Internet Telephone to accept these messages as valid. The Internet Telephone extracts the relevant information from this option and uses it to configure the Connect Server IP address, the port number (4100), a command value of one, 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 Internet Telephone (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 option

The format of the Encapsulated Vendor Specific option is Type, Length, and Data as shown below.

Type (1 octet):

There are five choices:

- 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)

Providing a choice of five types enables the Internet Telephone to work in environments where the initial choice could already be in use by a different vendor. Pick only 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 “Data (variable number of octets)” on page 207).

Data (variable number of octets)

The Data field contains an ASCII-encoded character string that can be optionally null-terminated. This string can be NULL terminated, although the NULL is not required for parsing. The string is:

“Nortel-i20xx-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr.”

The parameters for the data field are outlined in Table 27 on page 208.

Table 27
Data field parameters

Parameter	Description
Nortel-i2004-A	Uniquely identifies that this is the Nortel option and is a response from a server that can provide the correct configuration information to the i2002 and i2004 Internet Telephones, and the i2005 Software Phone.
ASCII characters	
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.
iii.jjj.kkk.lll:ppppp	Identifies IP address and port number for server (ASCII-encoded decimal)
aaa	Identifies action for server (ASCII encoded decimal, range 0 – 255)
rrr	Identifies retry count for server (ASCII encoded decimal, range 0 – 255)

1 "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 1 octet (0x00 – 0xFF) in the Internet Telephone. These fields must be no more than three digits long.

2 Two connect servers and an optional external application server (XAS) can be specified in the DHCP string:

— The first server is always considered "Primary".

— The second server always considered "Secondary".

— An optional external application server can be appended to the connect servers. Presently, Net6 is the external application server (see item 8 on page 210 for details).

3 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 semi-colon (;). 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, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

4 Action code values:

a 0 – reserved

b 1 – UNIStim Hello (currently this type is the only valid choice)

c 2 – 254 – reserved

d 255 – reserved

5 **iii.jjj.kkk.lll** are ASCII-encoded decimal numbers representing 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 Internet Telephone. These fields must be no more than three digits long.

6 **ppppp** is the port number in ASCII-encoded decimal. It does not need to be five digits long as the **:** and **,** delimiters guarantee parsing. For example, '05001', '5001', '1', '00001' would be parsed correctly and accepted as correct. The valid range is 0-65535 (stored internally in the Internet Telephone as hexadecimal in range 0 – 0xFFFF). This field must be no more than five digits long.

7 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.

8 When using the Full DHCP option on the i2004 Internet Telephone, the IP address of an exchange application server (XAS) (such as the Net6 Server) can be provided. To do this, append the XAS's IP address and port to the Nortel DHCP option that is currently used to specify the first and second server's IP address, ports, retry and action codes.

The format of the exchange application server's IP address and port is:
iii.jjj.kkk.lll:ppppp

Note 1: The port action code (aaa) and retry count (rrr) are not included.

Note 2: XAS always uses port 5000.

