>THIS IS **THE WAY**

>THIS IS NORTEL™

# > IP Telephony Client Deployment Technical Solution Guide

Enterprise Solution Engineering
Document Date: January 2006
Document Version: 1.0

# Copyright © 2006 Nortel Networks

# Trademarks

**Disclaimer**

This engineering document contains the best information available at the time of publication in terms of supporting the application and engineering of Nortel products in the customer environment. They are solely for use by Nortel customers and meant as a guide for network engineers and planners from a network engineering perspective. All information is subject to interpretation based on internal Nortel test methodologies, which were used to derive the various capacity and equipment performance criteria and should be reviewed with Nortel engineering primes prior to implementation in a live environment.

# Abstract

This Technical Solution Guide defines the recommended designs for implementing IP Telephony clients on a Converged Campus infrastructure. The document provides an overview of the best design practices to successfully implement IP Telephony. Design considerations regarding scalability, security, and virtual LAN (VLAN) deployment are discussed in detail.

The audience for this Technical Solution Guide is intended to be Nortel sales teams, partner sales teams, and end-user customers. All of these groups can benefit from understanding the common design practices and recommended components for deploying IP Telephony Clients.

For any comments, edits, corrections, or general feedback, please contact Dan DeBacker (ddebacke@nortel.com).

# Revision control

| No | Date | Version | Revised by | Remarks |
|---|---|---|---|---|
| 1 | 01/09/06 | 1.0 | D. DeBacker | Final draft of version 1.0 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Acknowledgements

Roy Davis

Scott Fincher

Tim Mendonca

Philippe Michelet

Ralph Santitoro

Jean Turgeon

John Vant Erve

# Table of contents

# Figures and tables

# 1. Overview

The deployment of IP Telephony Clients combines a highly available network infrastructure with proven, feature-rich business telephony and applications. Nortel solutions provide a strong foundation for innovative converged applications such as IP Telephony. The underlying infrastructure must be able to support a multitude of applications and services across a single network. In order to maintain an expected Quality of Experience for the users (minimum latency, packet loss, and jitter) the network must be resilient, reliable, secure, easy to manage (installation, debugging, and monitoring) and still provide flexibility with high performance.

This solution guide highlights various deployment scenarios for IP Telephony, with a focus on the client deployment options with and without authentication. The use of VLAN technology for separation of IP Telephony traffic from normal data traffic is covered, along with the implementation of Quality of Service (QoS) to ensure the best possible end-to-end Quality of Experience for the users of the IP Telephony solutions. Implementation of these solutions on a Converged Campus infrastructure ensures the highest levels of business continuity, reliability, and application availability. The solutions are also easy to implement and manage, thereby reducing total cost of ownership (TCO) and increasing return on investment (ROI).

Solution features:

- Resilient infrastructure with N-1 redundancy (active/active)
- Flexible deployment options for IP Telephony Clients
- QoS capable infrastructure for end-to-end Quality of Experience
- Security of IP Telephony Clients

## 1.1 Scope of document

This document covers the components required and design options for the deployment of IP Telephony Clients on a Converged Campus infrastructure. It highlights the Nortel recommended designs and best practices for implementing IP Telephony specific to the client-side deployment options. While it is impossible to cover every design scenario, this document covers the most prevalent situations encountered within the Enterprise environment. The following highlights the components covered within these designs:

Ethernet switching platforms – edge

- Ethernet Routing Switch 8300
- Ethernet Routing Switch 5520
- Ethernet Switch 460
- Ethernet Switch 470

IP Telephony Clients

- IP Phone 2001, 2002, 2004, 2007, 2033, 1110, 1120E, 1140E
- IP Softphone 2050
- Multimedia Client (used with MCS)

Converged infrastructure technologies

- IEEE 802.1x/Extensible Authentication Protocol (EAP)

- Virtual LANs (VLAN)
- Power over Ethernet (PoE)
- Quality of Service
- Auto Detection Auto Configuration (ADAC) for IP Phones

This document does not cover the design and deployment of wireless Voice over IP (VoIP) client devices. This topic is covered in a separate Technical Solution Guide (*Voice over Wireless LAN Technical Solution Guide*).

# 2. IP Telephony Client deployments

The deployment of IP Telephony Clients requires a clear and consistent strategy in regard to Quality of Service and the actual configuration of the network infrastructure to adequately support a converged environment. The Nortel recommendation for deployment includes the use of a multiple VLAN strategy to segregate voice from data traffic. This is not a requirement for all installations, but remains the overall recommendation for Nortel IP Telephony deployments. The advantages of a multiple VLAN strategy are articulated in the following sections of this document.