For example, 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.”
```

For more information about Net6, refer to the *i2004 Internet Telephone User Guide*.

Refer to “Configuration string examples” on page 211 for additional examples.

Configuration string examples

The following tables illustrate the configuration strings with one or more Connect Servers and exchange application servers:

- the Nortel Class Identifier is separated from the servers by a comma (,)
- the servers are separated by semi-colons (;)
- the IP address and port numbers are separated by a colon (:)
- the string is terminated with a period (.)

Table 28
Configuration string for one Connect Server

<table>
<tr><td colspan="2">Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr.</td></tr>
<tr><td>Nortel Class Identifier Field</td><td>Primary Connect Server</td></tr>
<tr><td>Nortel-i2004-A</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td></tr>
</table>

Table 29
Configuration string for two Connect Servers

<table>
<tr><td colspan="3">Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.</td></tr>
<tr><td>Nortel Class Identifier Field</td><td>Primary Connect Server</td><td>Secondary Connect Server</td></tr>
<tr><td>Nortel-i2004-A</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td></tr>
</table>

Table 30
Configuration string for one Connect Server and an XAS (such as Net6)

<table>
<tr><td colspan="4">Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp.</td></tr>
<tr><td>Nortel Class Identifier Field</td><td>Primary Connect Server</td><td>Placeholder Secondary Connect Server</td><td>XAS (such as Net6)</td></tr>
<tr><td>Nortel-i2004-A</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>iii.jjj.kkk.lll:ppppp</td></tr>
<tr><td colspan="4"><b><i>Note:</i></b> Three IP addresses must be specified when using just one Connect Server and an exchange application server (XAS).
If only two IP addresses are specified, the Internet Telephone assumes the second IP address is for the second Connect Server. The Internet Telephone does not recognize that it is for the exchange application server (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 Internet Telephone expects to find it).
Nortel Networks recommends simply repeating the IP address of the first Connect Server for the second Connect Server, to create the placeholder IP address.</td></tr>
</table>

Table 31
Configuration string for two Connect Servers and an XAS (such as Net6)

<table>
<tr><td colspan="4">Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp.</td></tr>
<tr><td>Nortel Class Identifier Field</td><td>Primary Connect Server</td><td>Secondary Connect Server</td><td>XAS (such as Net6)</td></tr>
<tr><td>Nortel-i2004-A</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>iii.jjj.kkk.lll:ppppp</td></tr>
</table>

Format for Nortel Networks Internet Telephone DHCP site-specific option

This section describes the Nortel-specific, site-specific option for the i2002 and i2004 Internet Telephones, and i2050 Software Phone. This option uses the “reserved for site specific use” DHCP options (128 to 254 - refer to RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the Internet Telephone to accept these messages as valid.

The Internet Telephone retrieves the relevant information and uses it to configure the IP address for the primary and (optionally) secondary TPSs. Either this site-specific option must be present or a similarly encoded vendor-specific option must be sent (as previously described); 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 Internet Telephone. 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 option

The format of the field is Type, Length, Data. The format of the site-specific option is the same as the encapsulated vendor-specific option (see “Format of the option” on page 207).

Operating the VoIP network

Contents

This section contains information on the following topics:

System management 216
OTM 216
Element Manager 217
Network monitoring 219
Set VoIP QoS objectives 220
Intranet QoS monitoring. 221
ITG Operational Measurements (OM) 222
OM report description 222
User feedback 223
QoS monitoring and reporting tools 224
Available tools 224
Network Management 225
SNMP Network Management Systems 225
OTM and Network Management System 226
Policy Management 226
IP Trunk 3.0 (or later) network inventory and configuration 227

System management

The system can be managed using the Optivity Telephony Manager (OTM) or Element Manager.

OTM

Optivity Telephony Manager (OTM) is an integrated suite of system management tools. Compatible with a standard PC, it provides a single point of access and control to manage the systems.

OTM uses IP technology to target the following:

- single point of connectivity to the system and related devices
- data collection for traffic and billing records
- collection, processing, distribution, and notification of alarms and events
- data propagation
- performance measurement tools (Traffic Analysis package, and Real-time Conferencing Protocol (RTCP) statistics from the Terminal Proxy Server (TPS) and Voice Gateway Media Cards)
- web-based management applications, including security

OTM can be integrated with the suite of Optivity management tools to provide comprehensive management of the voice and data network.

For more information on OTM, refer to:

- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)
- *Optivity Telephony Manager: System Administration* (553-3001-330)

Element Manager

Element Manager is a web server, with a user interface that provides an alternative to the overlay-based and command line interface.
Element Manager simplifies system management in areas such as:

- Gatekeeper services
- IP services
- IP Peer Networking configuration
- software, firmware, and patch downloads

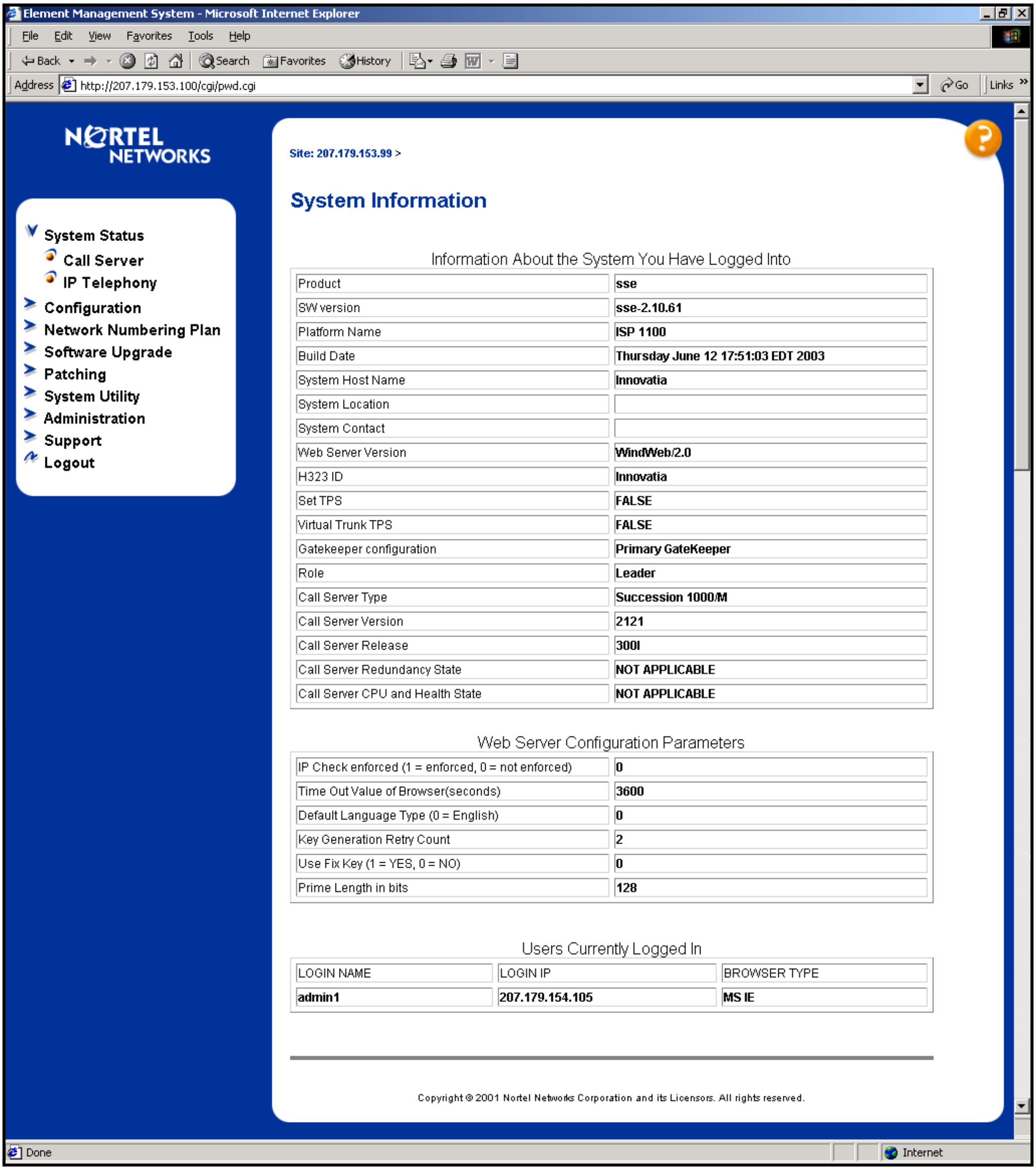
Element Manager organizes system parameters into logical groups. Single webpages provide access to information previously accessible in overlays. Parameter and acronym descriptions help reduce configuration errors. Parameter value selection is simplified through use of:

- pre-selected default values
- drop-down lists of choices
- range values indications
- Yes/No check boxes

The Element Manager user interface is shown in Figure 32 on page 218.

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

Figure 32
Element Manager user interface main menu



Site: 207.179.153.99 >

System Information

Information About the System You Have Logged Into

Product	sse
SW version	sse-2.10.61
Platform Name	ISP 1100
Build Date	Thursday June 12 17:51:03 EDT 2003
System Host Name	Innovatia
System Location	
System Contact	
Web Server Version	WindWeb/2.0
H323 ID	Innovatia
Set TPS	FALSE
Virtual Trunk TPS	FALSE
Gatekeeper configuration	Primary GateKeeper
Role	Leader
Call Server Type	Succession 1000M
Call Server Version	2121
Call Server Release	300I
Call Server Redundancy State	NOT APPLICABLE
Call Server CPU and Health State	NOT APPLICABLE

Web Server Configuration Parameters

IP Check enforced (1 = enforced, 0 = not enforced)	0
Time Out Value of Browser(seconds)	3600
Default Language Type (0 = English)	0
Key Generation Retry Count	2
Use Fix Key (1 = YES, 0 = NO)	0
Prime Length in bits	128

Users Currently Logged In

LOGIN NAME	LOGIN IP	BROWSER TYPE
admin1	207.179.154.105	MS IE

Copyright © 2001 Nortel Networks Corporation and its Licensors. All rights reserved.

Network monitoring

The design process is continual, even after implementation of the VoIP network and commissioning of voice services over the network. Network changes in the following – VoIP traffic, general intranet traffic patterns, network policies, network topology, user expectations and networking technology – can render a design obsolete or non-compliant with QoS objectives. Review the design periodically against prevailing and trended network conditions and traffic patterns, at least once every two to three weeks initially, then eventually on a quarterly basis.

It is assumed that the customer's organization already has processes in place to monitor, analyze, and re-design 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's organization must be incorporate additional monitoring and planing processes, as follows:

- Collect, analyze, and trend VoIP traffic patterns.
- Monitor and trend one-way delay and packet loss.
- Monitor Operational Measurements (see page 222)
- Perform changes in VoIP network and intranet when planning thresholds are reached.

By instituting these new processes, the VoIP network can be managed to meet desired QoS objectives.

Set VoIP QoS objectives

State the design objective of the VoIP network. This sets the standard for evaluating compliance to meeting users' needs. When the VoIP network is first installed, the design objective expectations have been set, based on the work done in “Network performance evaluation overview” on page 99. Initially, set the QoS objective so that for each destination pair, the mean+s of one-way delay and packet loss is below some threshold value to maintain calls between those two sites at a required QoS level. The graphs of Figure 18 on page 103 and Figure 19 on page 104, with the QoS measurements, help determine what threshold levels are appropriate.

Table 32 describes examples of VoIP QoS objectives.

Table 32
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.

After deciding on a set of QoS objectives, determine the planning threshold. The planning thresholds are based on the QoS objectives. These thresholds are used to trigger network implementation decisions when the prevailing QoS is within range of the targeted values. This gives time for implementation processes to follow through. The planning thresholds can be set 5% to 15% below the QoS objectives, depending 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 about every minute. The amount of load generated by this is not considered significant. At the end of the month, the hours with the highest one-way delay are noted; within those hours, the packet loss and standard deviation statistics can be computed.

See “Network performance measurement tools” on page 106 for information about where to obtain other more specialized delay and route monitoring tools.

At the end of the month, analyze each site’s QoS information. Table 33 provides a sample.

Table 33
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	Objective
Santa Clara/ Richardson	135	166	1	2	Excellent	Good	Excellent
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 the route’s performance.

ITG Operational Measurements (OM)

The Voice Gateway Media Card collects Operational Measurements from the Internet Telephones and DSP channels and saves the information to a log file every 60 minutes. The Operational Measurements include:

- Internet Telephone Registration Attempted Count
- Internet Telephone Registration Confirmed Count
- Internet Telephone Unregistration Count
- Internet Telephone Audio Stream Set Up Count
- Internet Telephone Average Jitter (msec)
- Internet Telephone Maximum Jitter (msec)
- Internet Telephone Packets Lost/Late (%)
- Internet Telephone Total Voice Time (minutes and seconds)
- Gateway Channel Audio Stream Set Up Count
- Gateway Channel Average Jitter (msec)
- Gateway Channel Maximum Jitter (msec)
- 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 the OTM server. Using OTM you can run an adhoc report or schedule a regular report. 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 standard deviation statistics generated. Compare the data to target network QoS objectives.

Declines in QoS can be observed through the comparison of QoS between last period and current period. A consistent, inferior measurement of QoS compared with 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. Files are automatically deleted 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 Helpdesk 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). This means there is greater delay experienced per hop. If there are low bandwidth links in the path, then the one-way delay is noticeably higher in terms of average and variation.

QoS monitoring and reporting tools

These tools monitor and report on 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 on-going basis, other more intrusive tools are used to generate synthetic VoIP traffic. The more intrusive tools are similar to those used to perform pre-sales network assessments.

Nortel Networks recommends the 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.

Available tools

Some examples of QoS monitoring and reporting tools include:

- NetIQ Chariot^{TM}
- RMON
- MultiRouter Traffic graphing tool
- SNMP NMS traffic reports

For more detailed information regarding specific QoS assessment, monitoring and reporting tools available, please contact your Nortel Networks sales representative.

Network Management

SNMP Network Management Systems

Simple Network Management Protocol (SNMP)-based Network Management Systems (NMS) provide a useful way of monitoring a real-time network from end-to-end. This is important for networks using VoIP. User complaints of slow downloads are no longer enough to diagnose problems. NMS can ensure 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
- centralized alarm management through SNMP traps
- notify network administrators of problems

IP Trunk 3.0 (or later) can be integrated into an NMS to provide an complete view of the converged voice and data network. Problems can be isolated much more quickly when looking at the entire network.

SNMP Agent support is provided in OTM 1.1 and later. This integrates OTM with existing NMS software, which allows alarms collected from an from devices to be forwarded to the NMS.

Nortel Networks also provides a complete line of Enterprise Network management software with Optivity Enterprise Network Management Solutions product line.

OTM and Network Management System

OTM can be combined with Optivity Network Management System (Optivity NMS), Release 9.01 and later. This provides an integrated data, voice, and video network, as part of the Nortel Networks Unified Networking system. The result is integrated LAN, WAN, and voice network management.

Optivity NMS is an enterprise-level network management solution providing fault, performance, configuration, and security management for Nortel Networks internetworking devices. Optivity NMS enables network administrators to monitor and manage the network through a single view, and access any Optivity NMS server in the network from one client installation. It provides system-level management, instead of managing one device at a time. Optivity NMS provides graphical views from physical connections between the LANs and WANs to the logical connections of a VLAN.

OTM server activity can be monitored through Optivity NMS.

OTM Alarm Manager receives Simple Network Management Protocol (SNMP) traps from managed elements. Through Alarm Notification, OTM sends filtered traps to Optivity NMS.

For detailed information on integrating OTM with Optivity NMS, see *Installing and Configuring OTM* (553-3001-280).

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 Networks Optivity Policy Services, refer to Appendix A on page 229, or contact your Nortel Networks representative.

IP Trunk 3.0 (or later) network inventory and configuration

Record the current IP Trunk 3.0 (or later) design and log all adds, moves, and changes to the IP Trunk 3.0 (or later) network that occur. The following data must be kept:

- ITG site information
  - location
  - dialing plan
  - IP addressing
- Provisioning of IP Trunk 3.0 (or later) nodes
  - number of cards and ports
- IP Trunk 3.0 (or later) node and card parameters
  - fallback threshold level
  - codec image
  - voice and fax payload
  - voice and fax playout delay
  - audio gain, echo cancellor tail delay size, Silence Suppression threshold
  - software version

Appendix A: Configuring the BPS / Baystack 450

Contents

This section contains information on the following topics:

Creating telephony VLANs on the Business Policy Switch 230
Business Policy Switch/BayStack 450 configuration. 230
Definitions 230
BPS VLAN. 231
Tagging after packets exit the BPS 233
VLAN configuration using the BPS web interface 234
QoS configuration for the BPS/Baystack 450. 253
The BPS interface group assignment 255
The BPS User Priority Assignment Table 256
The BPS DSCP queue assignment 257
The BPS Priority Mapping Table. 258
Baystack 450 802.1p user priority configuration 260

Creating telephony VLANs on the Business Policy Switch

The following sections describe an example of configuring voice and data VLANs on a single port of a Layer 2 switch.

Business Policy Switch/BayStack 450 configuration

Detailed Business Policy Switch (BPS)/Baystack 450 configuration information is provided in the following sections. The Web-based graphical screen shots are exclusively for the BPS with V1.2 firmware. The text-based screen shots from the terminal interface apply to both the BPS and the BayStack 450.

Definitions

Table 34 provides the definitions for common Ethernet VLAN terms and terms used by the Nortel Networks Business Policy Switch 2000.

Table 34
VLAN terms and definitions (Part 1 of 2)

Term	Definition
Port VLAN Identifier (PVID)	Associates a port to a VLAN. The default is 0. Incoming untagged frames are sent to this VLAN 0.
Tagged frame	32-bit field (VLAN tag) in the Ethernet frame header that identifies the frame to a VLAN.
Untagged frame	The extra 32-bit VLAN tag is not included in this Ethernet frame.
Tagged Member	A port that is a member of the same VLAN community that adds a VLAN tag to Ethernet frames that exit the port.
Untagged Member	A port that is a member of a VLAN community that removes the VLAN tag from Ethernet frames that exit the port.
Registered packet	A tagged Ethernet frame's VLAN ID that matches the receiving port's VLAN membership.

Table 34
VLAN terms and definitions (Part 2 of 2)

Term	Definition
Unregistered packet	A tagged Ethernet frame's VLAN ID that does not match the receiving port's VLAN membership.
Multi-Link Trunk (MLT)	A single virtual high-bandwidth connection that uses up to 4 Ethernet ports. Can connect to another Ethernet switch or server.

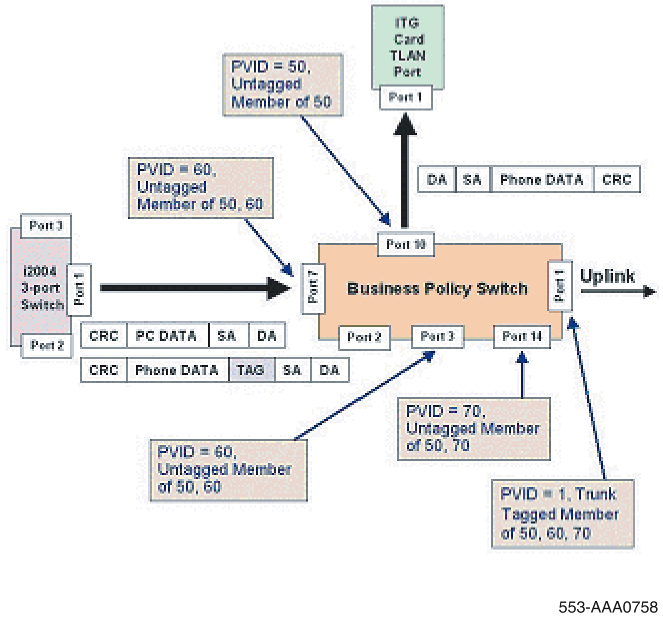
BPS VLAN

The scenario

An i2004 Internet Telephone is connected to ports 3, 7, and 14 on the BPS. The system is connected to port 10. The i2004 Internet Telephone tags its packets with VLAN ID 50. The Succession Media Card in the system cannot tag its packets nor does it understand tagged packets. Therefore, the VLAN tag must be removed prior to packets arriving at the system. The 3-port switch is used with each of the Internet Telephones. A PC is connected to each Internet Telephone through the telephone's 3-port switch.

Figure 33 on page 232 shows the VLAN assignments on the BPS switch.

Figure 33
VLAN assignment on BPS



The global configuration for the BPS is as follows:

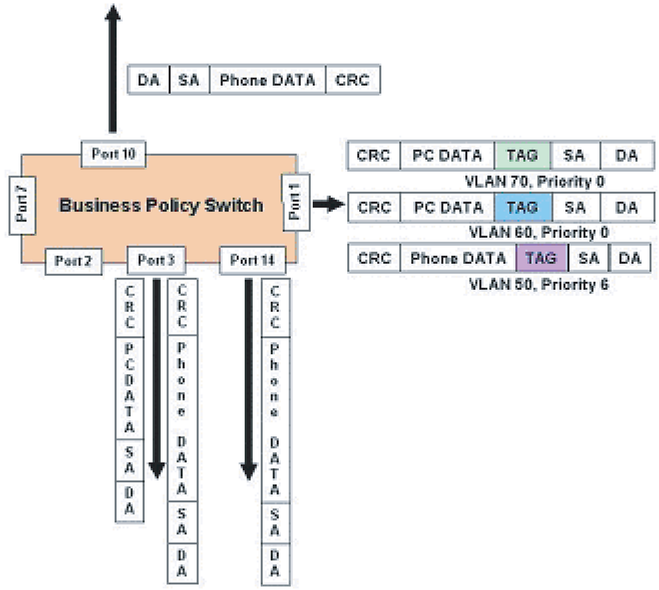
- No port filtering
- VLAN ID 50 for Internet Telephone packets (Telephony VLAN)
- VLAN ID 60 and 70 for data packets

Tagging after packets exit the BPS

The uplink (Port 1 in Figure 34) on the BPS must be configured both as a tagged trunk, and as a tagged member of all VLANs whose members are on other switches in the network. As the packets exit onto the uplink, they are tagged with their associated VLAN tag.

The packets exiting the ports of their respective devices (PC or Internet Telephone) have their 802.1Q VLAN tags removed since the ports are configured as "untagged members". See Figure 34.

Figure 34
VLAN tagging after packets have travelled through the BPS


DA | SA | Phone DATA | CRC
Port 10
Business Policy Switch
Port 7
Port 1
Port 2
Port 3
Port 14
CRC | PC DATA | TAG | SA | DA
VLAN 70, Priority 0
CRC | PC DATA | TAG | SA | DA
VLAN 60, Priority 0
CRC | Phone DATA | TAG | SA | DA
VLAN 50, Priority 6
CRC | PC DATA | SA | DA
CRC | Phone DATA | SA | DA
CRC | Phone DATA | SA | DA

553-AAA0759

VLAN configuration using the BPS web interface

The following sections describe how to configure the VLAN using the BPS web interfaces.

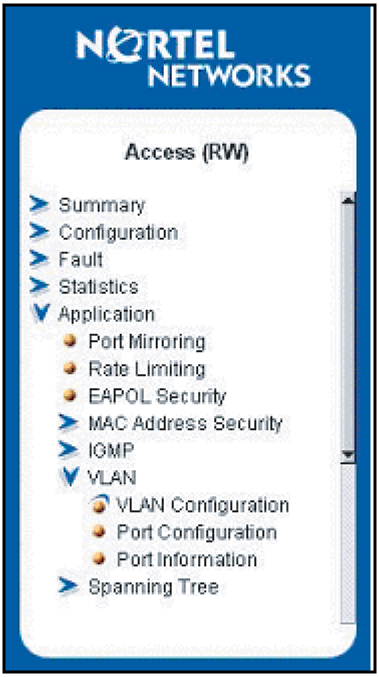
Creating multiple port-based VLANs

To create multiple port-based VLANs, perform the steps in Procedure 7.

Procedure 7
Creating multiple port-based VLANs

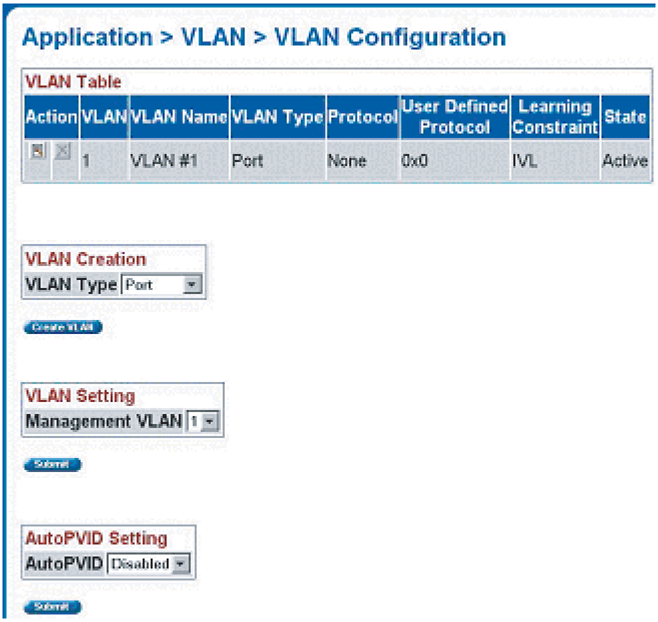
1 From the main VLAN menu shown in Figure 35, choose **Application > VLAN > VLAN Configuration**.

Figure 35
BPS VLAN main menu



2 In the **VLAN Creation** drop-down menu, select **Port** for **VLAN Type**. Click the **Create VLAN** button below the drop-down menu. This creates a port-based VLAN. See Figure 36 on page 235.

Figure 36
BPS VLAN configuration menu



Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
	1	VLAN #1	Port	None	0x0	IVL	Active

VLAN Creation

VLAN Type: Port

VLAN Setting

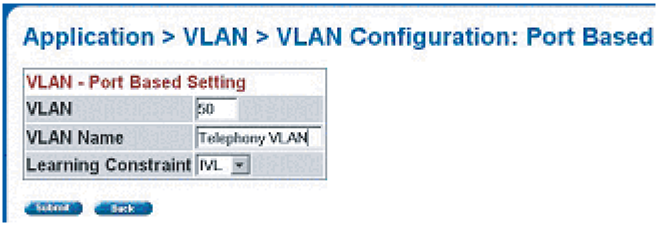
Management VLAN: 1

AutoPVID Setting

AutoPVID: Disabled

3 On the **VLAN – Port Based Setting** page, enter the **VLAN ID** and **VLAN Name**; for example, **50** for **VLAN ID** and **Telephony VLAN** for **VLAN Name**. See Figure 37 on page 236.

Figure 37
BPS VLAN port configuration menu



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting	
VLAN	50
VLAN Name	Telephony VLAN
Learning Constraint	IVL

553-AAA0762

4 Click the **Submit** button.

End of Procedure

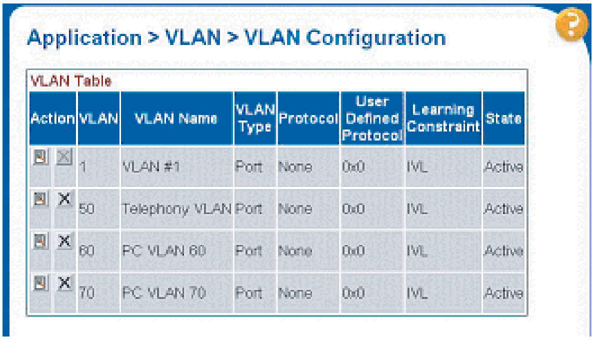
VLAN naming

The VLAN name provides an easy way to remember the usage of the VLAN. In this example, “Telephony VLAN” is the name for VLAN 50 which is used for IP Telephony.

Repeat steps 2 through 4 of Procedure 7 on page 234 to configure VLANs 60 and 70. In this example, VLANs 60 and 70 use the VLAN names “PC VLAN 60" and “PC VLAN 70". These names make it easy to remember that these VLANs are used for PCs, and that 60 and 70 are the VLAN IDs.

Once all of the VLANs are created, the VLAN Configuration VLAN table appears, as seen in Figure 38 on page 237.

Figure 38
Completed VLAN configuration VLAN table



Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
▣ ☒	1	VLAN #1	Port	None	0x0	IVL	Active
▣ ☒	50	Telephony VLAN	Port	None	0x0	IVL	Active
▣ ☒	60	PC VLAN 60	Port	None	0x0	IVL	Active
▣ ☒	70	PC VLAN 70	Port	None	0x0	IVL	Active

553-AAA0763

VLAN port membership assignment

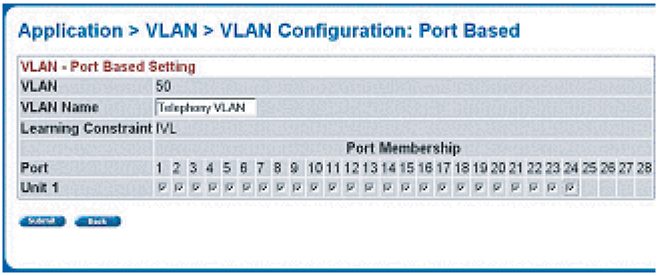
This section describes how to configure different ports on the switch to become a member of a particular VLAN. This means that traffic marked with a particular VLAN ID can travel through those ports that are members of this VLAN ID.

Procedure 8
Assigning membership to VLAN ports

1. In the **VLAN Configuration VLAN Table** menu (see Figure 38 on page 237), click the **Action** button (in the **Action** column – far left) for VLAN 50.

2. In the **VLAN Configuration: Port Based** window that appears, (see Figure 39 on page 238), check the box under all ports that belong in this VLAN. In this case, all 24 ports on the switch are members of VLAN ID 50, the Telephony VLAN. All telephony packets marked with VLAN ID 50 can now access the marked ports.

Figure 39
VLAN 50 port membership configuration menu



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN	50
VLAN Name	Telephony VLAN
Learning Constraint	IVL

	Port Membership																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑				

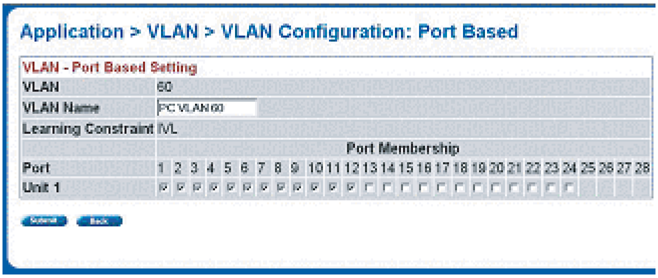
553-AAA0770

3 When the ports are selected, click on the **Submit** button.

4 Repeat steps 1 through 3 for the remaining VLANs (60 and 70). Refer to Figure 40 on page 238 and Figure 41 on page 239 for the final VLAN configuration for VLAN 60 and 70. In this example, VLAN 60 packets have membership only in ports 1-12. VLAN 70 packets have membership only in ports 1 and 13-24.

Figure 40 shows ports 1-12 configured with port membership in VLAN 60.

Figure 40
VLAN 60 port membership configuration menu



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

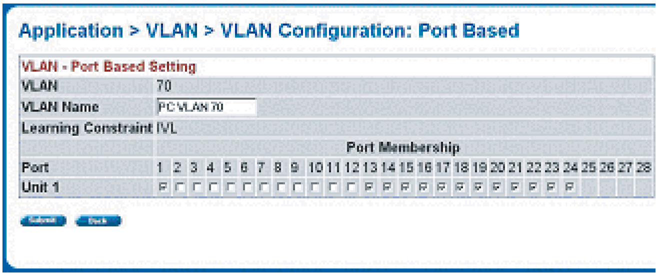
VLAN	60
VLAN Name	PC VLAN 60
Learning Constraint	IVL

	Port Membership																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□				

553-AAA0771

In Figure 41 on page 239, ports 1 and 13–24 are configured to have port membership in VLAN 70.

Figure 41
VLAN 70 port membership configuration menu



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN 70

VLAN Name PC VLAN 70

Learning Constraint IVL

	Port Membership																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☑	□	□	□	□	□	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑				

553-AAA0772

End of Procedure

Note: All VLAN IDs must have membership to port 1 which is the uplink connection. Any VLAN IDs that are not members of the uplink (port 1), will be blocked from the uplink, and only local connectivity to other port members on the switch will be available.

Configuring PVIDs

This section describes how to configure additional capabilities for the VLAN. In this example, the PVIDs and Link Type for each port are configured.

Procedure 9
Configuring the PVID and Link Type for each port

1 From the main VLAN configuration menu, choose **Port Configuration**. See Figure 35 on page 234.

2 Within the **Port Configuration** menu (refer to Figure 42 on page 240), configure **PVID** 60 for ports 2–9, 11 and 12. Configure **PVID** 70 for ports 13–24.

3 In this same menu, configure port 10 with **PVID** 50. This is the port to which the system is connected. Set **Port Priority** to 6. This is the 802.1p user priority used to tag all traffic entering that port from the system. Nortel Networks has designated 802.1p user priority 6 for IP telephony traffic.

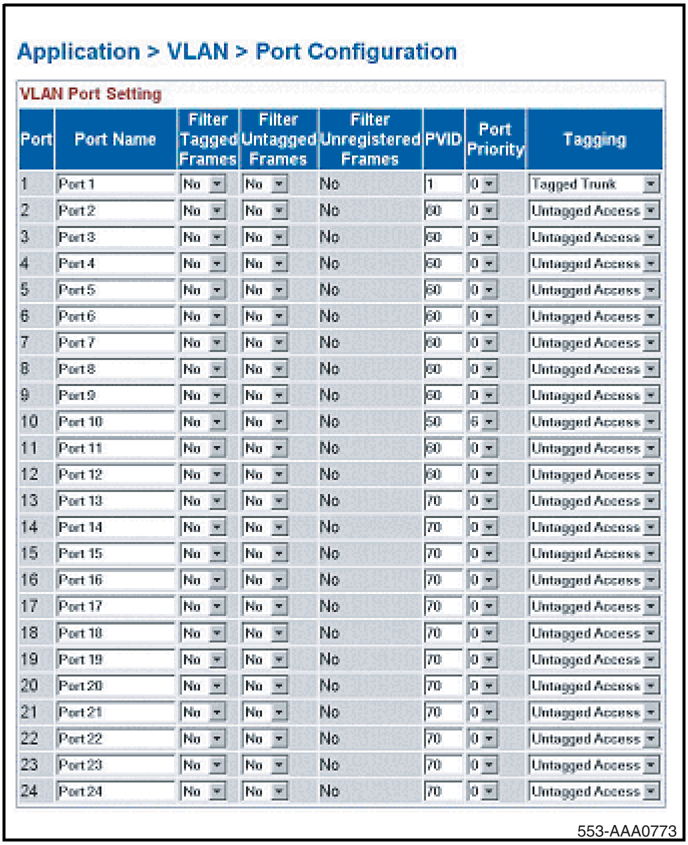
4 In the **Port Configuration** menu (see Figure 42 on page 240), in the **Tagging** column, select **Tagged** in the drop-down box to configure Port 1 as the “Tagged Trunk” link type.

5 When completed, click on the **Submit** button.

Note: The tagged trunk uplink must be a member of every VLAN that uses the uplink.

End of Procedure

Figure 42
BPS VLAN port membership menu



Application > VLAN > Port Configuration

VLAN Port Setting

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
1	Port 1	No	No	No	1	0	Tagged Trunk
2	Port 2	No	No	No	60	0	Untagged Access
3	Port 3	No	No	No	60	0	Untagged Access
4	Port 4	No	No	No	60	0	Untagged Access
5	Port 5	No	No	No	60	0	Untagged Access
6	Port 6	No	No	No	60	0	Untagged Access
7	Port 7	No	No	No	60	0	Untagged Access
8	Port 8	No	No	No	60	0	Untagged Access
9	Port 9	No	No	No	60	0	Untagged Access
10	Port 10	No	No	No	50	5	Untagged Access
11	Port 11	No	No	No	60	0	Untagged Access
12	Port 12	No	No	No	60	0	Untagged Access
13	Port 13	No	No	No	70	0	Untagged Access
14	Port 14	No	No	No	70	0	Untagged Access
15	Port 15	No	No	No	70	0	Untagged Access
16	Port 16	No	No	No	70	0	Untagged Access
17	Port 17	No	No	No	70	0	Untagged Access
18	Port 18	No	No	No	70	0	Untagged Access
19	Port 19	No	No	No	70	0	Untagged Access
20	Port 20	No	No	No	70	0	Untagged Access
21	Port 21	No	No	No	70	0	Untagged Access
22	Port 22	No	No	No	70	0	Untagged Access
23	Port 23	No	No	No	70	0	Untagged Access
24	Port 24	No	No	No	70	0	Untagged Access

553-AAA0773

Interface trust configuration

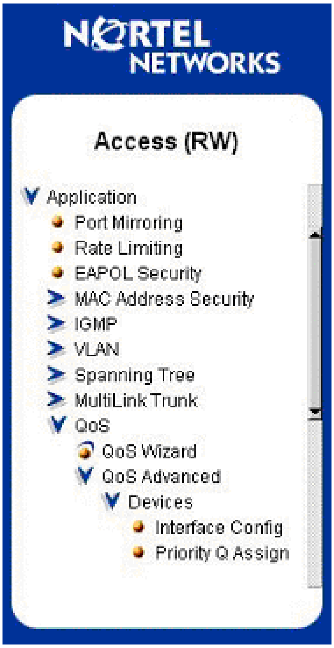
After the VLANs are configured, it is necessary to configure the Telephony VLAN ports to trust the packet QoS markings. This prioritizes the packets appropriately on the BPS. The i2002 and i2004 Internet Telephone pre-mark their packets with the Expedited Forwarding (EF) DSCP and 802.1p user priority 6.

Once the BPS is configured to trust pre-marked telephony packets, it places the pre-marked telephony packets in its highest priority queue, Queue 1. This ensures that the telephony packets achieve low latency, even during network congestion.

Procedure 10
Configuring trust relationships

1 In the main menu (see Figure 43 on page 242), select the following: **Application > QoS > QoS Advanced > Devices > Interface Config**.

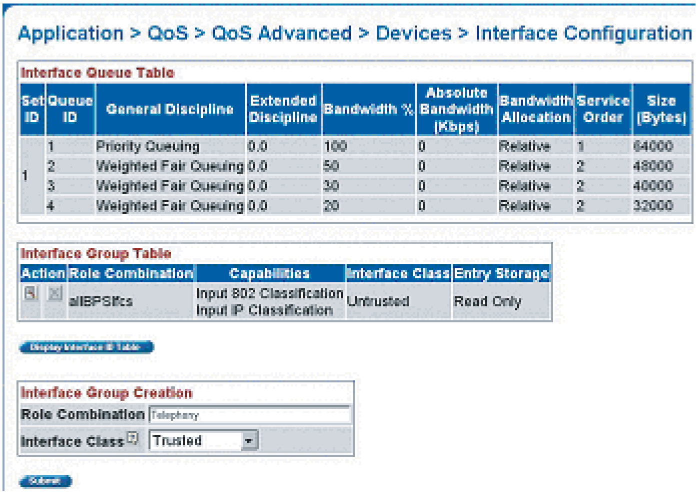
Figure 43
BPS main menu – QoS advanced



2 The **Interface Configuration** screen displays, as seen in Figure 44 on page 243. On this screen, go to the **Interface Group Creation** box and enter **Telephony** as the **Role Combination**.

3 In the drop-down box, select **Trusted** as the **Interface Class**.

Figure 44
BPS interface configuration



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000

Interface Group Table

Action	Role Combination	Capabilities	Interface Class	Entry Storage
	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only

Interface Group Creation

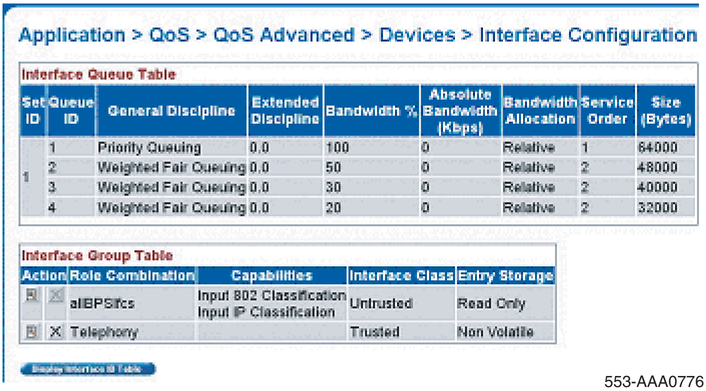
Role Combination	Telephony
Interface Class	Trusted

553-AAA0775

The **Telephony Role Combination** described in Step 2 is used to configure all telephony ports as trusted interfaces. This means that the BPS trusts the DSCP and 802.1p packet values. The BPS also maps the pre-marked packets to one of the four BPS queues, based on the internal default mapping tables of DSCP to queue. BPS retains the DSCP and 802.1p markings of the packets as they exit the switch.

The **Interface Group Table** is now updated to include the new **Telephony Role Combination.** See Figure 45 on page 244.

Figure 45
Updated BPS interface Group Table



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000

Interface Group Table

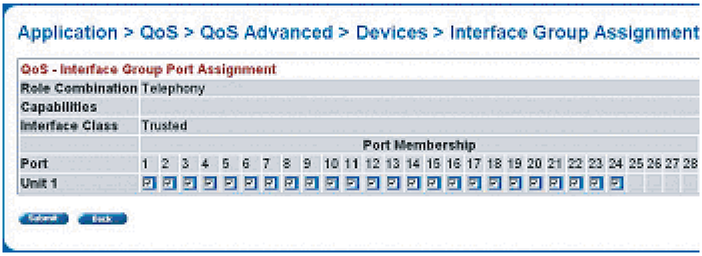
Action	Role Combination	Capabilities	Interface Class	Entry Storage
✎ ✕	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only
✎ ✕	Telephony		Trusted	Non Volatile

553-AAA0776

4 In the **Interface Group Table**, click the **Action** button for the **Telephony Role Combination**. This opens a new window where the ports to be configured as trusted interfaces are selected.

5 Select all 24 ports (see Figure 46 on page 245) since Internet Telephones can be connected to any of the 24 ports. The port membership for the **Telephony Role Combination** must correspond to the port membership for VLAN 50, the Telephony VLAN.

Figure 46
Telephony Role Combination port membership



Application > QoS > QoS Advanced > Devices > Interface Group Assignment

QoS - Interface Group Port Assignment

Role Combination	Telephony																											
Capabilities																												
Interface Class	Trusted																											
	Port Membership																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑				

553-AAA0777

End of Procedure

The QoS policies for the telephony traffic are complete. This example is a simple QoS policy, where all pre-marked packets (assumed to be from the telephony devices) are received on trusted interfaces, and prioritized based on their QoS markings. More sophisticated QoS policies may be implemented through the **Rules** sub-menus, for example, **IP Classification** or **Layer 2 Classification**. **Actions**, **Meters** and **Policies** can be added to provide additional filtering, if necessary.

VLAN configuration using the terminal interface

The following sections describe the VLAN configuration process using the terminal interface. The configuration screens are essentially the same for both the BPS and the BayStack 450.

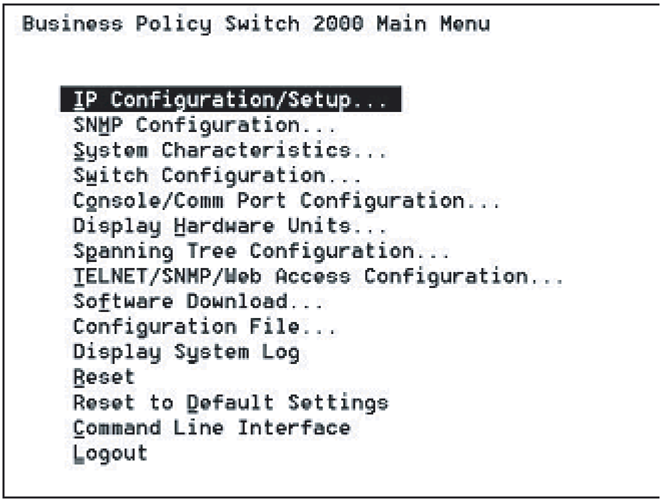
Creating multiple port-based VLANs

Follow the steps in Procedure 11 on page 246 to create multiple port-based VLANs.

Procedure 11
Configuring the VLAN for multiple ports

1 From the main menu, select “**Switch Configuration**”. See Figure 47.

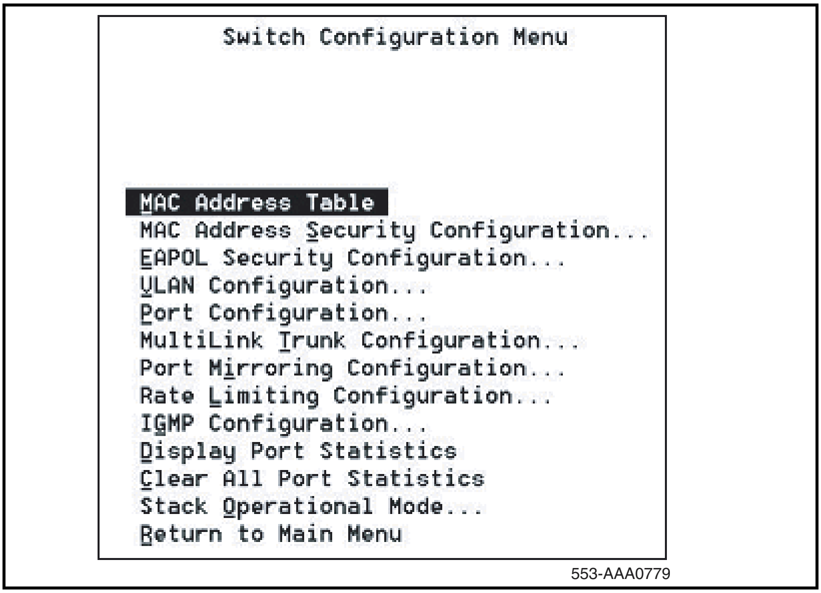
Figure 47
Main terminal interface menu


Business Policy Switch 2000 Main Menu
IP Configuration/Setup...
SNMP Configuration...
System Characteristics...
Switch Configuration...
Console/Comm Port Configuration...
Display Hardware Units...
Spanning Tree Configuration...
TELNET/SNMP/Web Access Configuration...
Software Download...
Configuration File...
Display System Log
Reset
Reset to Default Settings
Command Line Interface
Logout

553-AAA0778

2 In the **Switch Configuration** menu select **VLAN Configuration**. See Figure 48 on page 247.

Figure 48
Switch configuration menu

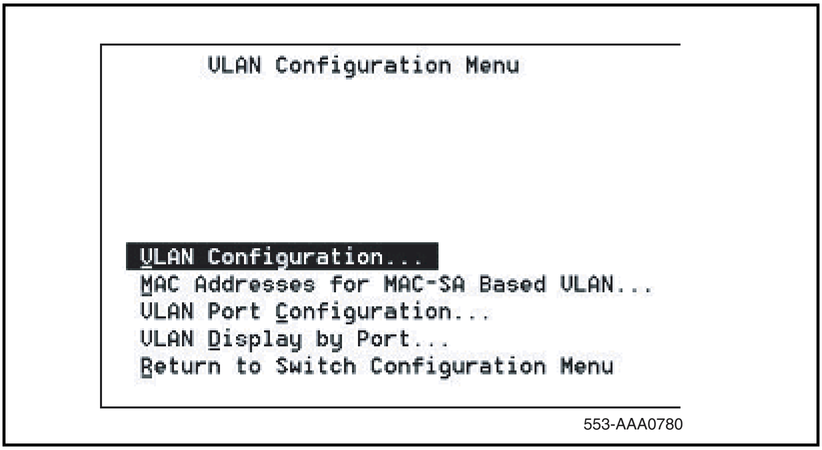


```
              Switch Configuration Menu



 MAC Address Table
 MAC Address Security Configuration...
 EAPOL Security Configuration...
 VLAN Configuration...
 Port Configuration...
 MultiLink Trunk Configuration...
 Port Mirroring Configuration...
 Rate Limiting Configuration...
 IGMP Configuration...
 Display Port Statistics
 Clear All Port Statistics
 Stack Operational Mode...
 Return to Main Menu
```

553-AAA0779

The **VLAN Configuration** menu appears. See Figure 49 on page 247.

Figure 49
VLAN configuration main menu

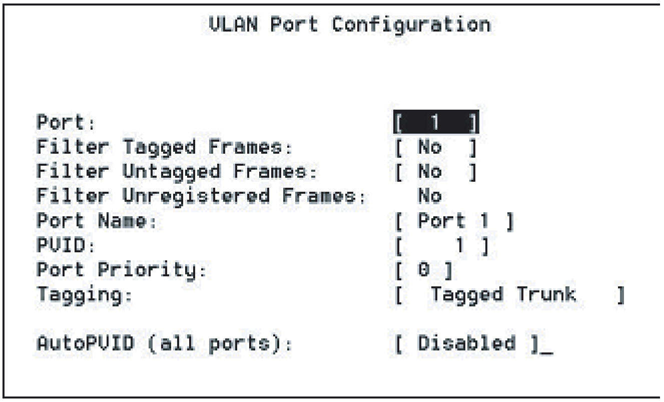


```
            VLAN Configuration Menu



 VLAN Configuration...
 MAC Addresses for MAC-SA Based VLAN...
 VLAN Port Configuration...
 VLAN Display by Port...
 Return to Switch Configuration Menu
```

553-AAA0780

3 Select **VLAN Port Configuration**. See Figure 50 on page 248. In the **Tagging** field, select **Tagged Trunk**. This is the uplink port.

Figure 50
VLAN port configuration menu



```
                         VLAN Port Configuration


   Port:                                  [   1   ]
   Filter Tagged Frames:                  [ No   ]
   Filter Untagged Frames:                [ No   ]
   Filter Unregistered Frames:              No
   Port Name:                             [ Port 1 ]
   PVID:                                  [      1 ]
   Port Priority:                         [ 0 ]
   Tagging:                               [  Tagged Trunk    ]

   AutoPVID (all ports):                  [ Disabled ]_
```

553-AAA0781

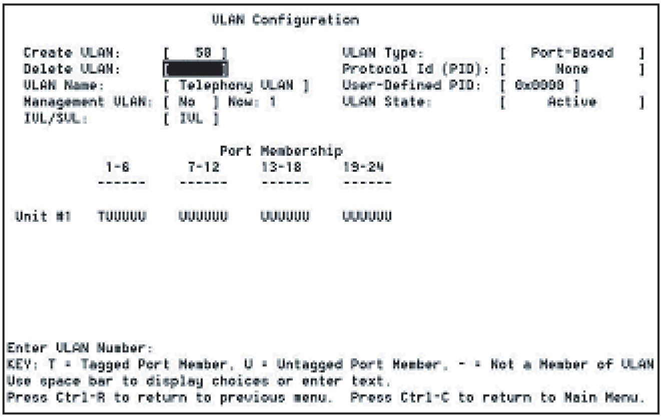
4 From the **VLAN Configuration** menu (Figure 49 on page 247), select the **VLAN Configuration** option. In the **VLAN Configuration** screen (see Figure 51), enter the required VLAN ID (in this example, **50**) in the **Create VLAN** field.

5 In the Port Membership fields, select the port member type by using the space bar and then the **Enter** key to select the value. See Figure 51. The **Port Membership** type can consist of the following:

- '**–**' (not a member),
- '**U**' (an untagged port member) or
- '**T**' (tagged port member)

6 In the **VLAN State** field, select **Active.** See Figure 51 on page 249.

Figure 51
VLAN configuration menu – VID 50

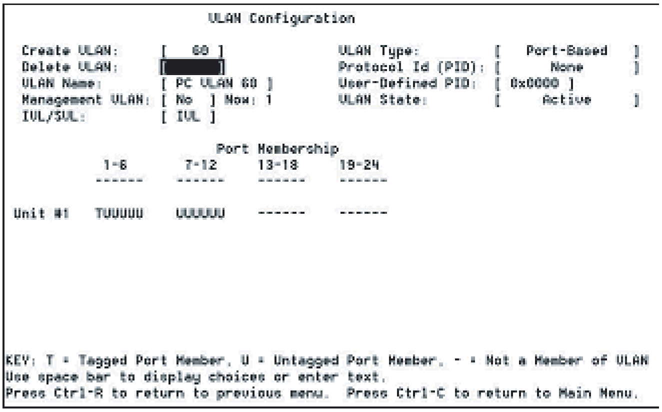


```
                          VLAN Configuration

 Create VLAN:         [    50 ]            VLAN Type:          [   Port-Based    ]
 Delete VLAN:         [       ]            Protocol Id (PID):  [      None       ]
 VLAN Name:           [ Telephony VLAN ]   User-Defined PID:   [ 0x0000 ]
 Management VLAN:     [ No   ] Now: 1      VLAN State:         [     Active      ]
 IVL/SVL:             [ IVL ]

                           Port Membership
            1-6        7-12      13-18      19-24
           ------     ------     ------     ------

Unit #1    TUUUUU     UUUUUU     UUUUUU     UUUUUU




Enter VLAN Number:
KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

553-AAA0782

7 Repeat steps 5, 6, and 7 for the remaining VLANs to be configured (VID 60 and 70). See Figure 52 and Figure 53 on page 250.

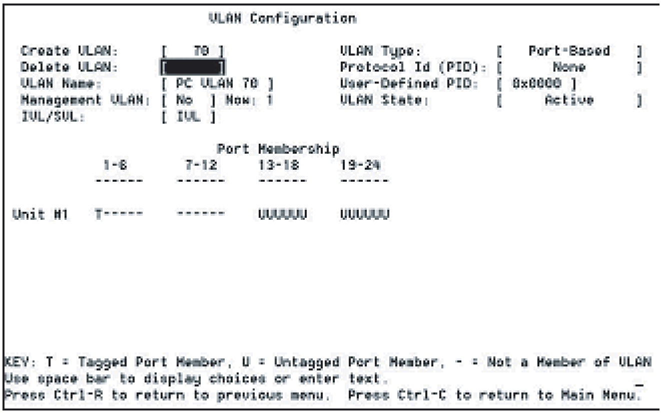
Figure 52
VLAN configuration menu – VID 60



```
                          VLAN Configuration

 Create VLAN:         [    60 ]            VLAN Type:          [   Port-Based    ]
 Delete VLAN:         [       ]            Protocol Id (PID):  [      None       ]
 VLAN Name:           [ PC VLAN 60 ]       User-Defined PID:   [ 0x0000 ]
 Management VLAN:     [ No   ] Now: 1      VLAN State:         [     Active      ]
 IVL/SVL:             [ IVL ]

                           Port Membership
            1-6        7-12      13-18      19-24
           ------     ------     ------     ------

Unit #1    TUUUUU     UUUUUU     ------     ------




KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

553-AAA0783

Figure 53
VLAN configuration menu – VID 70



```
                          VLAN Configuration

 Create VLAN:        [   70 ]             VLAN Type:           [   Port-Based    ]
 Delete VLAN:        [      ]             Protocol Id (PID):   [      None       ]
 VLAN Name:          [ PC VLAN 70 ]       User-Defined PID:    [ 0x0000 ]
 Management VLAN:    [ No   ] Now: 1      VLAN State:          [     Active      ]
 IVL/SVL:            [ IVL ]

                           Port Membership
              1-6       7-12      13-18     19-24
             ------    ------    ------    ------

Unit #1      T-----    ------    UUUUUU    UUUUUU




KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

553-AAA0784

8 Return to the **VLAN Port Configuration** screen. See Figure 50 on page 248.

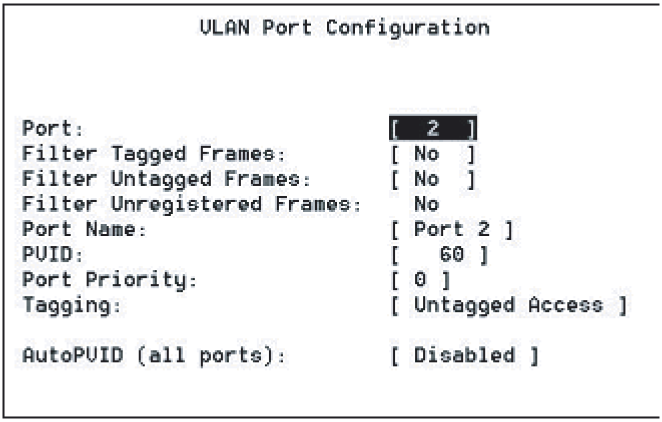
9 Select each **Port** to be configured. In the **PVID** field, enter the required PVID for the particular port. Configure each port separately.

End of Procedure

In this example, all 24 ports must be configured. The **Port Priority** refers to the 802.1p User Priority of the VLAN specified by the PVID.

Figures 54, 55, and 56 are sample configurations for ports 2, 10 and 15. Port 2 belongs to VLAN 60. Port 15 belongs to VLAN 70. Port 10 belongs to VLAN 50. Port priority (802.1p user priority) is set to 6 for Port 10, as Port 10 is connected to the Succession System Controller.

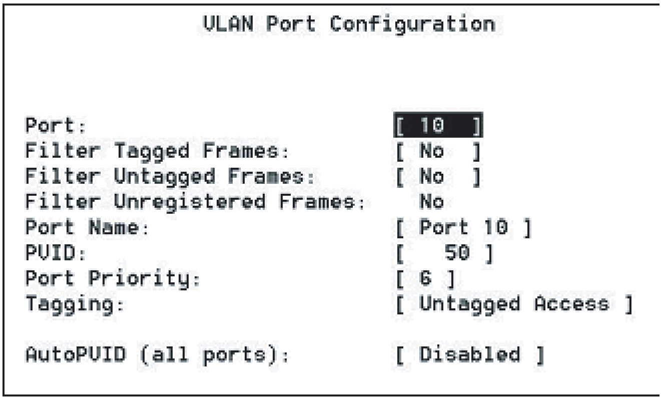
Figure 54
Configuration for VLAN ID 60, port 2



```
                    VLAN Port Configuration



Port:                               [  2  ]
Filter Tagged Frames:               [ No  ]
Filter Untagged Frames:             [ No  ]
Filter Unregistered Frames:           No
Port Name:                          [ Port 2 ]
PVID:                               [   60 ]
Port Priority:                      [ 0 ]
Tagging:                            [ Untagged Access ]

AutoPVID (all ports):               [ Disabled ]
```

553-AAA0785

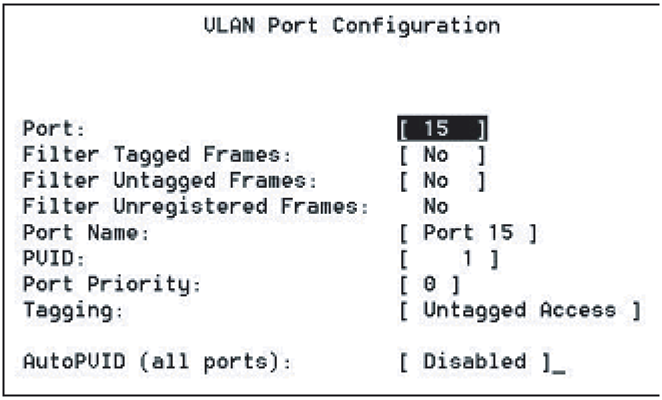
Figure 55
Configuration for VLAN ID 50, port 10



```
                    VLAN Port Configuration



Port:                               [ 10  ]
Filter Tagged Frames:               [ No  ]
Filter Untagged Frames:             [ No  ]
Filter Unregistered Frames:           No
Port Name:                          [ Port 10 ]
PVID:                               [   50 ]
Port Priority:                      [ 6 ]
Tagging:                            [ Untagged Access ]

AutoPVID (all ports):               [ Disabled ]
```

553-AAA0800

Figure 56
Configuration for VLAN ID 70, port 15



```
                    VLAN Port Configuration



Port:                              [ 15   ]
Filter Tagged Frames:              [ No   ]
Filter Untagged Frames:            [ No   ]
Filter Unregistered Frames:          No
Port Name:                         [ Port 15 ]
PVID:                              [     1 ]
Port Priority:                     [ 0 ]
Tagging:                           [ Untagged Access ]

AutoPVID (all ports):              [ Disabled ]_
```

553-AAA0801

End of Procedure

QoS configuration for the BPS/Baystack 450

QoS functionality on the BPS

QoS activity on the BPS takes place in several stages. The first stage involves using a method to identify the traffic, such as traffic filters.

After identifying the class of traffic, actions can be configured to drop, mark, or pass the network traffic. Dropping the traffic involves preventing the information from passing through the device. Marking the traffic changes the flow identifier values such as the DSCP or 802.1p user priority bits. Marking the traffic affects the behavior of the network traffic downstream. The BPS can also allow the traffic to pass unaltered.

All traffic that passes through the switch is placed in hardware queues for outbound ports. A single packet is not spread among multiple queues.

Each interface can have two or more queues associated with it. Multiple queues that are related by their schedule for servicing, can be associated as a queue set. On the BPS there are two scheduling methods, Priority Queues (PQ) and Weighted Round-Robin (WRR).

Figure 57 on page 254 shows an example of an Interface Queue Table. Under the **Set ID** column, Set ID 1 and Set ID 2 refer to Queue Set 1 and Queue Set 2.

Queue Set 1 has the following parameters:

- **General Discipline** (scheduling)
  - — Priority Queueing + Weighted Fair Queueing (Weighted Round-Robin)
- Highest priority queue
  - — **Queue ID** 1
- Weighted Round-Robin queues
  - — **Queue ID** 2 (50% bandwidth)
  - — **Queue ID** 3 (30% bandwidth)
  - — **Queue ID** 4 (20% bandwidth)

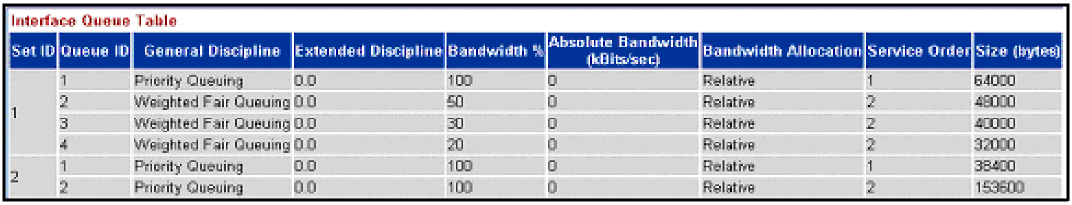
> ***Note:*** All packets in the highest priority queue, Queue ID 1, are serviced before the packets in any other queues. When Queue ID 1 is empty, the packets in queues 2, 3, and 4 are serviced in a Round-Robin method. In this example, it is possible for packets in queues 2, 3, and 4 to starve (never be serviced), if Queue ID 1 is continuously busy.

Queue Set 2 has the following parameters:

- **General Discipline** (scheduling)
  - — Priority Queueing)
- Highest priority queue
  - — **Queue ID** 1
- Lowest priority queue
  - — **Queue ID** 2

> ***Note:*** In this example, all packets in Queue ID 1 are serviced before the packets in Queue ID 2.

Figure 57
Interface Queue Table



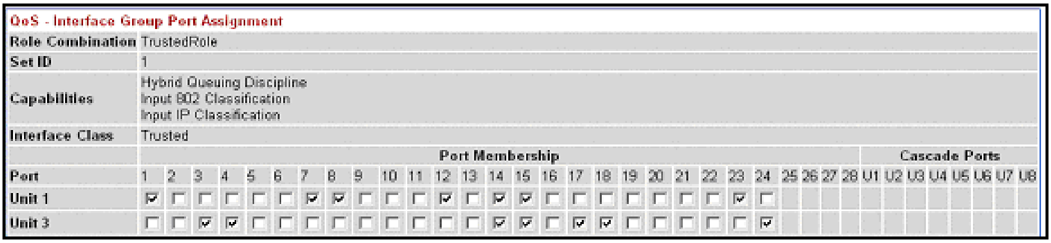
Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (kBits/sec)	Bandwidth Allocation	Service Order	Size (bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000
2	1	Priority Queuing	0.0	100	0	Relative	1	38400
	2	Priority Queuing	0.0	100	0	Relative	2	153600

The BPS interface group assignment

QoS configuration on the BPS consists of assigning each Internet Telephone Ethernet port to a ‘Trusted’ Interface Group. See Figure 58 on page 255.

Figure 58
QoS interface group port assignment



QoS - Interface Group Port Assignment

Role Combination	TrustedRole
Set ID	1
Capabilities	Hybrid Queuing Discipline Input 802 Classification Input IP Classification
Interface Class	Trusted

	Port Membership																												Cascade Ports							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	U1	U2	U3	U4	U5	U6	U7	U8
Unit 1	☑	□	□	□	□	□	☑	☑	□	□	□	☑	□	☑	☑	□	□	□	□	□	□	□	☑	□												
Unit 3	□	□	☑	☑	□	□	□	□	□	□	□	□	□	☑	☑	□	☑	☑	□	□	□	□	□	☑												

The remaining desktop PC Ethernet ports are assigned to the default untrusted role. A trusted port keeps the DSCP and 802.1p bits intact. Untrusted ports have the DSCP and 802.1p values reset. VoIP traffic coming out of the i2050 software Internet Telephone is prioritized by applying policies using Optivity Policy Services (OPS) 2.0. See Appendix C on page 275 for more information.

The BPS with Media Dependant Adapter (MDA) uplinks must have its ports set to trusted roles as well, to ensure that the QoS services are passed on.

Another method of deploying QoS in the BPS is to set all the ports to ‘trusted’. This implementation is simple to deploy. However, it is necessary that the traffic coming out of the PC Ethernet ports and Internet Telephone ports is not abused. Setting desktop PC connections to a trusted role on the BPS allows applications such as the i2050 software Internet Telephone to prioritize voice traffic. It is possible that a user could configure a PC to mark DiffServ CodePoints so network traffic gets prioritized. This requires a high level of expertise, but the possibility of abuse exists. Therefore, this method of deployment is not recommended.

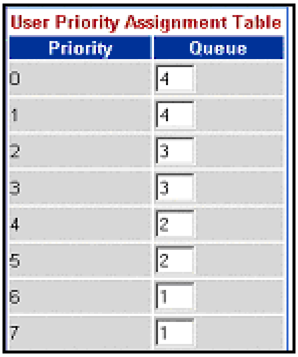
The BPS User Priority Assignment Table

The User Priority Assignment Table maps 802.1p user priority values to hardware queues in the BPS. The Assignment Table information designates egress traffic to specific outbound queues.

In the example shown in Figure 57 on page 254, there are two queue sets pre-defined in the BPS. The mappings are defined in each queue set. The Assignment Table is applicable for each queue set, as there could be two queue sets if the MDA card is utilized. By default, the 802.1p user priority that is mapped to a queue is defined by Nortel Networks as a default value.

See Figure 59 for an example of a User Priority Assignment Table.

Figure 59
User Priority Assignment Table



User Priority Assignment Table

Priority	Queue
0	4
1	4
2	3
3	3
4	2
5	2
6	1
7	1

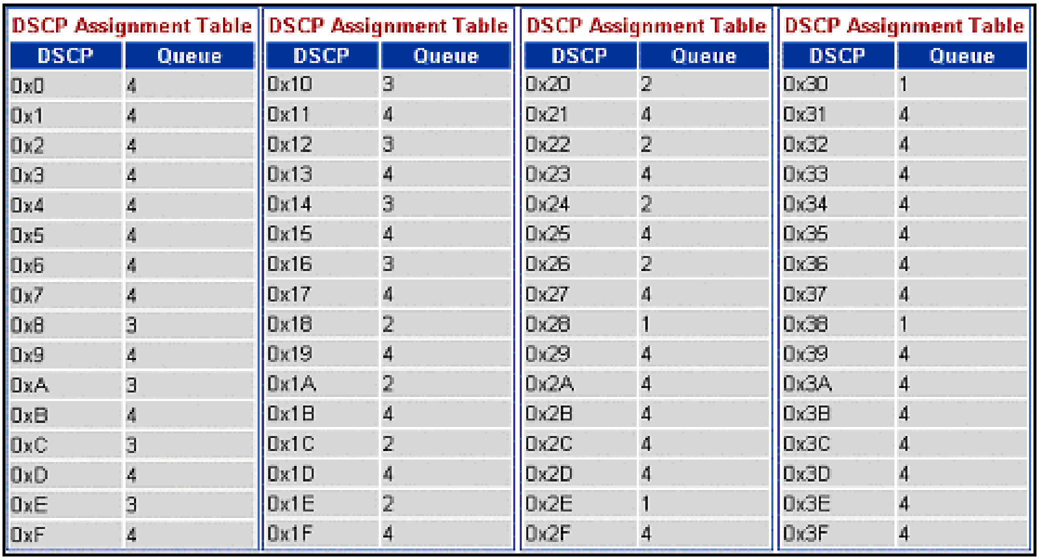
The BPS DSCP queue assignment

The DSCP Assignment Table maps the Layer 3 DiffServ CodePoint (DSCP) to internal hardware queues on the BPS. There are two queue sets predefined in the BPS. The mappings are already defined for each queue set.

By default, the BPS DSCP queue assignments map VoIP voice and signaling packets to the first queue. Nortel Networks has designated that VoIP voice packets are marked by default with the DSCP of 46 (0x2E). VoIP signaling packets (call setup) are marked by default with the DSCP value of 40 (0x28).

Figure 60 shows an example of a DSCP Assignment Table.

Figure 60
DSCP Assignment Table



DSCP Assignment Table

DSCP	Queue
0x0	4
0x1	4
0x2	4
0x3	4
0x4	4
0x5	4
0x6	4
0x7	4
0x8	3
0x9	4
0xA	3
0xB	4
0xC	3
0xD	4
0xE	3
0xF	4

DSCP Assignment Table

DSCP	Queue
0x10	3
0x11	4
0x12	3
0x13	4
0x14	3
0x15	4
0x16	3
0x17	4
0x18	2
0x19	4
0x1A	2
0x1B	4
0x1C	2
0x1D	4
0x1E	2
0x1F	4

DSCP Assignment Table

DSCP	Queue
0x20	2
0x21	4
0x22	2
0x23	4
0x24	2
0x25	4
0x26	2
0x27	4
0x28	1
0x29	4
0x2A	4
0x2B	4
0x2C	4
0x2D	4
0x2E	1
0x2F	4

DSCP Assignment Table

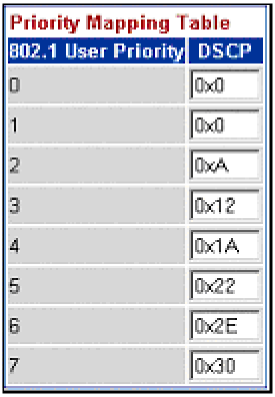
DSCP	Queue
0x30	1
0x31	4
0x32	4
0x33	4
0x34	4
0x35	4
0x36	4
0x37	4
0x38	1
0x39	4
0x3A	4
0x3B	4
0x3C	4
0x3D	4
0x3E	4
0x3F	4

The BPS Priority Mapping Table

The Priority Mapping Table maps 802.1 user priority values to DSCP values. These values do not need to be changed as Nortel Networks defines them by default.

Figure 61 shows an example of a Priority Mapping Table.