To ensure a successful converged environment, you must have Quality of Service. QoS must be supported on the infrastructure from end to end, and a consistent QoS strategy is required to allow the prioritization of VoIP packets, thus providing the best possible Quality of Experience for the end users. Nortel has developed a QoS architecture that will help provide this consistency. This QoS architecture is discussed in detail in the following sections of this document.

# 3. IP Telephony Clients

Nortel IP Phones are the portals to application access, supporting a comprehensive suite of telephony features from Nortel Communication Servers and application presentation for information exchange from network-based application gateways. Serving the needs of organizations of all sizes – from those with users who have basic communications requirements to those whose needs span high call volumes, multimedia presentation and mobility, Nortel has solutions for every worker. Nortel offers desktop solutions for the campus-based worker who prefers a physical phone at the desktop, along with a variety of wireless and soft-client solutions offering real-time communications access for workers who are constantly on the go. With Nortel IP Telephony Clients, customers benefit from the latest in telecommunications technology while leveraging the reliability, quality and cost effectiveness only Nortel can deliver.

## 3.1 Nortel IP Phone 2001

- Multiline set with two-line 24-character bit-mapped LCD display
- One LED for visual ringing alerter/message waiting
- Supports headset splitter box
- Listen speakerphone capability
- Supports local AC or direct inline power from 802.3af-compliant switches
- Four soft keys, five fixed keys, two programmable feature keys and up/down navigation
- Desk or wall mounting
- ADA-compliant dialpad for IP contact center sets

## 3.2 Nortel IP Phone 2002

- Multiline set with two-line 24-character LCD display
- Dual-use incoming call indicator and message waiting light
- Supports direct headset connection (set has built-in amplifier)
- Supports four self-labeling programmable features and four soft feature keys
- Navigation cluster keys gives fast menu, sublist, and call log scrolling
- High-fidelity full-duplex speakerphone supports disabled users with hearing aids
- Supports local AC or direct inline power from 802.3af-compliant switches
- Desk or wall mounting
- ADA-compliant dialpad
- Integrated three-port switch

## 3.3 Nortel IP Phone 2004

- Multiline set with four-line 24-character LCD display
- Dual-use incoming call indicator and message waiting light
- Supports direct headset connection (set has built-in amplifier)
- Supports six self-labeling programmable features and four soft feature keys
- Navigation cluster keys gives fast menu, sublist, and call log scrolling
- High-fidelity full-duplex speakerphone supports disabled users with hearing aids
- Adjustable LCD contrast
- Supports local AC or direct inline power from 802.3af-compliant switches
- Desk or wall mounting
- AD-compliant dialpad
- Integrated three-port switch

## 3.4 Nortel IP Phone 2007

- Multiline set with Enhanced Color 5.7” QVGA LCD Display
- Built-in Touch Screen with customized stylus as standard
- Additional onscreen message waiting indication
- Supports up to 12 self-labeling programmable features and four soft feature keys (communication server dependent)
- Supports local AC or direct inline power from 802.3af standard–compliant switches
- Dual-use incoming call indicator and message waiting light
- Supports web-centric and multimedia-based content as presented by network-based application gateways
- Integrated RJ-8 port supports direct amplified and unamplified headset connection

- User-selectable ringtones
- Adjustable LCD brightness and contrast
- Personalized soft keys
- Desk or wall mounting
- ADA-compliant dialpad
- Integrated three-port switch

## 3.5 Nortel IP Phone 2033

- Single line with the same telephony features of the IP Phone 2001
- Easy to distinguish display
- Backlit 3 x 24 LCD for enhanced viewing angles
- Full duplex handsfree (IEEE 1329 compliant)
- 360 degree room coverage
- Ten fixed keys (Line, Release, Hold, Mute, Volume Up/Down, Messages, Services and Scroll Up/Down)
- Intelligent and Synchronized status indicator with three LEDs viewable from varying angles within the room
- Three self-labeling soft feature keys
- Up to two extension microphones can be added
- High-quality audio – comfort noise generation, silence suppression
- Supports local AC power

## 3.6 Nortel IP Phone 1110

- Single-line phone
- Vertical design for smaller footprint
- High resolution backlit graphical pixel-based display
- Eight fixed keys (Hold, Goodbye, Line/Handsfree (listen only), Volume Up/Down, Expand, Services, Inbox)