Figure 61
Priority Mapping Table

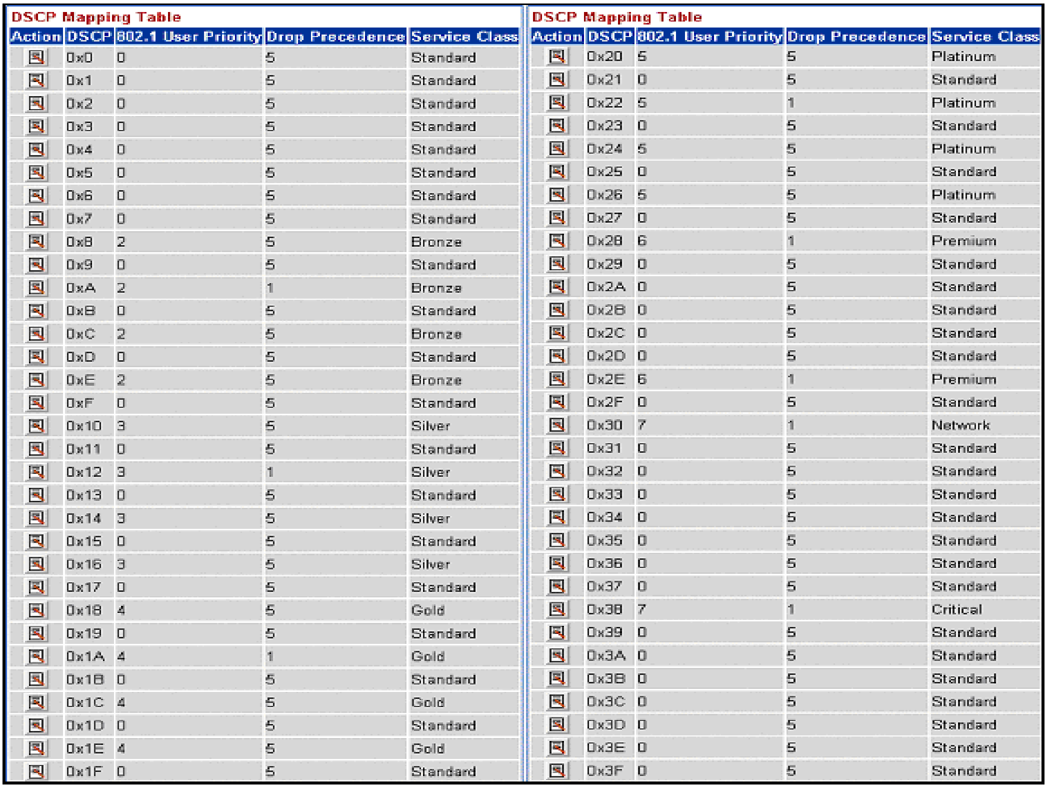


Priority Mapping Table

802.1 User Priority	DSCP
0	0x0
1	0x0
2	0xA
3	0x12
4	0x1A
5	0x22
6	0x2E
7	0x30

Figure 62 on page 259 is an example of the BPS DSCP Mapping Table.

Figure 62
DSCP Mapping Table



DSCP Mapping Table

Action	DSCP	802.1 User Priority	Drop Precedence	Service Class
	0x0	0	5	Standard
	0x1	0	5	Standard
	0x2	0	5	Standard
	0x3	0	5	Standard
	0x4	0	5	Standard
	0x5	0	5	Standard
	0x6	0	5	Standard
	0x7	0	5	Standard
	0x8	2	5	Bronze
	0x9	0	5	Standard
	0xA	2	1	Bronze
	0xB	0	5	Standard
	0xC	2	5	Bronze
	0xD	0	5	Standard
	0xE	2	5	Bronze
	0xF	0	5	Standard
	0x10	3	5	Silver
	0x11	0	5	Standard
	0x12	3	1	Silver
	0x13	0	5	Standard
	0x14	3	5	Silver
	0x15	0	5	Standard
	0x16	3	5	Silver
	0x17	0	5	Standard
	0x18	4	5	Gold
	0x19	0	5	Standard
	0x1A	4	1	Gold
	0x1B	0	5	Standard
	0x1C	4	5	Gold
	0x1D	0	5	Standard
	0x1E	4	5	Gold
	0x1F	0	5	Standard

DSCP Mapping Table

Action	DSCP	802.1 User Priority	Drop Precedence	Service Class
	0x20	5	5	Platinum
	0x21	0	5	Standard
	0x22	5	1	Platinum
	0x23	0	5	Standard
	0x24	5	5	Platinum
	0x25	0	5	Standard
	0x26	5	5	Platinum
	0x27	0	5	Standard
	0x28	6	1	Premium
	0x29	0	5	Standard
	0x2A	0	5	Standard
	0x2B	0	5	Standard
	0x2C	0	5	Standard
	0x2D	0	5	Standard
	0x2E	6	1	Premium
	0x2F	0	5	Standard
	0x30	7	1	Network
	0x31	0	5	Standard
	0x32	0	5	Standard
	0x33	0	5	Standard
	0x34	0	5	Standard
	0x35	0	5	Standard
	0x36	0	5	Standard
	0x37	0	5	Standard
	0x38	7	1	Critical
	0x39	0	5	Standard
	0x3A	0	5	Standard
	0x3B	0	5	Standard
	0x3C	0	5	Standard
	0x3D	0	5	Standard
	0x3E	0	5	Standard
	0x3F	0	5	Standard

Baystack 450 802.1p user priority configuration

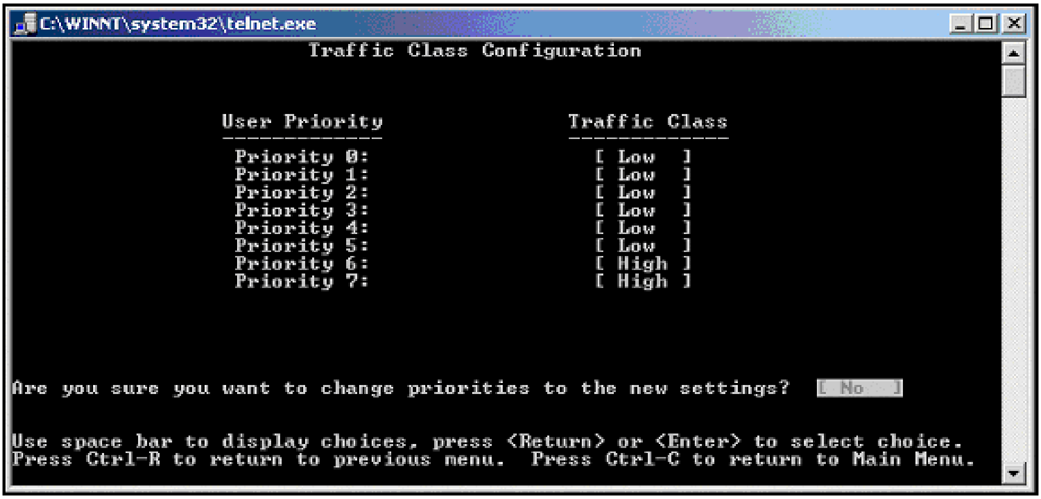
The BayStack 450 switch is a Layer 2-aware device. The BayStack 450 cannot prioritize packets based on the DSCP set in the IP packet header. Instead, Layer 2 802.1p user priority bits are used to differentiate packets.

To support prioritization of 802.1p user priorities on the Baystack 450, it is necessary to configure the Traffic Class Configuration under the **Switch Configuration -> VLAN Configuration** menu option.

Nortel Networks has defined a default value of ‘110’ (User Priority 6) for 802.1p marking. To implement VoIP using QoS on the BayStack 450, the user priority value of 6 should be assigned a **high** traffic class. See Figure 63 on page 260.

In the end, the configuration enables the prioritization of Ethernet packets on the upstream and downstream.

Figure 63
Traffic class configuration on the Baystack 450



```
                        Traffic Class Configuration


                 User Priority                 Traffic Class
                 -------------                 -------------
                  Priority 0:                    [ Low  ]
                  Priority 1:                    [ Low  ]
                  Priority 2:                    [ Low  ]
                  Priority 3:                    [ Low  ]
                  Priority 4:                    [ Low  ]
                  Priority 5:                    [ Low  ]
                  Priority 6:                    [ High ]
                  Priority 7:                    [ High ]




Are you sure you want to change priorities to the new settings?  [ No  ]


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Appendix B: Configuring QoS on the Passport 8600

Contents

This section contains information on the following topics:

DiffServ core network with BPS 2000 261

DiffServ core network with Baystack 450 264

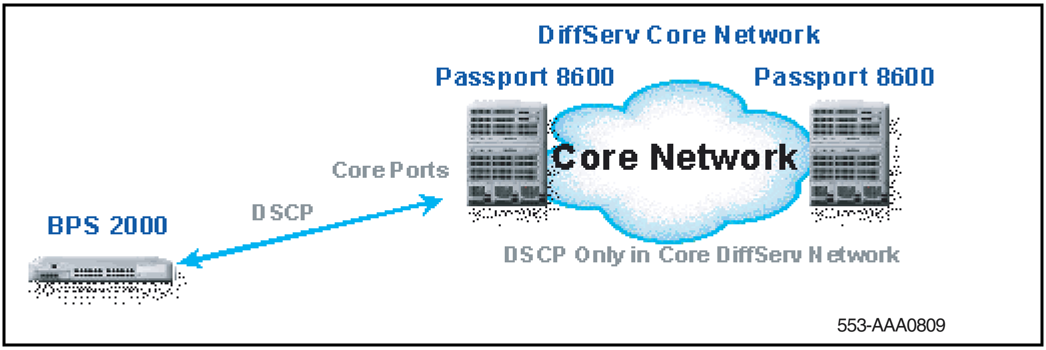
QoS on the Passport 8600 265

Layer 3 QoS mechanisms 270

DiffServ core network with BPS 2000

The Business Policy Switch (BPS) 2000 supports the ability to classify and mark traffic based on DiffServ and 802.1p values. The BPS 2000 can serve as the DiffServ edge device that performs mapping and network classification. Uplink ports from the BPS 2000 to the Passport 8600 can be set to ‘trusted’ core ports as the network traffic is assumed to be valid. Figure 64 on page 262 shows an example of a DiffServ core network with the BPS 2000 and the Passport 8600 switches.

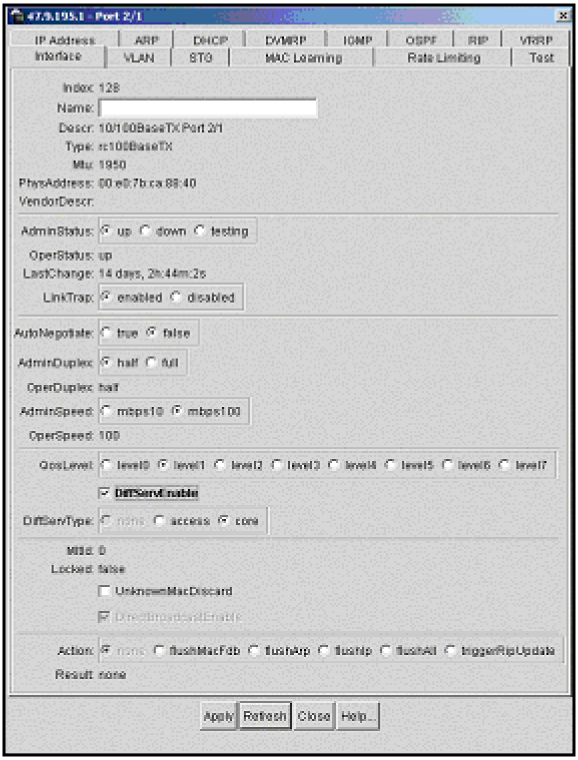
Figure 64
DiffServ core network with BPS 2000



The easiest way to configure this port is to use Device Manager. Enter the **edit** mode on the appropriate port and set the following options:

- Check the **DiffServEnable** checkbox.
- Set the **DiffServType** to **core**.

Figure 65
Configuring a port using Device Manager



Index: 128
Name:
Descr: 10/100BaseTX Port 2/1
Type: rc100BaseTX
Mtu: 1950
PhysAddress: 00:e0:7b:ca:88:40
VendorDescr:

AdminStatus: ● up ○ down ○ testing
OperStatus: up
LastChange: 14 days, 2h:44m:2s
LinkTrap: ● enabled ○ disabled

AutoNegotiate: ○ true ● false
AdminDuplex: ● half ○ full
OperDuplex: half
AdminSpeed: ○ mbps10 ● mbps100
OperSpeed: 100

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7
☑ DiffServEnable
DiffServType: ○ none ○ access ● core

MltId: 0
Locked: false
□ UnknownMacDiscard
☑ DirectBroadcastEnable

Action: ● none ○ flushMacFdb ○ flushArp ○ flushIp ○ flushAll ○ triggerRipUpdate
Result: none

To configure a port using a telnet session, enter config mode for the appropriate port interface:

/config/ethernet/<interface>/<port number>#

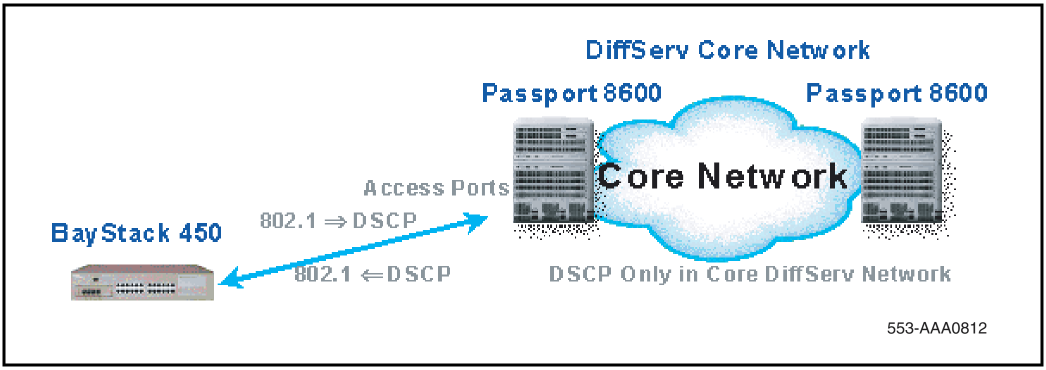
Ensure the following values are set:

- **enable-diffserv: true**
- **access-diffserv: false**

DiffServ core network with Baystack 450

In a core network with a BayStack 450, the Baystack 450 prioritizes network traffic based on 802.1p user priorities. Therefore, the BayStack 450 is dependent upon a DiffServ edge router such as the Passport 8600 to map 802.1p to DSCP. For Passport 8600 interfaces connected to BayStack 450 switches, it is necessary to have the interface set to Access Ports and to ensure the DiffServ feature is enabled on the interface. Figure 66 is an example of a DiffServ core network with a Baystack 450 switch.

Figure 66
DiffServ core network with Baystack 450



The easiest way to configure this port is to use Device Manager. Enter the **edit** mode on the appropriate port and set the following options:

- Check the **DiffServEnable** checkbox.
- Set the **DiffServType** to **access**.

To configure a port using a telnet session, enter config mode for the appropriate port interface:

/config/ethernet/<interface>/<port number>#

Ensure the following values are set:

- **enable-diffserv: true**
- **access-diffserv: true**

Note: A traffic filter must be created to ensure proper mapping from 802.1p to DiffServ for this access port.

QoS on the Passport 8600

The Passport 8600 switch provides a hardware-based Quality of Service (QoS). The hardware on the routing switch enables it to classify 802.1p- and DiffServ CodePoint (DSCP)-marked packets. The Passport 8600 has eight output queues per port into which packets are placed. The eight queues on the Passport 8600 are serviced according to a guaranteed Weight Round Robin (WRR) routine. See Table 35.

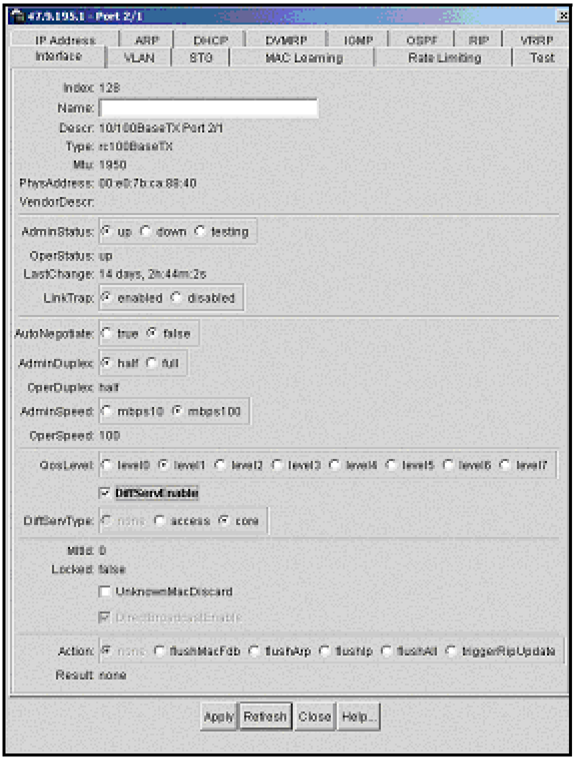
Table 35
WWR on the Passport 8600

IP service class	DSCP	Packet transmission opportunity	Percentage weight
Network	7	2	6%
Premium	6	32	100%
Platform	5	10	31%
Gold	4	8	25%
Silver	3	6	18%
Bronze	2	4	12%
Standard	1	2	6%
User-defined	0	0	0%

Passport 8600 port QoS configuration

The Passport 8600 ports are configured for the core DiffServ type. To enable QoS on the ports of the Passport 8600, the DiffServEnable check box must be selected. Set the DiffServType to core. See Figure 67 on page 266.

Figure 67
Passport 8600 port configuration



Index: 128
Name:
Descr: 10/100BaseTX Port 2/1
Type: rc100BaseTX
Mtu: 1950
PhysAddress: 00:e0:7b:ca:89:40
VendorDescr:

AdminStatus: ● up ○ down ○ testing
OperStatus: up
LastChange: 14 days, 2h:44m:2s
LinkTrap: ● enabled ○ disabled

AutoNegotiate: ○ true ● false
AdminDuplex: ● half ○ full
OperDuplex: half
AdminSpeed: ○ mbps10 ● mbps100
OperSpeed: 100

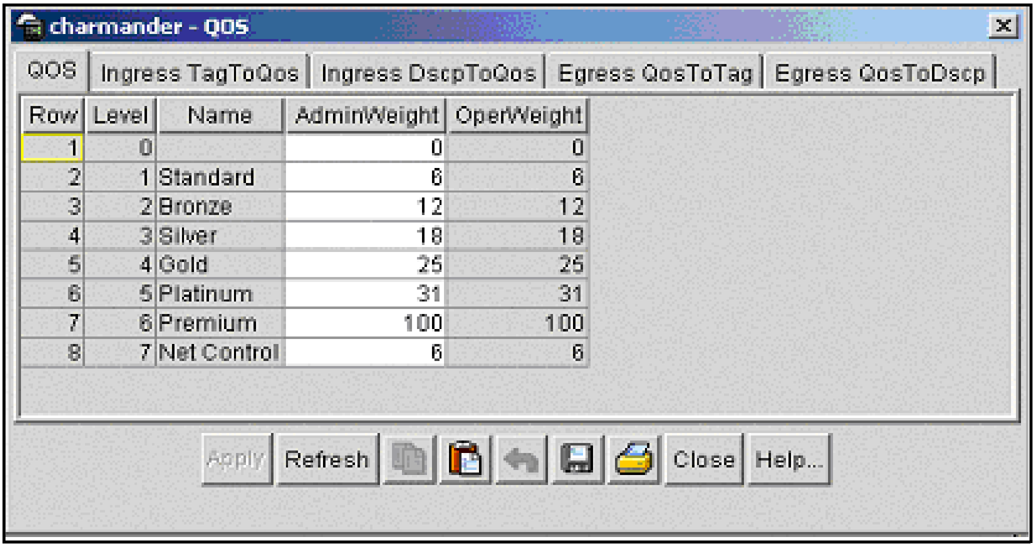
QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7
☑ DiffServEnable
DiffServType: ○ none ○ access ● core

MltId: 0
Locked: false
□ UnknownMacDiscard
☑ DirectBroadcastEnable

Action: ● none ○ flushMacFdb ○ flushArp ○ flushIp ○ flushAll ○ triggerRipUpdate
Result: none

The DSCP marking and 802.1p bits are forwarded and routed unaffected, if the ports are configured for the core DiffServ type. Untagged and bridged packets are placed into QoS queues based on DSCP-to-QoS mappings. Untagged and routed packets are placed into QoS queues based on DSCP-to-QoS mappings. Figure 68 on page 267 shows the Passport 8600 QoS mappings.

Figure 68
Passport 8600 Qos mappings



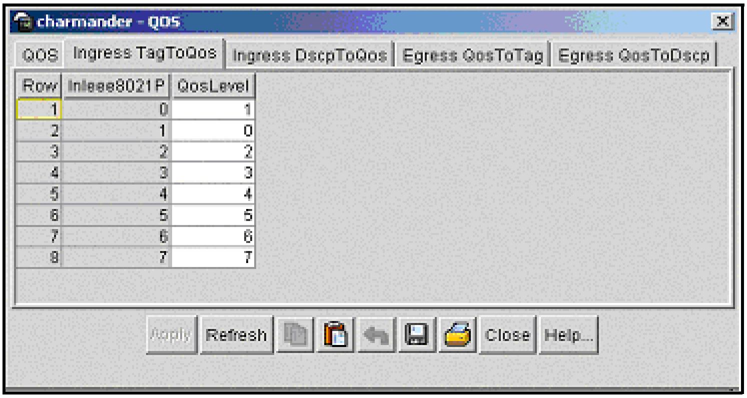
Row	Level	Name	AdminWeight	OperWeight
1	0		0	0
2	1	Standard	6	6
3	2	Bronze	12	12
4	3	Silver	18	18
5	4	Gold	25	25
6	5	Platinum	31	31
7	6	Premium	100	100
8	7	Net Control	6	6

Internet Telephones do not support 802.1p user priority markings. The importance of 802.1p priorities comes into play when using Layer 2 switches that do not view information at an IP level.

Nortel Networks has defined that the Internet Telephones mark the 802.1p priority with a value of ‘110’, a decimal value of 6 (0.6). By default, the Internet Telephone 802.1p priority is mapped to QoS level 6. It is not necessary to changes these values.

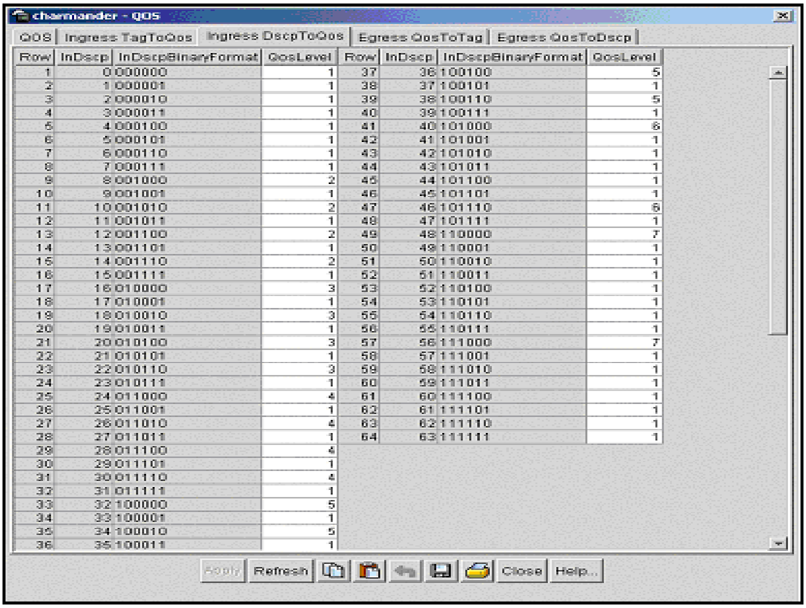
DSCP queue assignment tables show the mapping of Layer 3 DSCP to internal hardware queues on the BPS 2000. The default settings of the Passport 8600 DSCP to QoS assignments already map VoIP voice and control packets to QoS level 6. Nortel Networks standards have defined that VoIP voice packets are to be marked with DSCP values of 46 (0x2E) and VoIP signaling packets (call setup) are to be marked with DSCP values of 40 (0x28). See Figure 69 on page 268, Figure 70 on page 268, Figure 71 on page 269, and Figure 72 on page 269.

Figure 69
Passport 8600 ingress tag to QoS mapping



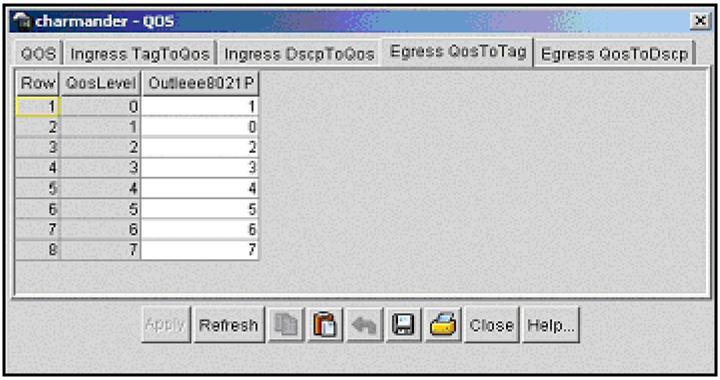
Row	InIeee8021P	QosLevel
1	0	1
2	1	0
3	2	2
4	3	3
5	4	4
6	5	5
7	6	6
8	7	7

Figure 70
Passport 8600 ingress DSCP to QoS mapping



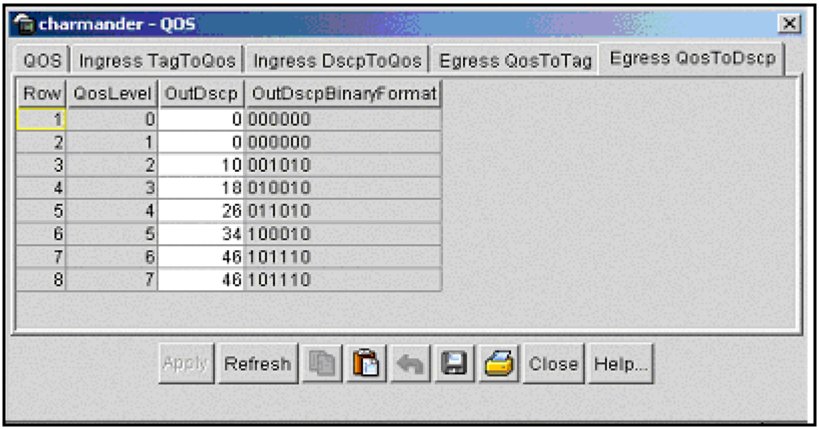
Row	InDscp	InDscpBinaryFormat	QosLevel	Row	InDscp	InDscpBinaryFormat	QosLevel
1	0	000000	1	37	36	100100	5
2	1	000001	1	38	37	100101	1
3	2	000010	1	39	38	100110	5
4	3	000011	1	40	39	100111	1
5	4	000100	1	41	40	101000	6
6	5	000101	1	42	41	101001	1
7	6	000110	1	43	42	101010	1
8	7	000111	1	44	43	101011	1
9	8	001000	2	45	44	101100	1
10	9	001001	1	46	45	101101	1
11	10	001010	2	47	46	101110	6
12	11	001011	1	48	47	101111	1
13	12	001100	2	49	48	110000	7
14	13	001101	1	50	49	110001	1
15	14	001110	2	51	50	110010	1
16	15	001111	1	52	51	110011	1
17	16	010000	3	53	52	110100	1
18	17	010001	1	54	53	110101	1
19	18	010010	3	55	54	110110	1
20	19	010011	1	56	55	110111	1
21	20	010100	3	57	56	111000	7
22	21	010101	1	58	57	111001	1
23	22	010110	3	59	58	111010	1
24	23	010111	1	60	59	111011	1
25	24	011000	4	61	60	111100	1
26	25	011001	1	62	61	111101	1
27	26	011010	4	63	62	111110	1
28	27	011011	1	64	63	111111	1
29	28	011100	4				
30	29	011101	1				
31	30	011110	4				
32	31	011111	1				
33	32	100000	5				
34	33	100001	1				
35	34	100010	5				
36	35	100011	1				

Figure 71
Passport 8600 egress QoS to tag mapping



Row	QosLevel	OutIeee8021P
1	0	1
2	1	0
3	2	2
4	3	3
5	4	4
6	5	5
7	6	6
8	7	7

Figure 72
Passport 8600 egress QoS to DSCP mapping



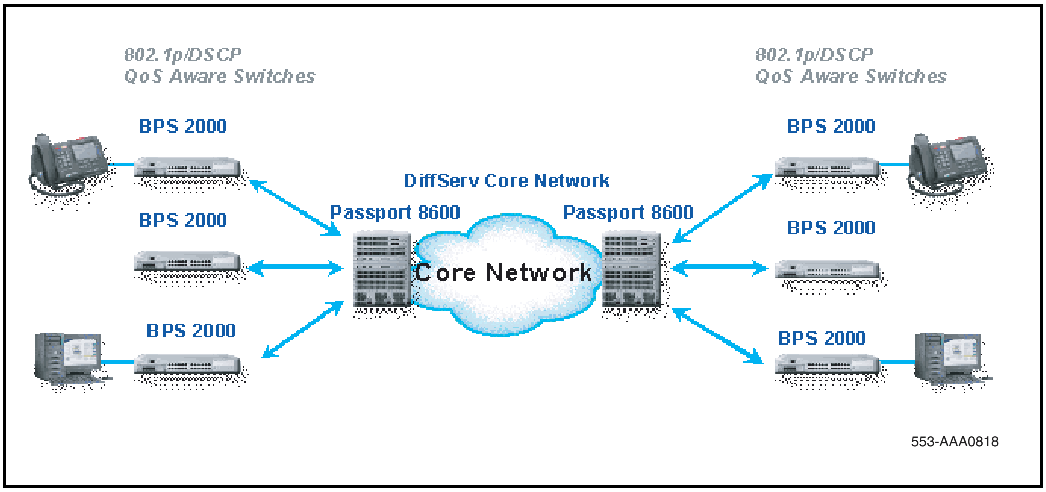
Row	QosLevel	OutDscp	OutDscpBinaryFormat
1	0	0	000000
2	1	0	000000
3	2	10	001010
4	3	18	010010
5	4	26	011010
6	5	34	100010
7	6	46	101110
8	7	46	101110

Layer 3 QoS mechanisms

QoS services are engineered at a Layer 3 level using DiffServ for end-to-end QoS. End-to-end QoS means providing QoS services in both directions from the IP Line card to the Internet Telephones. DiffServ is a Layer 3 QoS service, that enables the prioritization of IP traffic.

There are 6 bits in the second byte of the IPv4 header, referred to as the DiffServ CodePoint (DSCP). They are used to identify the priority of the IP packet on a per-hop basis. Figure 73 is an example of DiffServ-based QoS architecture.

Figure 73
DiffServ-based QoS architecture



Examples of Layer 3 configuration

In these examples, the network consists of Passport 8600 and BPS 2000 devices. The ITGL cards and the Internet Telephones have been configured to Nortel Networks standards for DSCP. VoIP traffic for voice stream has the Expedited Forwarding (EF) DSCP value of decimal 46 (binary 101110). Voice signaling packets have the Class Selector 5 (CS5) DSCP value of decimal 40 (binary 101000).

Nortel Networks Service Classes (NNSC) provides standardized behaviors for marking IP telephony packets. This ensures that VoIP traffic gets mapped to premium queues on Nortel Networks devices.

The standardized default QoS behaviors of Nortel Networks routers/switches enables the prioritization of voice packets. Passport 8600 and BPS 2000 are L2/L3 QoS-aware devices. These devices are capable of prioritizing traffic based on DSCP and 802.1p. The interfaces on the Passport 8600 and BPS 2000 can be configured to choose to distrust or trust 802.1p and DSCP marked traffic.

The BPS 2000 and Passport 8600 places DSCP marked IP packets into the same priority queue. By default, trusted (core) ports on the Passport 8600 and BPS 2000 place DSCP marked traffic into the Premium queue. The Passport 8600 and BPS 2000 are essentially plug-and-play, providing QoS services based on DSCP. The VoIP traffic that is marked with QoS bits will be re-marked to DSCP and 802.1p values of 0 when entering untrusted ports.

Recommended network architecture

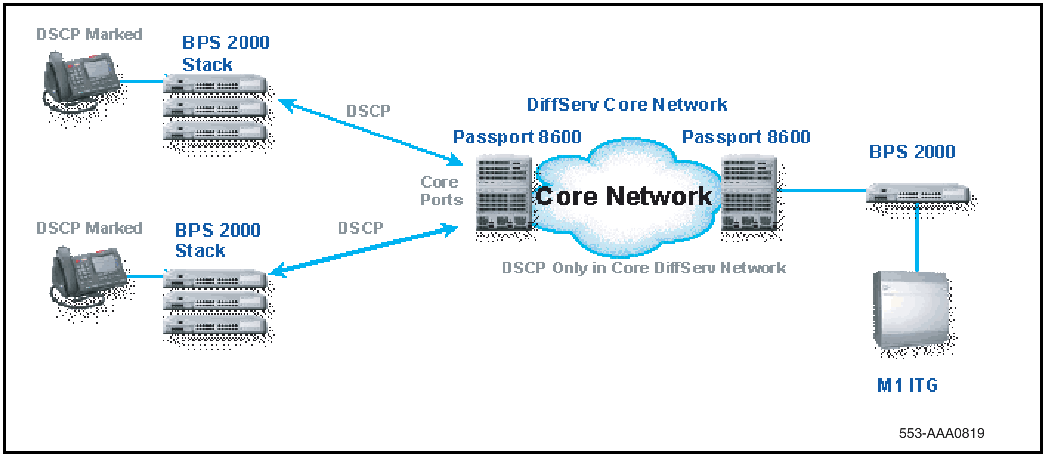
The following sections describe the recommended network architecture for the LAN.

Pure BPS 2000 and Passport 8600 environment

The recommended network architecture in the LAN environment consists consists primarily of Passport 8600 devices and Business Policy Switch 2000 to offer end-to-end DiffServ. The main advantage to this solution is that there is minimal engineering to implement QoS. This implementation requires minimal network management once the network infrastructure is put into place. This simple solution decreases the cost of training employees for network management.

The BPS 2000 and Passport 8600 have been selected as the fundamental network elements as the QoS features are simple to configure and QoS mapping behaviors are configured by default. The pure BPS 2000 and Passport 8600 network architecture functions strictly on DSCP propagating the network. See Figure 74.

Figure 74
Pure BPS 2000 and Passport 8600 environment



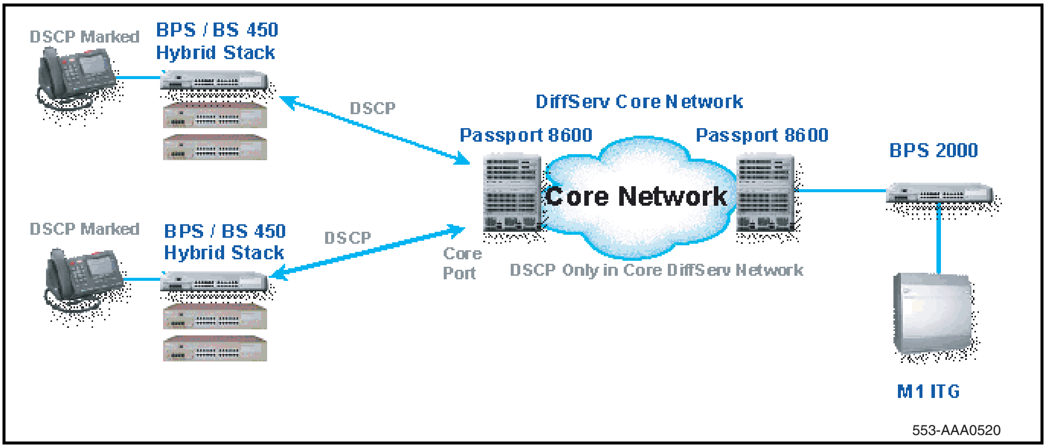
BPS 2000 / BayStack 450 and Passport 8600 environment

In addition to the recommended network architecture consisting of only Business Policy Switch 2000 and Passport 8600 devices, the BayStack 450 can be configured to offer DiffServ capabilities.

By replacing the base unit with a Business Policy Switch 2000, traffic entering the 10/100 Mbps interfaces of the BayStack 450 can be classified and queued. Essentially, the traffic is propagated through the stack up to the BPS 2000, which serves as the uplink on the BPS 2000. The BPS 2000 then acts as the QoS device that performs the queuing, based on the DSCP markings on the IP traffic. See Figure 75.

This implementation reduces the cost of replacing all of the units in a BayStack 450 stack with Business Policy Switch 2000. In BayStack 450 stacks where the redundancy is offered using VRRP, multiple BayStack 450 switches must be replaced to offer DiffServ QoS and redundancy at the same time. To ensure that no network traffic abuse occurs, the cascade ports should be set to ‘untrusted’ roles and the appropriate policies are set using Optivity Policy Services 2.0. See “Optivity Policy Services” on page 84.

Figure 75
BPS 2000/Baystack 450 and Passport 8600 environment



Note: There is no prioritization of packets between individual BayStack 450 switches in the stack.

Appendix C: Optivity Policy Services

Contents

This section contains information on the following topics:

Policies 275
Creating policies for Internet telephones on untrusted ports 279

Policies

A policy is defined as a traffic rule that is implemented based on the following:

- traffic classification
- scheduling
- traffic governing (actions)

Optivity Policy Services (OPS) 2.0 uses policies to govern the flow of traffic travelling through a BPS 2000 and Business Communications Server (BCS). The OPS traffic conditions allow the network administrator to specify the type of network traffic a policy acts upon.

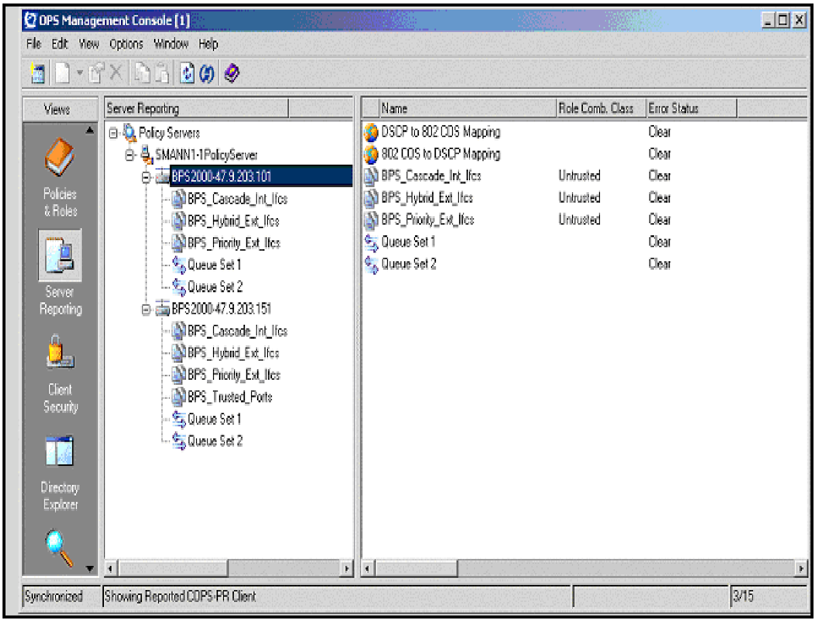
Traffic classification can be determined based on the following:

- VLAN ID
- user priority value
- DSCP value
- protocol type
- IP addresses
- port number

OPS network-management software uses actions to control network traffic by controlling packet flow, by denying packets, or by policing packet flow. Scheduling is used to determine the time and dates a policy are effective. In the event that conflicting policies are put in place, the numeric priority level of the policy is used to determine which policy is selected.

Figure 76 on page 277 and Figure 77 on page 278 show the OPS Management Console.

Figure 76
OPS Management Console



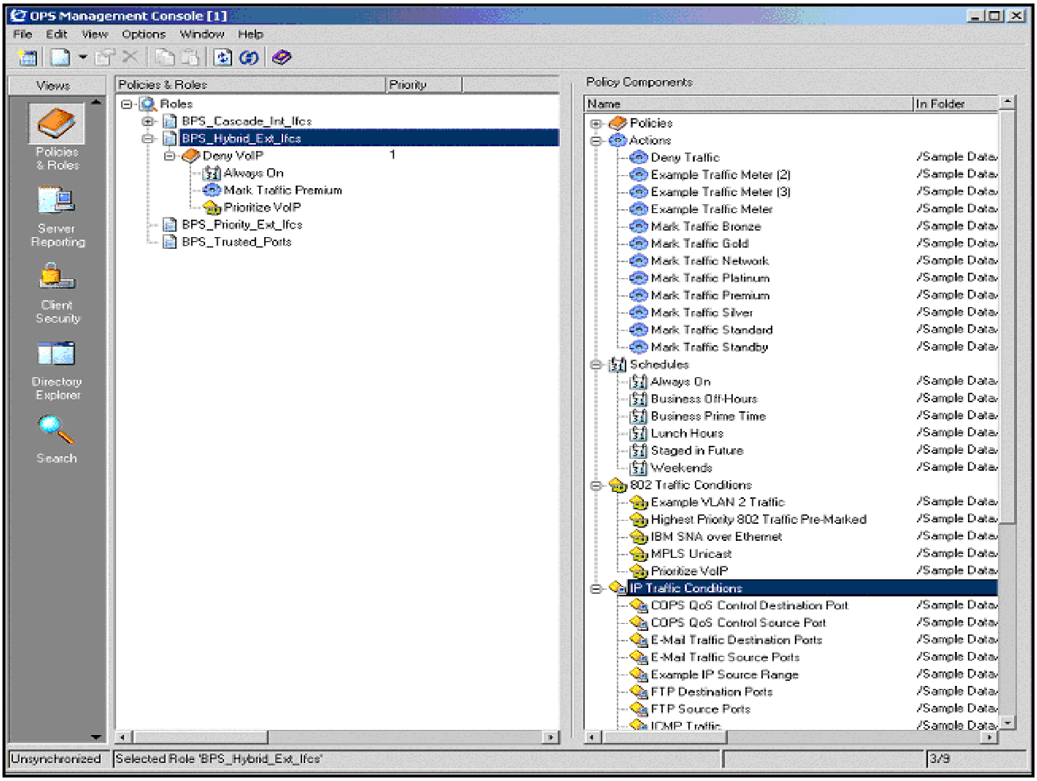
Server Reporting

- Policy Servers
  - SMANN1-1PolicyServer
    - BPS2000-47.9.203.101
      - BPS_Cascade_Int_Ifcs
      - BPS_Hybrid_Ext_Ifcs
      - BPS_Priority_Ext_Ifcs
      - Queue Set 1
      - Queue Set 2
    - BPS2000-47.9.203.151
      - BPS_Cascade_Int_Ifcs
      - BPS_Hybrid_Ext_Ifcs
      - BPS_Priority_Ext_Ifcs
      - BPS_Trusted_Ports
      - Queue Set 1
      - Queue Set 2

Name	Role Comb. Class	Error Status
DSCP to 802 COS Mapping		Clear
802 COS to DSCP Mapping		Clear
BPS_Cascade_Int_Ifcs	Untrusted	Clear
BPS_Hybrid_Ext_Ifcs	Untrusted	Clear
BPS_Priority_Ext_Ifcs	Untrusted	Clear
Queue Set 1		Clear
Queue Set 2		Clear

Synchronized | Showing Reported COPS-PR Client | 3/15

Figure 77
OPS Management Console—expanded view



Policies & Roles	Priority
Roles	
BPS_Cascade_Int_Ifcs	
BPS_Hybrid_Ext_Ifcs	
Deny VoIP	1
Always On	
Mark Traffic Premium	
Prioritize VoIP	
BPS_Priority_Ext_Ifcs	
BPS_Trusted_Ports	

Policy Components

Name	In Folder
Policies	
Actions	
Deny Traffic	/Sample Data/
Example Traffic Meter (2)	/Sample Data/
Example Traffic Meter (3)	/Sample Data/
Example Traffic Meter	/Sample Data/
Mark Traffic Bronze	/Sample Data/
Mark Traffic Gold	/Sample Data/
Mark Traffic Network	/Sample Data/
Mark Traffic Platinum	/Sample Data/
Mark Traffic Premium	/Sample Data/
Mark Traffic Silver	/Sample Data/
Mark Traffic Standard	/Sample Data/
Mark Traffic Standby	/Sample Data/
Schedules	
Always On	/Sample Data/
Business Off-Hours	/Sample Data/
Business Prime Time	/Sample Data/
Lunch Hours	/Sample Data/
Staged in Future	/Sample Data/
Weekends	/Sample Data/
802 Traffic Conditions	
Example VLAN 2 Traffic	/Sample Data/
Highest Priority 802 Traffic Pre-Marked	/Sample Data/
IBM SNA over Ethernet	/Sample Data/
MPLS Unicast	/Sample Data/
Prioritize VoIP	/Sample Data/
IP Traffic Conditions	
COPS QoS Control Destination Port	/Sample Data/
COPS QoS Control Source Port	/Sample Data/
E-Mail Traffic Destination Ports	/Sample Data/
E-Mail Traffic Source Ports	/Sample Data/
Example IP Source Range	/Sample Data/
FTP Destination Ports	/Sample Data/
FTP Source Ports	/Sample Data/
ICMP Traffic	/Sample Data/

Unsynchronized | Selected Role 'BPS_Hybrid_Ext_Ifcs' | 3/9

To put a policy into effect, it must be applied to a role. A role serves as a identifier that clusters together interfaces with similar functions. Roles can be created as 'trusted' or 'untrusted' using the BPS 2000 web GUI interface.

Creating policies for Internet telephones on untrusted ports

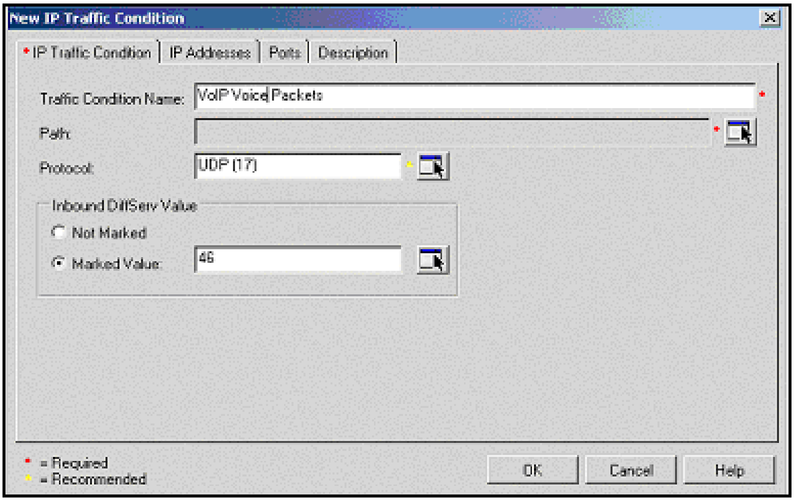
IP traffic conditions

It is necessary to first define the IP traffic conditions that specify what VoIP traffic is coming out of the i2050 software client. There are two types of traffic:

- voice packets
- control packets

A new IP traffic condition is created for the VoIP voice packets to be filtered, based on UDP protocol network traffic and Inbound DiffServ Value marked as 46. Another new IP traffic condition is created for the VoIP data packets to be filtered, based on TCP protocol and Inbound DiffServ Value marked as 40. See Figure 78 and Figure 79 on page 280.

Figure 78
New IP traffic condition – voice packets



Traffic Condition Name: VoIP Voice Packets *

Path: *

Protocol: UDP (17) *

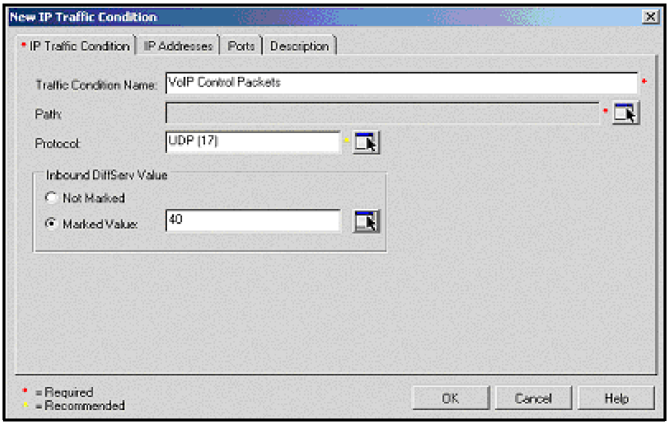
Inbound DiffServ Value

○ Not Marked

● Marked Value: 46

* = Required
* = Recommended

Figure 79
New IP traffic condition – control packets



Traffic Condition Name: VoIP Control Packets *

Path: *

Protocol: UDP (17) *

Inbound DiffServ Value

○ Not Marked

● Marked Value: 40

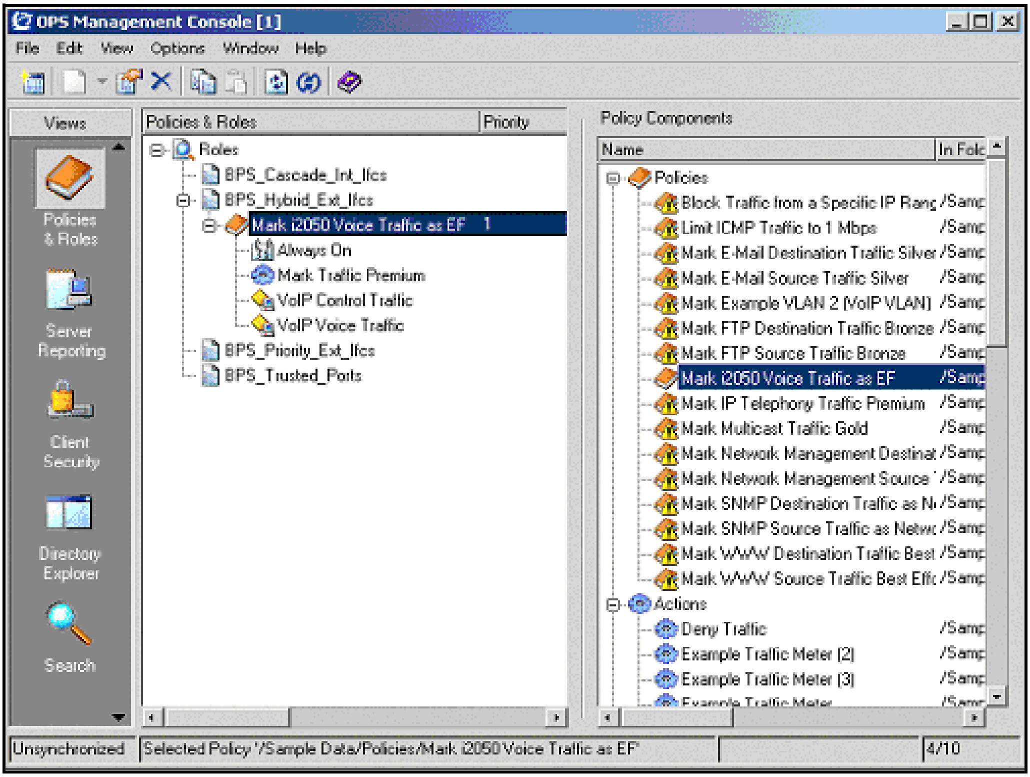
* = Required
* = Recommended

Optivity Policy Services 2.0 already has predefined schedules and actions that can be used. In this example, a policy for marking i2050 VoIP traffic can be created with the following parameters:

- IP Traffic Condition: VoIP Voice Packets and VoIP Control Packets (as created in “IP traffic conditions” on page 279)
- Schedules: Always On (predefined schedule)
- Actions: mark traffic Premium (predefined action)

See Figure 80 on page 281.

Figure 80
Mark voice traffic


OPS Management Console [1]
File Edit View Options Window Help
Views
Policies & Roles
Server Reporting
Client Security
Directory Explorer
Search
Policies & Roles
Priority
Roles
BPS_Cascade_Int_Ifcs
BPS_Hybrid_Ext_Ifcs
Mark i2050 Voice Traffic as EF 1
Always On
Mark Traffic Premium
VoIP Control Traffic
VoIP Voice Traffic
BPS_Priority_Ext_Ifcs
BPS_Trusted_Ports
Policy Components
Name
In Fold
Policies
Block Traffic from a Specific IP Rang /Samp
Limit ICMP Traffic to 1 Mbps /Samp
Mark E-Mail Destination Traffic Silver /Samp
Mark E-Mail Source Traffic Silver /Samp
Mark Example VLAN 2 (VoIP VLAN) /Samp
Mark FTP Destination Traffic Bronze /Samp
Mark FTP Source Traffic Bronze /Samp
Mark i2050 Voice Traffic as EF /Samp
Mark IP Telephony Traffic Premium /Samp
Mark Multicast Traffic Gold /Samp
Mark Network Management Destinat /Samp
Mark Network Management Source /Samp
Mark SNMP Destination Traffic as N /Samp
Mark SNMP Source Traffic as Netwo /Samp
Mark WWW Destination Traffic Best /Samp
Mark WWW Source Traffic Best Effo /Samp
Actions
Deny Traffic /Samp
Example Traffic Meter (2) /Samp
Example Traffic Meter (3) /Samp
Example Traffic Meter /Samp
Unsynchronized
4/10

Selected Policy '/Sample Data/Policies/Mark i2050 Voice Traffic as EF'

Appendix D: Port number tables

Contents

This section contains information on the following topics:

Introduction 283
Succession Call Server port numbers 284
Succession Signaling Server port numbers 286
IP Line port numbers 287
IP Trunk port numbers 289
Internet Telephony Gateway (ITG) port numbers 290
OTM port numbers 291
Remote Office port numbers 291
CallPilot port numbers 292
Symposium port numbers 296

Introduction

This appendix has port number tables for all Meridian 1, Succession 1000, Succession 1000M VoIP products.

All ports specified in the following tables are “Listen” ports. That is, these tables specify the destination IP address and destination 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.

Succession Call Server port numbers

Table 36
Succession Call Server port numbers (Part 1 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
CS	TCP	3313	ipDB-		proprietary
CS	TCP	3312	ipDB-		proprietary
CS	TCP	32783	ipDB-		proprietary
CS	TCP	32782	ipDB-	Rx IPDB CEMUX	
CS	TCP	32780	ipDB-	IPDB CLAN	
CS	TCP	32784	ipDB-	IPDB TTY	
CS	TCP	32781	ipDB-	SSD	
CS	TCP	8888	any	elan / ami	
CS	TCP	15000	any	Succession Call Server link	
CS	TCP	32784	any	ipDB TTY	
CS	TCP	2010	qo0	CEMUX related	
CS	TCP	1013	any		proprietary
CS	TCP	1017	any		proprietary
CS	TCP	1019	any		proprietary
CS	TCP	7734	any	DTP	
CS	TCP	111	any	sunrpc - portmapper for RPC	
CS	TCP	513	any	rlogin	
CS	TCP	21	any	ftp	used by OTM
CS	TCP	1022	any		

Table 36
Succession Call Server port numbers (Part 2 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
CS	UDP	1929	any	DBA	proprietary
CS	UDP	15000	qu0	rudp	
CS	UDP	5002	any	SNMP query	
CS	UDP	5001	any	SNMP agent	
CS	UDP	161	any	snmp	
CS	UDP	32779	any	IPDB HB	
CS	UDP	67	any	bootp	
CS	UDP	111	any	sunrpc - portmapper	
CS	UDP	69	any	tftp	

Succession Signaling Server port numbers

Table 37
Succession Signaling Server port numbers (Part 1 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SIGSVR	TCP	80	any	http	
SIGSVR	TCP	1720	TLAN	H.323	
SIGSVR	TCP	1720	ELAN	Succession Call Server link	initiated connection on random port
SIGSVR	TCP	1009	any	unknown	
SIGSVR	TCP	23	any	telnet	
SIGSVR	TCP	513	any	rlogin	
SIGSVR	TCP	111	any	sunrep - portmapper	
SIGSVR	TCP	21	any	ftp	
SIGSVR	UDP	16500	any	virtual office	
SIGSVR	UDP	1718	TLAN	H.323	
SIGSVR	UDP	1719	TLAN	H.323	
SIGSVR	UDP	5100	TLAN	i2004	
SIGSVR	UDP	4100	TLAN	i2004	
SIGSVR	UDP	16540	any		proprietary
SIGSVR	UDP	7300	TLAN	i2004	
SIGSVR	UDP	16501	any	virtual office	main office listen for branch office
SIGSVR	UDP	16550	any	election	

Table 37
Succession Signaling Server port numbers (Part 2 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SIGSVR	UDP	15000	ELAN	rudp to Succession Call Server	
SIGSVR	UDP	15001	any	rudp to Succession Call Server	
SIGSVR	UDP	20001	any	sntp	
SIGSVR	UDP	67	any	bootp	
SIGSVR	UDP	162	any	snmp trap	
SIGSVR	UDP	161	ELAN	snmp query	
SIGSVR	UDP	111	any	sunrpc - portmapper	
SIGSVR	UDP	69	any	tftp	

IP Line port numbers

Table 38
IP Line port numbers (Part 1 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
ITG	TCP	1041	ELAN	Succession Call Server link	initiated connection on random port
ITG	TCP	1006	any		proprietary
ITG	TCP	111	any	sunrpc - portmapper	

Table 38
IP Line port numbers (Part 2 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
ITG	TCP	1009	any		proprietary
ITG	TCP	23	any	telnet	
ITG	TCP	21	any	ftp	
ITG	UDP	20001	any	sntp	
ITG	UDP	16550	any	election	
ITG	UDP	15000	ELAN	rudp to Succession Call Server	
ITG	UDP	15001	any		proprietary
ITG	UDP	514	any		proprietary
ITG	UDP	67	any	bootp	
ITG	UDP	161	ELAN	snmp	
ITG	UDP	111	any	sunrpc - portmapper	
ITG	UDP	69	any	tftp	
ITG	UDP	16543	any	intercard sig	
SMC	UDP	5201 -5263	TLAN	RTCP	odd numbers
SMC	UDP	5200 - 5262	TLAN	RTP	even numbers
ITGP	UDP	5201 - 5247	TLAN	RTCP	odd numbers
ITGP	UDP	5200 - 5246	TLAN	RTP	even numbers

IP Trunk port numbers

Table 39
IP Trunk port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
IP Trunk	TCP	6001	ELAN	DCHIP inter-card messaging	
IP Trunk	TCP	1720	TLAN	H.225	
IP Trunk	UDP	67	ELAN	BOOTP Server (on Leader Card)	
IP Trunk	UDP	161	ELAN	SNMP	
IP Trunk	UDP	2300 - 2362	TLAN	RTP	(2300+TCID*2)
IP Trunk	UDP	2301 - 2363	TLAN	RTCP	(2300+TCID*2+1)
IP Trunk	UDP	17300 - 17362	TLAN	RTP	(17300+TCID*2)
IP Trunk	UDP	17301 - 17363	TLAN	RTCP	(17300+TCID*2+1)
IP Trunk	UDP	15000	TLAN	MCDN Call Independent Messaging	
IP Trunk	UDP	2001 - 2002	TLAN	Inter-card communication	
IP Trunk	UDP	5000	TLAN	Network QoS monitor port	

Internet Telephony Gateway (ITG) port numbers

Table 40
ITGW port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
ITGW	TCP	1720, 1723	TLAN	(H.225/H.245)	signaling
ITGW	TCP	variable	TLAN	H.225	H.225 control channel
ITGW	UDP	1718, 1719	TLAN	H.323 RAS	signaling
ITGW	UDP	2300 - 2346	TLAN	RTP	(2300+TCID*2)
ITGW	UDP	2301 - 2347	TLAN	RTCP	(2300+TCID*2+1)
ITGW	UDP	2000, 2001	TLAN	inter-card messaging	
ITGW	UDP	161	TLAN	SNMP	

OTM port numbers

Table 41
OTM port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
OTM	TCP	80	any	HTTP	WebCS, DesktopServices, WebTBS
OTM	TCP	4789 - 5045	any	Virtual System Terminal	
OTM	TCP	139	any	NetBEUI	Windows client file sharing
OTM	TCP	3351	any	Btrieve	StationAdmin
OTM	TCP	1583	any	Btrieve	StationAdmin
OTM	UDP	162	any	SNMP	Alarm Traps (LD117), MaintWindows
OTM	TCP	5099	any	RMI	OTM DECT

Remote Office port numbers

Table 42
Remote Office port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
Remote Office	TCP	12800	TLAN	signaling	
Remote Office	UDP/RTP	20480, 20482	TLAN	RTP	voice

CallPilot port numbers

Table 43
CallPilot port numbers (Part 1 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	21	CLAN/ ELAN	FTP	
	TCP	25	CLAN/ ELAN	SMTP	
	TCP	80	CLAN/ ELAN	WWW	
	TCP	135	CLAN/ ELAN	Location Service	
	UDP	135	CLAN/ ELAN	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)	

Table 43
CallPilot port numbers (Part 2 of 5)

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	1025	CLAN/ ELAN	msdtc	
	TCP	1026	CLAN/ ELAN	msdtc	
	TCPTCP	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	

Table 43
CallPilot port numbers (Part 3 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	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 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	

Table 43
CallPilot port numbers (Part 4 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	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	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	
	UDP	5632	CLAN/ ELAN	pcAnywhere stat	
	TCP	7934	CLAN/ ELAN	IIS	
	TCP	8000	CLAN/ ELAN	Dialogic CTMS	
	TCP	10008	CLAN/ ELAN	CallPilot Access Protocol	

Table 43
CallPilot port numbers (Part 5 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	38037	CLAN/ ELAN	msgsys Intel CBA-Message System	
	TCP	56325	CLAN/ ELAN	CallPilot SLEE	

Symposium port numbers

Table 44
Symposium port numbers (Part 1 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SCCS - AML	TCP	8888	ELAN	AML (Meridian 1 ELAN)	
SCCS - HDX CORBA	TCP	Random port (see Comments)	CLAN	HDX (Host Data Exchange)	Allows exchange of data between SCCS and a 3rd party application or database.
SCCS - HDX CAPI	TCP	1550	CLAN		
SCCS - HDIX NameService	TCP	4422	CLAN		
SCCS - RPC Locator Ports		135			

Table 44
Symposium port numbers (Part 2 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SCCS - SNMP	UDP	161	CLAN or ELAN	SNMP	
SCCS - SNMP traps	UDP	162	CLAN or ELAN	SNMP Traps directed to user defined IP address.	
SCCS - pcAnywhere	TCP	5631	ELAN or CLAN	Remote Admin. Dial-up connection via Modem or LAN.	
SCCS - pcAnywhere	UDP	5632	ELAN or CLAN	Remote Admin. Dial-up connection via Modem or LAN.	
SCCS - MLSM (Mlink)	TCP	3000	CLAN	3rd party CTI to Meridian 1 TAPI.	TAPI is configurable.
SCCS - ACCESS (CPI)					
SCCS - RPC (Fat Client)					
SCCS - RTD (Fat Client)					
SCCS - NCC					
SCCS - Sybase SQL Server		5000			
SCCS - Sybase SQL Backup Server		5001			

Table 44
Symposium port numbers (Part 3 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SCCS - Sybase SQL Monitor Server		5002			
SCCS - DB Notifier		5003			
SCCS - NetBios port					
SCCS - DNS port					
SCCS to DMN		2500	ELAN		

Appendix E: Subnet mask conversion from CIDR to dotted decimal format

Overview

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 in order to configure IP addresses.

The CIDR format expresses the subnet mask as the number of bits counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. Therefore, a typical CIDR format subnet mask 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 Procedure 12 on page 300 to convert a subnet mask from CIDR format to dotted decimal format.

Procedure 12
Converting a subnet mask from CIDR format to dotted decimal format

1 Divide the CIDR format value by 8. The quotient (the number of times that eight divides into the CIDR format value) equals the number of dotted decimal fields containing 255.

In the example above, the subnet mask is expressed as /20. Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.

2 If there is a remainder, refer to Table 45 to obtain the dotted decimal value for the field following the last field containing “255”. In the example of /20 above, the remainder is four. In Table 45, a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next and last field is 240. Therefore the first three fields of the subnet mask are 255.255.240.

3 If there are any remaining fields in the dotted decimal format, they have a value of 0. Therefore, the complete subnet mask in dotted decimal format is 255.255.240.0.

End of Procedure

Table 45
CIDR format remainders

Remainder of CIDR format value divided by eight	Binary value	Dotted decimal value
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix F: DHCP supplemental information

Contents

This section contains information on the following topics:

Introduction to DHCP 302

DHCP messages 303

DHCP message format 303

DHCP message exchange. 304

DHCP options. 305

Vendor Specific/Encapsulated option 306

Site Specific option. 306

IP acquisition sequence 307

Case 1 307

Case 2 309

Case 3 310

Multiple DHCPOFFERS 311

Internet Telephone support for DHCP 312

Full DCHP 312

Partial DCHP 318

DHCP Auto Discovery 318s

Introduction to DHCP

To understand how the i2002 Internet Telephone, i2004 Internet Telephone, and the i2050 Software Phone acquire the needed network configuration parameters automatically, the following section briefly describes the Dynamic Host Configuration Protocol (DHCP). Read this section unfamiliar with DHCP. Topics discussed are helpful for the configuration and future maintenance of the DHCP server and ensure correct implementation with Internet Telephones.

DHCP is an extension of BootP. Like BootP, it operates on the client-server model. Unlike BootP, DHCP has more message types. 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.

In addition, DHCP has a lease system that controls the duration an IP address is leased to a client. The client can request a specific lease length, or the administrator can determine the maximum lease length. A lease can range from one minute to 99 years. When the lease is up or released by the client, the DHCP server automatically retrieves it and reassigns it to other clients, if necessary. This is an efficient and accurate way to configure clients quickly. This saves the administrator from an otherwise repetitive task. IP addresses can be shared among clients that do not require permanent IP addresses.

DHCP messages

There are seven different DHCP messages. Each message relates certain information between the client and server. See Table 46.

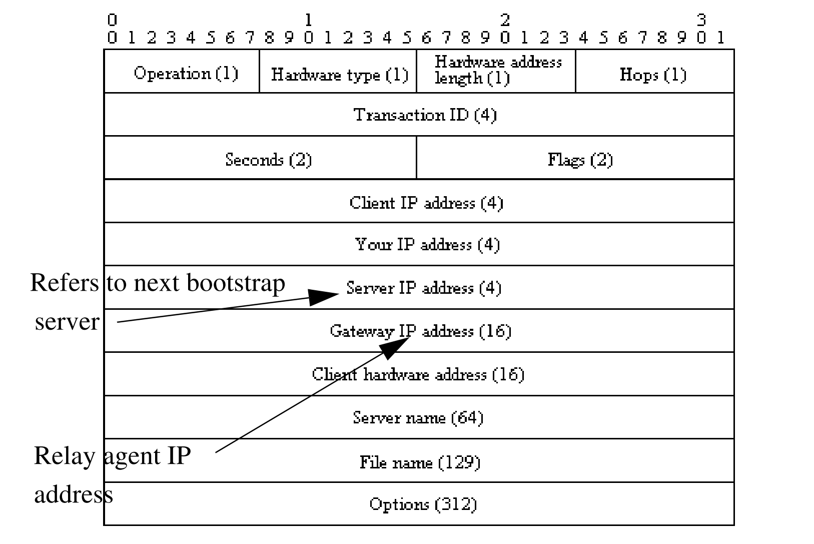
Table 46
DHCP message types

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 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 81 on page 304 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 brackets. If there is not enough data, or there is no data at all, zeros are used to fill in the extra spaces.

Figure 81
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 that are used in this project.

DHCP message exchange

For a client to receive services from a DHCP server, an exchange of DHCP messages between the client and server must take place. The sequence and types of DHCP message exchanged can differ, but the mechanism of acquiring and supplying information remains the same.

Usually the client initiates the exchange with a DHCP message broadcast. Using a broadcast 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, since it knows more about the network, is able to 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. Since the client does not have an IP address yet, the server uses the client's MAC address to uniquely identify it. When the client sees the broadcast, it matches its MAC address against the one in the message.

Using this method, the server and client can supply or receive information through the exchange of their DHCP messages.

DHCP options

DHCP options are the sub-fields of the Options field. They carry additional network configuration information requested by the client such as 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 – 77 are predefined, 1 – 254 can be used for Vendor Specific Options, and 128 – 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 sub-options. For example, the i2004 Internet Telephone requires vendor specific Voice Gateway Media Card information. The vendor, Nortel Networks, decided to carry this information in one of several Site Specific options and then encapsulate it into option 43. Since the information is specific to a Nortel Networks product, it is vendor-specific. Once encapsulated, the information appears as one or more sub-options inside option 43, which the Internet Telephone 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 128-254 are used for encoding.

For Nortel Network's Internet Telephones, 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 Networks 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.

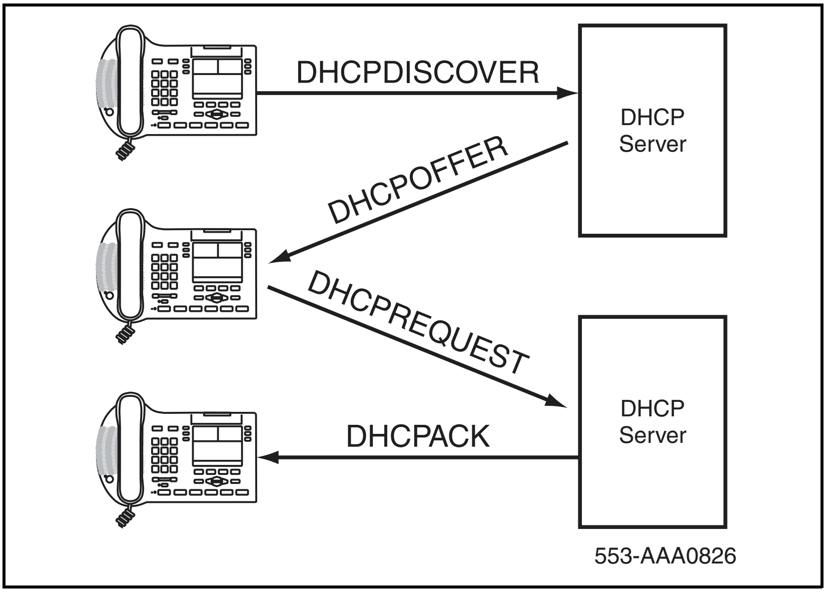
IP acquisition sequence

This section focuses on the mechanics and sequence of the DHCP message exchange as the Internet Telephone uses DHCP for IP acquisition. Although the Internet Telephone requests many network configuration parameters as well as an IP address, the following cases focus on the concept of "how" instead of "what" information is acquired. Also, the Internet Telephone is used as the sample client but most of the illustrations apply to other DHCP clients as well.

Case 1

Case 1 is a typical situation where an i2004 Internet Telephone requests services from a DHCP server. This is illustrated in Figure 82 on page 307 and explained in the following section.

Figure 82
IP acquisition phase – Case 1



1 The Internet Telephone 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 pool(s) for an available IP address and broadcasts a DHCPOFFER message if one is available. Usually the server ARPs or PINGs the IP address to make sure it is not being used.

4 The Internet Telephone 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 Internet Telephone sends out a DHCPREQUEST message with the DHCP server's IP address in the Server IP address field.

6 The DCHP server matches the IP address in the Server IP address field against its own to find out to whom the packet belongs.

7 If the IPs match and there is no problem supplying the requested information, the DHCP server assigns the IP address to the client by sending a DHCPACK.

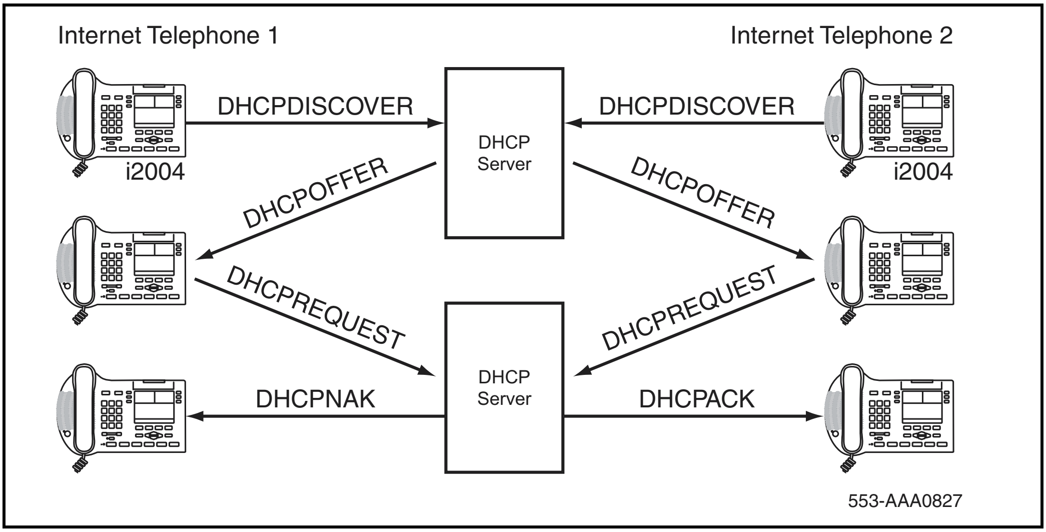
8 If the final offer is not rejected, the IP acquisition sequence is complete.

Case 2

The IP acquisition 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 83 on page 309.
- 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, telling the server the offer is rejected. The client must restart the IP acquisition by sending another DHCPDISCOVER message in search of another offer.

Figure 83
IP acquisition sequence – Case 2



Case 3

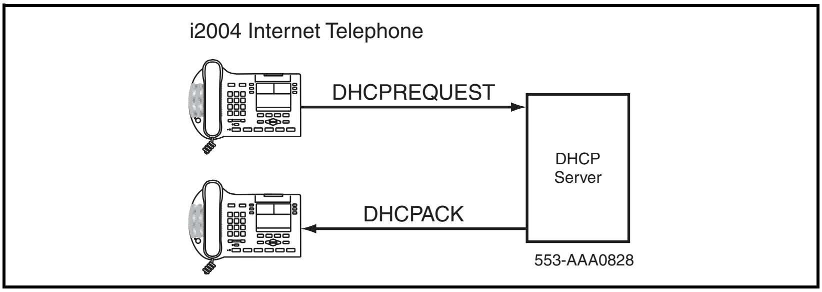
Finally, when a client is finished with a particular IP address, it sends a DHCPRELEASE message to the server which reclaims the IP address. If the client requires the same IP address again, it can initiate the process as follows:

1 The Internet Telephone broadcasts a DHCPREQUEST to a particular DHCP server by including the server's IP address in the Server IP Address field of the message. Since it knows 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 84 on page 310.

Figure 84
IP acquisition sequence – Case 3



Multiple DHCPOFFERS

In some networks, if more than one DHCP server is present, a client can receive multiple DHCPOFFER messages. Under these situations, the IP acquisition sequence depends on the client. The client can wait for multiple offers, or accept with the first offer it receives. If it accepts multiple offers, it compares them before choosing one with the most fitting configuration parameters. When a decision is made, the message exchange is the same as if there is only one DHCP server and proceeds as in the previous cases. The servers that were not chosen to provide the service do not participate in the exchange.

For example, the i2004 Internet Telephone responds only to DHCPOFFERs that have the same unique string identifier, “Nortel-i2004-A”, as the i2004 Internet Telephone. This string must appear in the beginning of the list of Voice Gateway Media Card parameters. Without this string, the i2004 Internet Telephone does not accept the DHPCOFFER, even if all parameters requested and Voice Gateway Media Card information are present. If no valid DHCPOFFERs are sent then, the i2004 Internet Telephone 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 range and no redundancy. DHCP redundancy is a property of DHCP servers. This 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.

Internet Telephone support for DHCP

This section covers the three uses of DHCP (Full, Partial, and VLAN Auto Discovery) by the i2002 and i2004 Internet Telephones.

An “i2004 aware” DHCP server is needed only for the Full DHCP and VLAN Auto discovery. An Internet Telephone can obtain its IP address and subnet mask using Partial DHCP. The “i2004 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 the 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 Internet Telephone firmware. However, in practice, Full DHCP and Auto VLAN are frequently used together.

Full DCHP

DHCP support in the Internet Telephone 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 i2004, encapsulated sub-type, or a Site Specific DHCP option.

In either case, a Nortel i2004-specific option must be returned by the i2004 aware DHCP server in all Offer and Acknowledgement (ACK) messages. The Internet Telephone uses this option’s data it to configure the information required to connect to the TPS.

The DHCP response is parsed to extract the Internet Telephone’s IP address, subnet mask, and gateway. The vendor specific field is then parsed to extract the Server 1 (minimum) and optionally Server 2. By default, Server 1 is always assumed to be the “primary” server after a DHCP session.

For the Internet Telephone to accept Offers/Acks, the messages must contain all of the following:

- A router option (needs a default router to function)
- A subnet mask option
- A Vendor Specific option as specified below or a Site Specific option as specified below.
    - — The initial DHCP implementation required only the Vendor Specific encapsulated sub-option. In inter-op 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 sub-ops 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 Nortel Networks i2004 Terminal DHCP Class Identifier Field

All Internet Telephones (i2002 and i2004 Internet Telephones, and i2050 Software Phone) 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 Nortel i2004
- “-A” uniquely identifies this version

Format for Nortel Networks i2004 Terminal DHCP Encapsulated Vendor Specific Field

This sub-option must be encapsulated in a DHCP Vendor Specific Option (refer to RFC 1541 and RFC 1533) and returned by the DHCP server as part of each DHCP OFFER and ACK message in order for the Internet Telephone to accept these messages as valid.

The Internet Telephone parses this option's data and use it to configure the information required to connect to the TPS.

> ***Note 1:*** Either this encapsulated sub-option must be present, or a similarly encoded site-specific option must be sent. See "Format of the Encapsulated Vendor Specific Sub-option field" on page 314. Configure the DHCP server to send one or the other – not both.
>
> ***Note 2:*** The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the Internet Telephone. 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 Sub-option field

The format of the field is as follows:

- **Type (1 octet):** 5 choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251). Providing a choice of five types allows the Internet Telephone to work in environments where the initial choice could already be in use by a different vendor. Pick 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 string "Nortel-i2004 -A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr." is described in Table 47.

Table 47
Encapsulated Vendor Specific Sub-option field

Parameter	Description
Nortel-i2004-A	Uniquely identifies this as the Nortel option Signifies this version of this specification
iii.jjj.kkk.lll:ppppp	Identifies IP address:port for server (ASCII encoded decimal)
aaa	Identifies Action for server (ASCII encoded decimal, range 0 – 255)
rrr	Identifies 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 The semicolon ";" is used to separate Primary from Secondary server information The period "." is used to signal end of structure

Table 48 on page 316 shows the “pieces” of the Nortel option string. The Nortel designator Nortel-i2004-A is separated from the Connecter Server stings using a comma. The Connect Servers are separated using a semi-colon.

Table 48
Nortel option string

<table>
<tr><td colspan="6">Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.</td></tr>
<tr><td>Nortel Class Identifier Field</td><td>comma</td><td>Primary Connect Server</td><td>semicolon</td><td>Secondary Connect Server</td><td>period</td></tr>
<tr><td>Nortel-i2004-A</td><td>,</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>;</td><td>iii.jjj.kkk.lll:ppppp,aaa,rrr</td><td>.</td></tr>
</table>

Note 1: “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. Internally to i2004 they are stored as 1 octet (0x00 – 0xFF). Note that these fields must be no more than 3 digits long.

Note 2: 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 semi-colon (;). 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, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Note 3: Action code values (0–255):
1 - UNIStim Hello (currently only this type is a valid choice)
all other values (0, 2–255) - reserved

Note 4: 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 "**.**" and "**:**" delimiters guarantee parsing. For example, '001', '01', and '1' would all be parsed correctly and interpreted as value 0x01 internal to the i2004. Note that these fields must be no more than three digits long each.

Note 5: ppppp is the port number in ASCII encoded decimal. The port number must be set to 4100.

Note 6: 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 for Nortel Networks i2004 Terminal DHCP Site Specific Option

This option uses the "reserved for site specific use" DHCP options (number 128 to 254 – refer to RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the Internet Telephone to accept these messages as valid.

The Internet Telephone 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 TPS's.

Note 1: 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 – not both.

Note 2: The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the Internet Telephone. 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 DHCP Site Specific field

The format of the DHCP Site Specific field is same as the format of the Encapsulated Vendor Specific Sub-option field. Refer to "Format of the Encapsulated Vendor Specific Sub-option field" on page 314.

Partial DCHP

Partial DHCP is the default DHCP response from a DHCP server which has not been configured to provide the Vendor Specific information. Using Partial DHCP, an Internet Telephone can obtain its IP address, subnet mask, and gateway IP address. The remainder of the configuration information is manually entered at the Internet Telephone.

DHCP Auto Discovery

DHCP Auto Discovery must be used only if the telephone and PC must be:

- 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 Internet Telephones. The server uses the Site Specific option in the DHCP offer message to convey the VLAN information to the Internet Telephone.

Configuring a DHCP Server for VLAN Discovery is optional. This configuration is done in addition to any done 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 will be the data VLAN and the tagged VLAN will be the voice VLAN. Enter the voice VLAN information into the data VLAN and subnet's DHCP server. Enter the standard Internet Telephone configuration string into the voice VLAN and subnet's DHCP server pool.

The following definition describes the Nortel i2004-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 DHCP OFFER and ACK message for the Internet Telephone to accept these messages as valid. The Internet Telephone pulls the relevant information out of this option and uses it 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 Internet Telephones to work in environments where the initial choice is already in use by a different vendor. Select only one Type byte.

Length (1 octet):

This is variable as 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 “+” or “,” is used to separate fields.
- ASCII “.” is used to signal end of structure.
- XXX, YYY and ZZZ are ASCII encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN Ids. There are a maximum of 10 VLAN IDs can be configured in the current version. String “none” or “NONE” means no VLAN (default VLAN).

The DHCP OFFER message carrying VLAN information is sent out 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 Internet Telephone.

Appendix G: Setup and configuration of DHCP servers

Contents

This section contains information on the following topics:

Install a Windows NT 4 or Windows 2000 server 322

Configure a Windows NT 4 server with DHCP 322

Configure a Windows 2000 server with DHCP 328

Install ISC's DHCP Server 334

Configure ISC's DHCP Server 334

Configure ISC's DHCP to work with the Internet Telephones 335

Example 1: Configuration file 337

Install and configure a Solaris 2 server 340

Install a Solaris 2 Server. 340

Configure a Solaris 2 server 340

Install a Windows NT 4 or Windows 2000 server

To set up 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.

WARNING
If installing 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

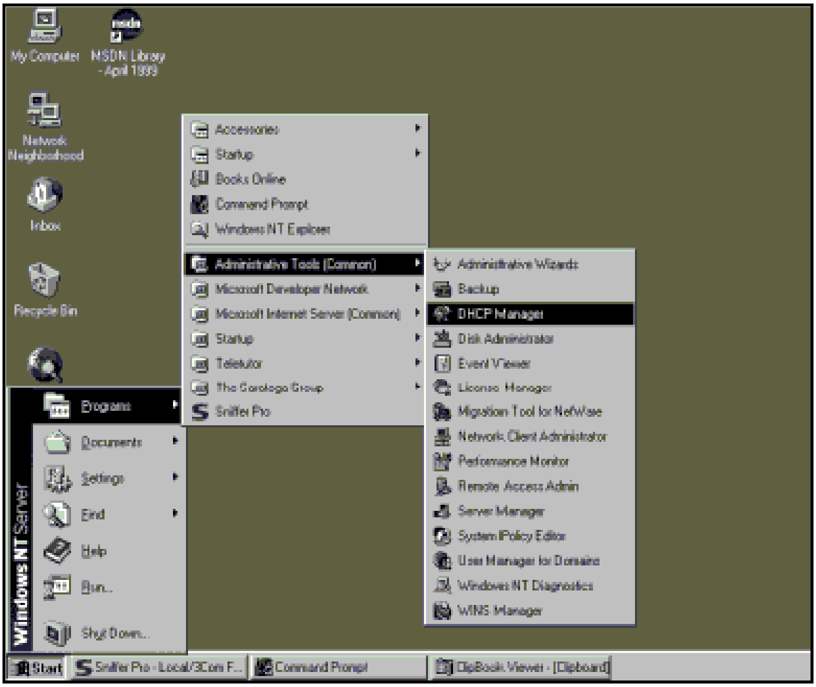
Configure a Windows NT 4 server with DHCP services using the DHCP Manager provided. Follow the steps in Procedure 13 to launch the DHCP Manager.

Procedure 13
Launching the DHCP Manager In Windows NT 4

1 Click on the Windows **Start** button.

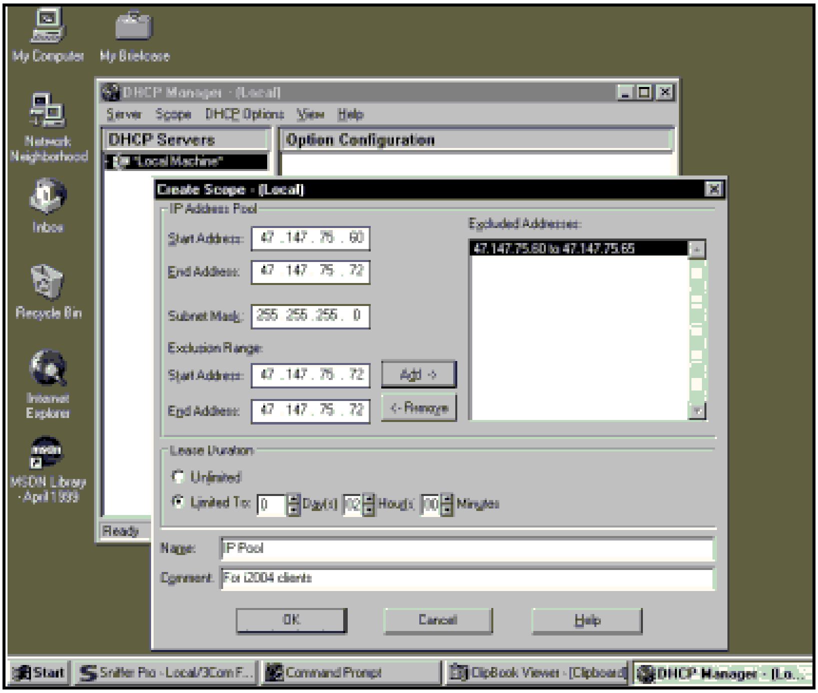
2 Select **Programs | Administrative tools (Common) | DHCP Manager**. See Figure 85 on page 323. The **DHCP Manager** window opens.

Figure 85
Windows NT 4 server screen



3 Double-click **Local Machines** in the left pane. The **Create Scope - (Local)** window opens. See Figure 86 on page 324.

Figure 86
Define a new scope



Create Scope - (Local)

IP Address Pool

Start Address: 47 .147 . 75 . 60

End Address: 47 . 147 . 75 . 72

Subnet Mask: 255 .255 .255 . 0

Exclusion Range:

Start Address: 47 .147 . 75 . 72

End Address: 47 . 147 . 75 . 72

Excluded Addresses:

47.147.75.60 to 47.147.75.65

Lease Duration

○ Unlimited

● Limited To: 0 Day(s) 02 Hour(s) 00 Minutes

Name: IP Pool

Comment: For i2004 clients

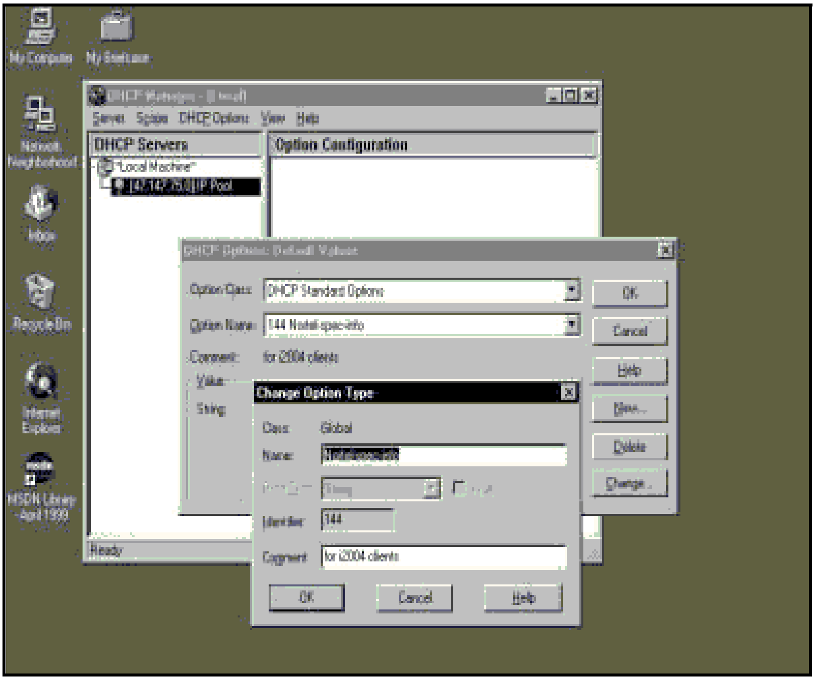
4 Create and then fill in the information. Click **OK** when finished.

5 In the **DHCP Manager - (Local)** window, highlight the scope that serves the Internet Telephones clients.

6 From the **DHCP Options** menu, select **Default Values**. The **DHCP Options - Default Values** window opens.

7 Click the **New** button. See Figure 87 on page 325. The **Change Option Type** window opens.

Figure 87
Define the Nortel-specific option



Option Class: DHCP Standard Options
Option Name: 144 Nortel-spec-info
Comment: for i2004 clients
Value
String

Class: Global
Name: Nortel-spec-info
Data Type: String
Identifier: 144
Comment: for i2004 clients

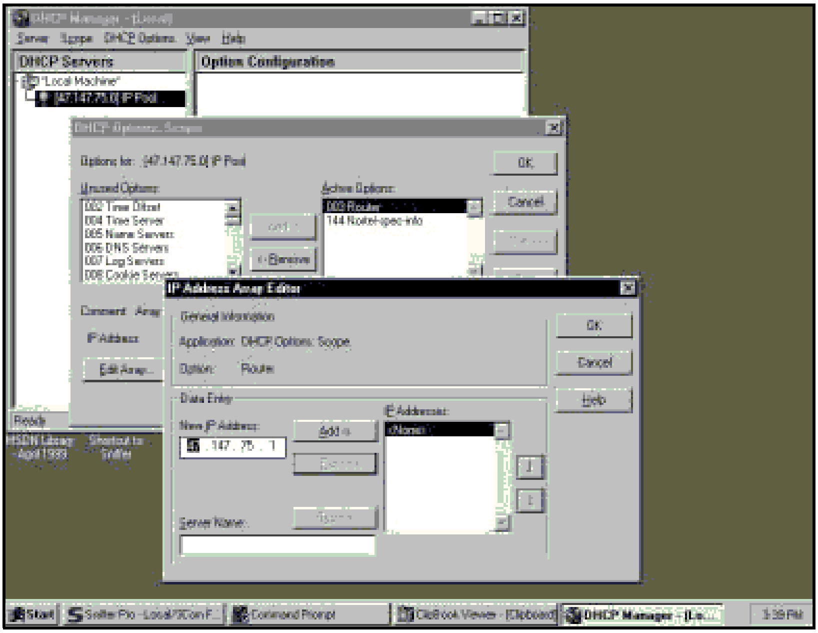
8 Fill in the information and click **OK** when finished. Click **OK** again.

9 From the **DHCP Manager - (Local)** window, highlight the scope to which the DHCP options are to be added.

10 From the **DHCP Options** menu, select **Scope**. The **DHCP Options Scope** window opens.

11 Choose standard DHCP options from the left panel and click the **Add ->** button to add them to the right panel. See Figure 88 on page 326.

Figure 88
Add standard DHCP options to scope



Options for: [47.147.75.0] IP Pool

Unused Options:
002 Time Offset
004 Time Server
005 Name Servers
006 DNS Servers
007 Log Servers
008 Cookie Servers

Active Options:
003 Router
144 Nortel-spec-info

Comment: Array

Application: DHCP Options: Scope

Option: Router

New IP Address: 47 . 147 . 75 . 1

IP Addresses:
<None>

Server Name:

12 Click the **Edit Array** button. The **IP Address Array Editor** window opens. Edit the default value and then click **OK**. Click OK again.

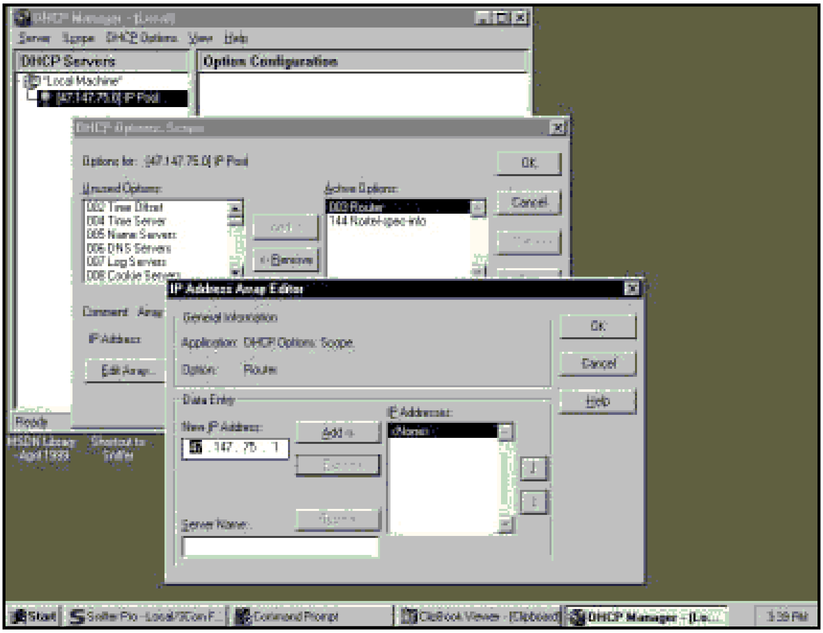
13 From the **DHCP Manager - (Local)** window, highlight the scope that needs to be activated.

14 From the **DHCP Options** menu, select **Scope**. The **DHCP Options Scope** window opens.

15 Click on the **Activate** button.

16 The light bulb next to the scope should turn yellow. See Figure 89 on page 327.

Figure 89
Activate the scope



Options for: [47.147.75.0] IP Pool

Application: DHCP Options: Scope

Option: Router

New IP Address: 47 . 147 . 75 . 1

Note: If DHCP Auto Discovery needs to be configured, see page 318.

End of Procedure

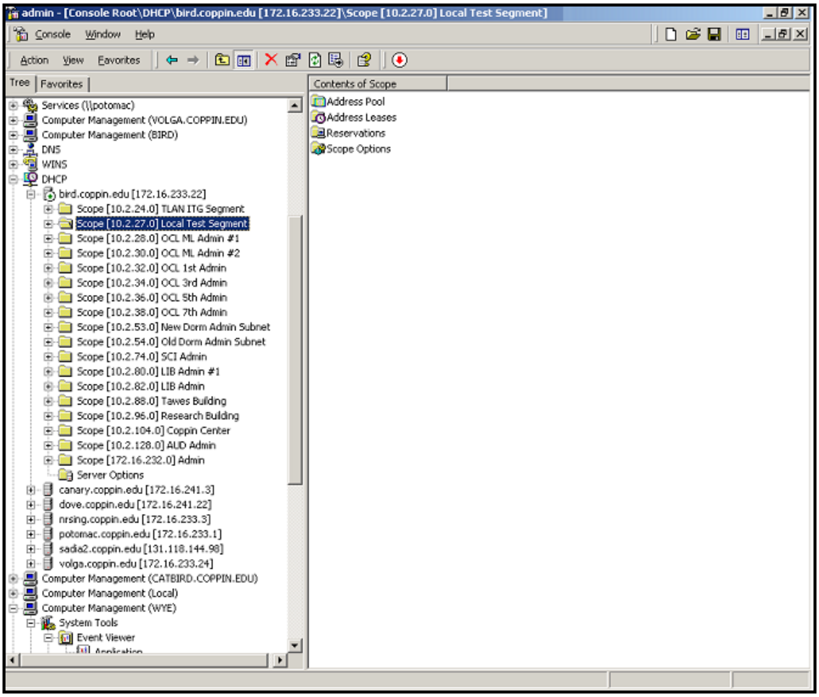
Configure a Windows 2000 server with DHCP

Configure a Windows 2000 server with DHCP services using the DHCP Manager. Follow the steps outlined in “Launching the DHCP Manager in Windows 2000” on page 328.

Procedure 14
Launching the DHCP Manager in Windows 2000

1 Click on the Windows **Start** button. Select **Programs | Administrative Tools | DHCP**. The administrative console window opens. See Figure 90 on page 328.

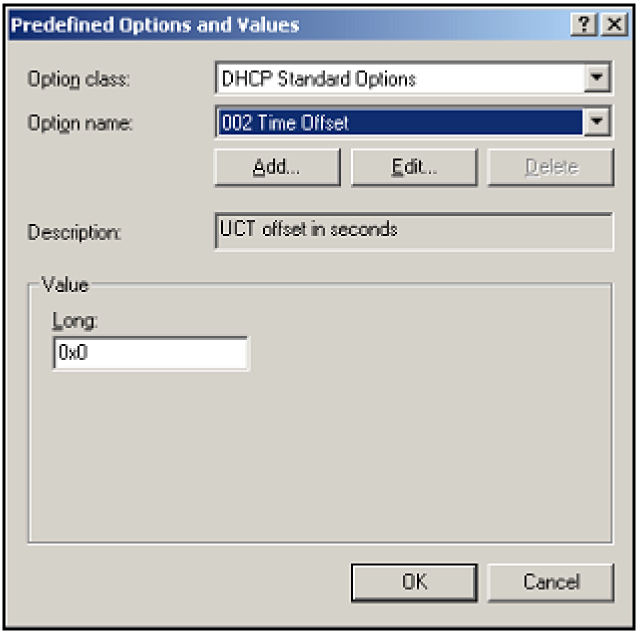
Figure 90
Windows 2000 administration console


admin - [Console Root\DHCP\bird.coppin.edu [172.16.233.22]\Scope [10.2.27.0] Local Test Segment]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Contents of Scope
Address Pool
Address Leases
Reservations
Scope Options
Services (\\potomac)
Computer Management (VOLGA.COPPIN.EDU)
Computer Management (BIRD)
DNS
WINS
DHCP
bird.coppin.edu [172.16.233.22]
Scope [10.2.24.0] TLAN ITG Segment
Scope [10.2.27.0] Local Test Segment
Scope [10.2.28.0] OCL ML Admin #1
Scope [10.2.30.0] OCL ML Admin #2
Scope [10.2.32.0] OCL 1st Admin
Scope [10.2.34.0] OCL 3rd Admin
Scope [10.2.36.0] OCL 5th Admin
Scope [10.2.38.0] OCL 7th Admin
Scope [10.2.53.0] New Dorm Admin Subnet
Scope [10.2.54.0] Old Dorm Admin Subnet
Scope [10.2.74.0] SCI Admin
Scope [10.2.80.0] LIB Admin #1
Scope [10.2.82.0] LIB Admin
Scope [10.2.88.0] Tawes Building
Scope [10.2.96.0] Research Building
Scope [10.2.104.0] Coppin Center
Scope [10.2.128.0] AUD Admin
Scope [172.16.232.0] Admin
Server Options
canary.coppin.edu [172.16.241.3]
dove.coppin.edu [172.16.241.22]
nrsing.coppin.edu [172.16.233.3]
potomac.coppin.edu [172.16.233.1]
sadia2.coppin.edu [131.118.144.98]
volga.coppin.edu [172.16.233.24]
Computer Management (CATBIRD.COPPIN.EDU)
Computer Management (Local)
Computer Management (WYE)
System Tools
Event Viewer
Application

2 Highlight DHCP and expand the DHCP option (if it is not already expanded).

3 Highlight the server and right-click to open the pop-up menu. Select **Set Predefined Options** from the menu. Do not go into the Vendor Specific settings. The **Predefined Options and Values** window opens. See Figure 91 on page 329.

Figure 91
Predefined Options and Values



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

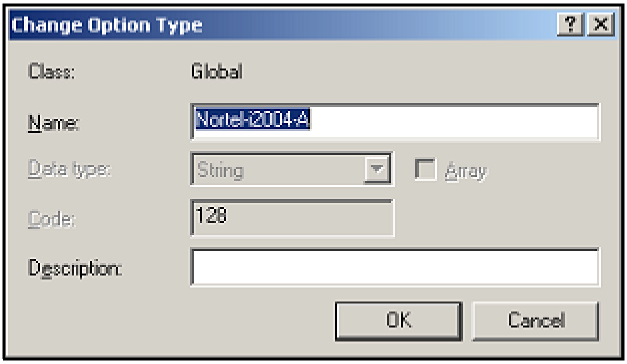
Description: UCT offset in seconds

Value

Long: 0x0

4 Click **Add**. The **Change Option Type** window opens. See Figure 92 on page 330.

Figure 92
Change Options Type



Class: Global

Name: Nortel-i2004-A

Data type: String ▾ □ Array

Code: 128

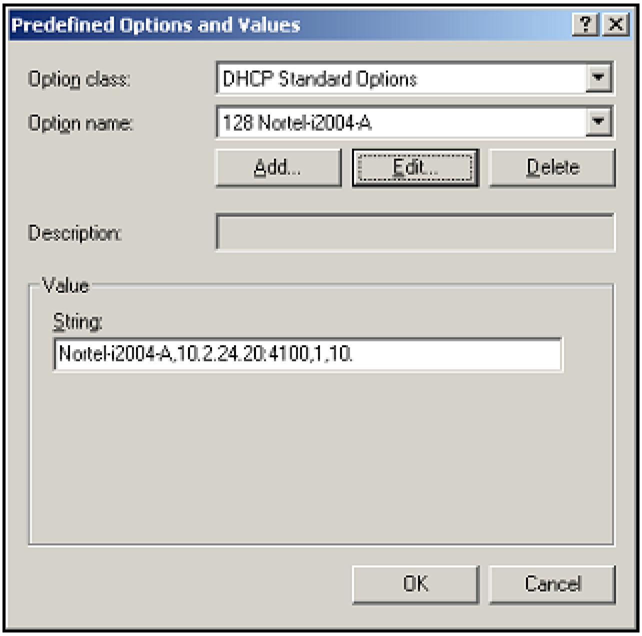
Description:

5 Enter the desired **Name**. For this example, the name of **Nortel-i2004-A** is entered. See Figure 92.

6 Select **Code** 128.

7 Click **OK** to close the window. The Predefined Options and Values window reopens with the string **128 Nortel-i2004-A** entered in the **Option name** field. See Figure 93 on page 331.

Figure 93
Predefined Options and Values with data entered



Option class: DHCP Standard Options

Option name: 128 Nortel-i2004-A

String: Nortel-i2004-A,10.2.24.20:4100,1,10.

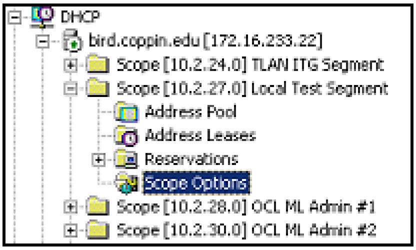
8 Under the **Value** area, enter the following string in the **String** field: **Nortel-i2004-A,x.x.x.x:4100,1,10**; using the following guidelines:

- 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.

9 Click **OK**.

10 The Option Type must now be added to the applicable scopes. Click on the scope **(Scope [x.x.x.x] name)** to expand the scope, then click **Scope Options.** See Figure 94 on page 332.

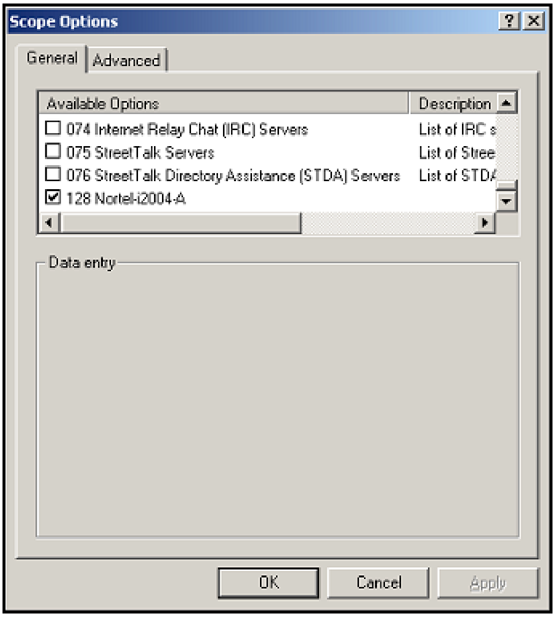
Figure 94
Scope and Scope Options



DHCP
bird.coppin.edu [172.16.233.22]
Scope [10.2.24.0] TLAN ITG Segment
Scope [10.2.27.0] Local Test Segment
Address Pool
Address Leases
Reservations
Scope Options
Scope [10.2.28.0] OCL ML Admin #1
Scope [10.2.30.0] OCL ML Admin #2

11 The **Scope Options** window opens. See Figure 95 on page 332. On the General tab, scroll to the bottom of the list and check the **128 Nortel-i2004-A** option.

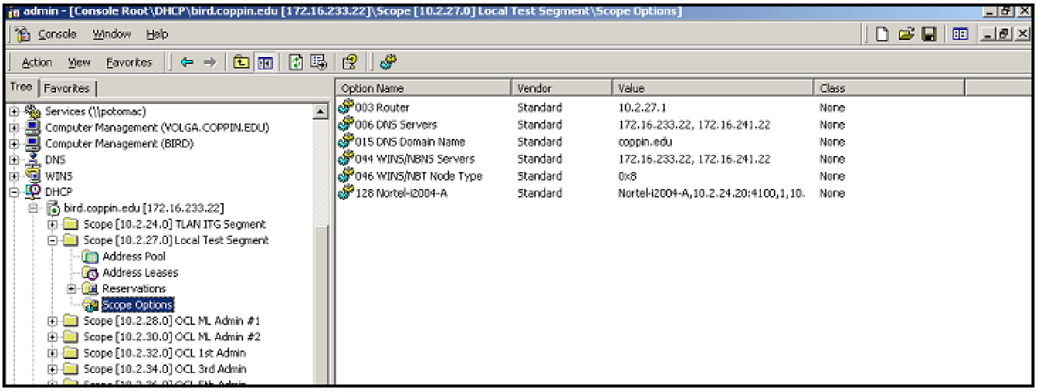
Figure 95
Scope Options



Available Options	Description
□ 074 Internet Relay Chat (IRC) Servers	List of IRC s
□ 075 StreetTalk Servers	List of Stree
□ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☑ 128 Nortel-i2004-A	

12 Click **OK**. The Option Name and Value appear in the right pane of the administrative console window. See Figure 96 on page 333.

Figure 96
Options Name and Value in administrative console



admin - [Console Root\DHCP\bird.coppin.edu [172.16.233.22]\Scope [10.2.27.0] Local Test Segment\Scope Options]

Console
Window
Help
Action
View
Favorites
Tree
Favorites
Services (\\potomac)
Computer Management (VOLGA.COPPIN.EDU)
Computer Management (BIRD)
DNS
WINS
DHCP
bird.coppin.edu [172.16.233.22]
Scope [10.2.24.0] TLAN ITG Segment
Scope [10.2.27.0] Local Test Segment
Address Pool
Address Leases
Reservations
Scope Options
Scope [10.2.28.0] OCL ML Admin #1
Scope [10.2.30.0] OCL ML Admin #2
Scope [10.2.32.0] OCL 1st Admin
Scope [10.2.34.0] OCL 3rd Admin

Option Name	Vendor	Value	Class
003 Router	Standard	10.2.27.1	None
006 DNS Servers	Standard	172.16.233.22, 172.16.241.22	None
015 DNS Domain Name	Standard	coppin.edu	None
044 WINS/NBNS Servers	Standard	172.16.233.22, 172.16.241.22	None
046 WINS/NBT Node Type	Standard	0x8	None
128 Nortel-i2004-A	Standard	Nortel-i2004-A,10.2.24.20:4100,1,10.	None

Note: If DHCP Auto Discovery needs to be configured, see page 318.

End of Procedure

Install ISC's DHCP Server

To set up ISC's DHCP server, read the README file and follow the instructions on how to compile, make, and build the server. Once setup is complete, configure the server by following the description in the "Configure ISC's DHCP Server" on page 334.

CAUTION
Although, Windows NT 4 also has the Vendor Encapsulation Option (option code 43), do not use it to encode the Voice Gateway Media Card information needed by the Internet Telephones. Windows NT 4 enables only 16 bytes of data to be encapsulated, which is not enough to encode all the information needed.

Window NT 4's DHCP server transmits any user-defined option associated within a scope if the client requests it. It does not have the ability to 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's DHCP Server

To configure ISC's 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 on 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 on relevant topics, as well as the location of other man files to read for additional information.

Configure ISC's DHCP to work with the Internet Telephones

Follow the steps in Procedure 15 on page 335 to configure the ISC's DHCP to work with the Internet Telephones.

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.

As indicated in the beginning of this section, read the man files and use "Example 1: Configuration file" on page 337 on to configure ISC's DHCP server to work with the Internet Telephones. Also, a copy of the configuration file used for this project is provided at the end of this section.

Procedure 15
Configuring ISC's DHCP server

1 Configure the server to identify a client correctly as the i2002 or i2004 Internet Telephone. This is done 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's DHCPDISCOVER message match this Hex-encoded string, then the server adds this client to the "i2004-clients" class. Once 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. Use the **allow** or **deny** statement to include or exclude the members of a particular class. For example, the follow 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 Networks special string
option vendor-encapsulated-options
80:3d:4e:6f:72:…;}
```

Note: If a client is not a member of this class, it is not assigned an IP address from this pool, even if there were no other available IP addresses.

4 The DHCPOFFER from the ISC server must include the Voice Gateway Media Card information if the client is an i2002 or i2004 Internet Telephone. There are two methods to encode the necessary information for the i2004 client:

a. Use the **vendor-encapsulated-options** option (as in the previous example) to encode the information as a sub option.

b. 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;

— replace the vendor-encapsulated option inside the pool statement with the definition,

option nortel-specific-info = “Nortel …”;

Note: If DHCP Auto Discovery needs to be configured, see page 318.

End of Procedure

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 i2004 client

option my-vendor-specific-info code 144 = string;


# Declaring a class for i2002 and i2004 clients.
# Add new clients to the class if their Class Identifier match the special i2004 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 Networks special string
          option nortel-specific-info = “Nortel…”;
}
          default-lease-time 180;
          max-lease-time 300;
}
}
```

Finally, before starting 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 set up the Solaris 2 server, consult the accompanying manual and online documentation.

Configure a Solaris 2 server

Follow the steps in Procedure 16 on page 340 to configure Solaris 2 with DHCP.

Procedure 16
Configuring a Solaris 2 server

1 Read the man pages listed below:

- dhcpconfig
- dhcptab
- in.dhcpd

Note: There are directions at the end of each page referring to other sources that are helpful.

2 Collect information about the network such as subnet mask, router/gateway and DNS server IP addresses as specified. Make sure 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 page 318.

End of Procedure

Procedure 17
Configuring Solaris 2 to work with Internet Telephones

1 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

2 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

3 Create a Client Identifier macro by entering in the following:

```
Nortel-i2004-A   m:NI2004="Nortel…”:
```

Or

Use the dhtadm command:

```
dhtadm  -A  -m  Nortel-i2004-A  -d   ‘:NI2004=”Nortel…”:’
```

4 Invoke the DHCP services on the Solaris server by entering at the prompt.:

```
in.dhcpd,
```

Specify –d and/or –v options for debug mode. See man page in.dhpcd for more details.

End of Procedure

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
```

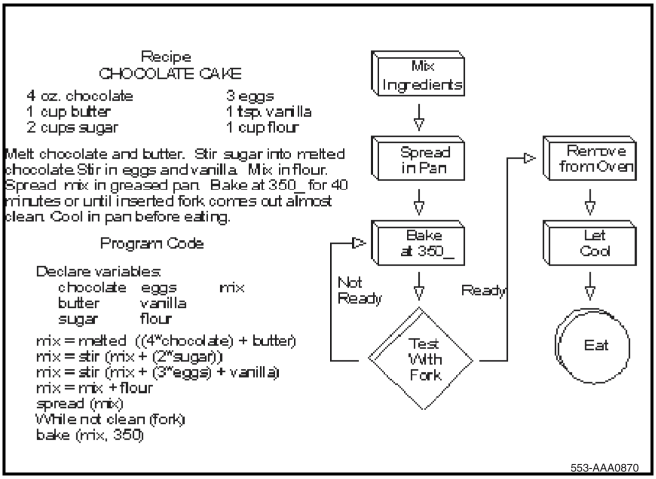
List of terms

Algorithm

A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. Algorithms can be expressed in any language, from natural languages like English or French to programming languages like FORTRAN.

We use algorithms every day. For example, a recipe for baking a cake is an algorithm (see Figure 97). Most programs, with the exception of some artificial intelligence applications, consist of algorithms. Inventing elegant algorithms – algorithms that are simple and require the fewest steps possible – is one of the principal challenges in programming.

Figure 97
Chocolate cake recipe



Recipe
CHOCOLATE CAKE

4 oz. chocolate 3 eggs
1 cup butter 1 tsp. vanilla
2 cups sugar 1 cup flour

Melt chocolate and butter. Stir sugar into melted chocolate Stir in eggs and vanilla. Mix in flour. Spread mix in greased pan. Bake at 350_ for 40 minutes or until inserted fork comes out almost clean. Cool in pan before eating.

Program Code

```
Declare variables:
    chocolate   eggs      mix
    butter      vanilla
    sugar       flour
mix = melted ((4*chocolate) + butter)
mix = stir (mix + (2*sugar))
mix = stir (mix + (3*eggs) + vanilla)
mix = mix + flour
spread (mix)
While not clean (fork)
bake (mix, 350)
```

ATM

Short for **Asynchronous Transfer Mode**, a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

Current implementations of ATM support data transfer rates of from 25 to 622 Mbps (megabits per second). This compares to a maximum of 100 Mbps for Ethernet, the current technology used for most LANs.

Some people think that ATM holds the answer to the Internet bandwidth problem, but others are skeptical. ATM creates a fixed channel, or route, between two points whenever data transfer begins. This differs from TCP/IP, in which messages are divided into packets and each packet can take a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it makes it less adaptable to sudden surges in network traffic.

When purchasing ATM service, you generally have a choice of four different types of service:

- Constant Bit Rate (CBR) specifies a fixed bit rate so that data is sent at a constant rate. This is analogous to a leased line.
- Variable Bit Rate (VBR) provides a specified throughput capacity but data is not sent evenly. This is a popular choice for voice and video conferencing data.

Unspecified Bit Rate (UBR) does not guarantee any throughput levels. This is used for applications, such as file transfer, that can tolerate delays.

Available Bit Rate (ABR) provides a guaranteed minimum capacity but allows data to be bursted at higher capacities when the network is free.

CBR

Constant Bit Rate. See **ATM** on page 344.

CIR

Committed Information Rate. A Frame relay term. CIR is the level of data traffic in bits that a carrier agrees to handle – not at all times, but averaged over a period of time.

Client

The client part of a client-server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

COPS-PR

Common Open Policy Service (COPS) is an IETF standard (RFC 2748). It provides a standard protocol for exchange of policy information between network servers, and network clients such as routers and switches. COPS-PR (COPS Usage for Policy Provisioning) is a provisioning layer designed to facilitate the implementation of new policies, as defined by Policy Information Bases (PIBs).

Network administrators can quickly deploy new services and configurations across a network, using the COPS-PR layer, to dynamically update network devices with new policies. It provides the necessary services to propagate DiffServ policy information across the network.

DiffServ

Differentiated Services. DiffServ specifies, on a per-packet basis, how IP traffic is handled. The handling is specified based on the packet’s DiffServ CodePoint (DSCP). A method for adding Quality of Service (QoS) to IP networks from the IETF, DiffServ is the preferred Layer 3 QoS mechanism for Succession 3.0.

Operating at Layer 3 only, Diffserv uses the IP Type Of Service (TOS) field as the Diffserv byte (DS byte).

DiffServ domain

A network segment that is DiffServ-aware.

DiffServ edge

Where the DiffServ domain begins. Defined in the DiffServ Architecture RFC 2475.

DiffServ Edge Node

The first Layer 3-aware device that a packet encounters.

DSCP

DiffServ CodePoint. Six bits in an IP packet header that specify how a packet is to be handled on an IP network.

DSP

Digital Signal Processing, which refers to manipulating analog information, such as sound or photographs that has been converted into a digital form. DSP also implies the use of a data compression technique.

When used as a noun, DSP stands for Digital Signal Processor, a special type of coprocessor designed for performing the mathematics involved in DSP. Most DSPs are programmable, which means that they can be used for manipulating different types of information, including sound, images, and video.

Full-duplex

Transmission in both directions at the same time can occur on the bandwidth. The full bandwidth of the link is available in either direction.

Gateway

In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, allow users on different e-mail systems to exchange messages.

H.323

A standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks. In theory, H.323 should enable users to participate in the same conference even though they are using different video conferencing applications. Although most video conferencing vendors have announced that their products will conform to H.323, it's too early to say whether such adherence will actually result in interoperability.

Half-duplex

Packets are transmitted in only one direction at a time. The send and receive bandwidth is shared. Packet collisions can occur on half-duplex links.

IEEE 802 standards

IEEE

Institute of Electrical and Electronics Engineers, pronounced I-triple-E. Founded in 1884 as the AIEE, the IEEE was formed in 1963 when AIEE merged with IRE. IEEE is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

802 standards

A set of network standards developed by the IEEE. They include:

- IEEE 802.1: Standards related to network management.
- IEEE 802.2: General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the logical link control (LLC) layer and the media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.
- IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.
- IEEE 802.4: Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).
- IEEE 802.5: Defines the MAC layer for token-ring networks.
- IEEE 802.6: Standard for Metropolitan Area Networks (MANs).

IEEE 802.1: network management

Refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- Security: Ensuring that the network is protected from unauthorized users.
- Performance: Eliminating bottlenecks in the network.
- Reliability: Making sure the network is available to users and responding to hardware and software malfunctions.

IEEE 802.1p

The Class of Service bits within an IEEE 802.1Q VLAN tag.

IEEE 802.1Q

The IEEE specification referring to Virtual Local Area Networks (VLANs). It includes "Class of Service" and VLAN ID.

IEEE 802.2: MAC Layer

The Media Access Control Layer is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

See a breakdown of the seven OSI layers in the Quick Reference section of Webopedia.

The MAC sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don't collide.

Different protocols are used for different shared networks, such as Ethernet, Token Ring, and Token Bus.

IP

Abbreviation of **Internet Protocol**, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

The current version of IP is IPv4. A new version, called IPv6 or IPng, is under development.

IPSec

A group of IP security measures. It defines privacy, integrity, authentication, security key management, and tunnelling methods. A secure version of IP, IPSec enables a secure VPN over the Internet, providing optional authentication and encryption at the packet level.

Layer 2 switching

Packets are forwarded based on the destination's MAC address. The switch automatically determines which switch port must be used to send the packet, based on the destination's MAC address. The MAC address location was determined from incoming packets from that MAC address received on that port.

Layer 3 switching

Packet traffic is grouped based on source and destination addresses. The first packet in a flow is routed by a software-based algorithm. Subsequent packets with the same source and destination addresses are switched based on the destination's MAC address (hardware mechanism). This is similar to multi-layer routing and routers with hardware assist.

MIB

Management Information Base. A database of network performance information that is stored on a Network Agent. It contains characteristics and parameters about network devices such as NICs, hubs, switches, and routers. This information is accessed by software like SNMP.

MID

Message Identifier.

MUA

Mail User Agent. The mail program used by an end-user computer to create and read e-mail messages.

NAT

Network Address Translation. It is defined as an internet standard that lets a LAN use both internal and external IP addresses. This protects an internal IP address from being accessed from outside. NAT translates the internal IP addresses to unique IP addresses before sending out packets. NAT is practical when only a few users in a domain need to communicate outside of the domain at the same time.

Object Identifier

Also known as OID. An object is identified as a numeric value that represents some aspect of a managed device. An Object Identifier (OID) is a sequence of numbers, separated by periods, which uniquely defines the object within an MIB.

OID

See **Object Identifier**.

Policy

A set of rules defining how certain network traffic should be treated. The rules consist of classification, marking, and queueing specifications.

Proxy Server

A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Proxy servers have two main purposes:

- **Improve Performance**: Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy server. First user X requests a certain webpage, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such as Compuserve and America Online, for example, employ an array of proxy servers.
- **Filter Requests**: Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of websites.

PSTN

Short for Public Switched Telephone Network, which refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks base on digital technologies, such as ISDN and FDDI.

Telephone service carried by the PSTN is often called plain old telephone service (POTS).

PVC

Permanent Virtual Circuit. All transmitted data between two points follows a pre-determined path.

QoS

Quality of Service. A networking term that specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This allows ATM providers to guarantee to their customers that end-to-end latency will not exceed a specified level.

RMON

Remote Monitoring specification. It is a set of SNMP-based MIBs (Management Information Bases) that define the monitoring, instrumenting, and diagnosis of LANS. It occurs at OSI Layer 2 (DLL). RMON-2 monitors above Layer 2, and can see across segments and through routers. See "SNMP" on page 352.

routing

The process of selecting the correct path for packets transmitted between IP networks by using software-based algorithms. Each packet is processed by the algorithm to determine its destination.

RTP

Real-time Transport Protocol. An IETF standard that supports transport of real-time data, like voice and video, over packet switched networks. It does not provide QoS control.

Server

A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Shared-media hub

A central connecting device in a network that joins communications lines together in a star configuration. Packets received on a shared-media hub are transmitted out of all other ports on the hub. This means all links must be half-duplex.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The first versions of SNMP were developed in the early 1980s. SNMP works by sending messages, called Protocol Data Units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP 1 reports only whether a device is functioning properly. The industry has attempted to define a new set of protocols called SNMP 2 that would provide additional information, but the standardization efforts have not been successful. Instead, network managers have turned to a related technology called RMON that provides more detailed information about network usage.

Subnet

Subnetwork. A segment of an IP network. Packets must be routed in and out of a subnet.

TDM

Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel.

Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

UDP

User Datagram Protocol. Part of the TCP/IP protocol suite. It allows for the exchange of datagrams without acknowledgement or guarantee of delivery. UDP is at Layer 4 of the OSI model.

VLAN

Virtual LAN. A logical grouping of network devices, located on different physical LAN segments, into a single domain. This allows the devices to interwork as though they were on the same segment.

WAN

Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Meridian 1, Succession 1000,
Succession 1000M

Data Networking for Voice over IP

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

Publication number: 553-3001-160
Document release: Standard 1.00
Date: October 2003
Produced in Canada