- Four soft-label keys
- Integrated three-port 10/100 switch
- Visual ringing alerter/message waiting LED
- Handsfree (listen-only)
- Active Ethernet link LED indication
- XAS supports data applications and web browsing
- 802.3af PoE (Class 2) or AC local power
- Desk or wall mounting options

## 3.7 Nortel IP Phone 1120E

- Multiline phone with four programmable line/feature key appearances
- Vertical design for smaller footprint
- High resolution backlit graphical pixel-based display
- Fourteen fixed keys (Hold, Goodbye, Handsfree, Headset, Volume Up/Down, Mute, Directory, Shift, Quit, Copy, Expand, Services, Inbox)
- Four soft-label keys
- Integrated three-port 10/100/1000 switch
- Integrated headset port for optional wired headset
- USB port for keyboard, mouse, and powered hubs
- Expansion module/console port
- Visual ringing alerter/message waiting LED
- Active Ethernet link LED indication
- XAS/G-XAS supports data applications and web browsing
- 802.3af PoE (Class 3) or AC local power
- Desk or wall mounting options

## 3.8 Nortel IP Phone 1140E

- Multiline phone with 12 programmable line/feature key appearances
- Vertical design for smaller footprint
- High resolution backlit graphical pixel-based display
- Fourteen fixed keys (Hold, Goodbye, Handsfree, Headset, Volume Up/Down, Mute, Directory, Shift, Quit, Copy, Expand, Services, Inbox)
- Four soft-label keys
- Integrated three-port 10/100/1000 switch
- Integrated headset port for optional wired headset
- USB port for keyboard, mouse, and powered hubs
- Expansion module/console port
- Visual ringing alerter/message waiting LED
- Active Ethernet link LED indication
- XAS/G-XAS supports data applications and web browsing
- 802.3af PoE (Class 3) or AC local power
- Desk or wall mounting options

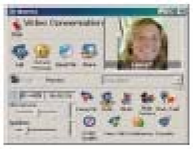
## 3.9 Nortel IP Softphone 2050

The Nortel IP Softphone 2050 provides access to the same services and capabilities as the Nortel IP Phones 2002 and 2004, but it uses the computer and audio resources of a standard PC or laptop. Supported by Nortel Business Communications Manager 50/200/400, Nortel Communication Server 1000, and hybrid Nortel Meridian 1 systems, the Nortel IP Softphone 2050 supports the following features:

- Easily twinned with any other set that the user may have in the office, providing a choice of how users answer or make calls
- Three slide-out feature trays (line/feature keys, dialpad, or combination)
- Supports five special-purpose service keys and four interactive keys
- TAPI compliance for operation with other telephony applications
- Supports direct headset connection through PC USB port
- Message waiting indicator alerts users to new voice messages and incoming calls
- Enhanced USB Audio Kit provides a telephony-optimized sound card to ensure superior audio quality
- Supports local directory imports. Reads Symantec ACT, Microsoft Outlook, and LDAP databases for seamless directory integration

## 3.10 Multimedia Client

Now you can talk, send instant messages, send and receive video, share text and images, and collaborate in real time, using a single Internet connection from your PC and the Nortel Multimedia Client. The Multimedia Client applications provide a wealth of powerful communications features, from traditional telephone service to advanced multimedia communications such as video calling, instant messaging, call screening, real-time call disposition, conferencing, file sharing, and whiteboarding. Advanced web communications include web collaboration, pushing web pages and cobrowsing the web with customers, coworkers, and associates.



The Multimedia Clients can be used to control communications over a PC headset or over the Nortel IP Phone 2004 or 2002, while becoming more productive and efficient and gaining greater control over daily communications. You will be able to efficiently perform diverse communications tasks in a single session, bring the human touch of face-to-face contact to remote communications, and manage incoming and outgoing communications in new ways.

# 4. Example topologies

The following figures depict typical deployment scenarios for IP Telephony clients.

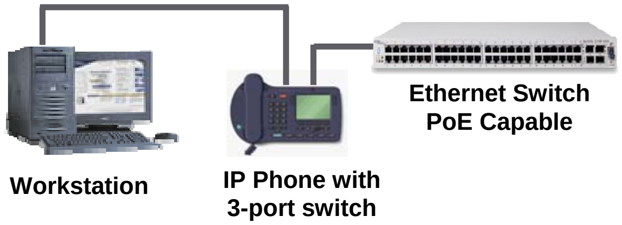


**Figure 1: Workstation/phone single drop to edge switch**

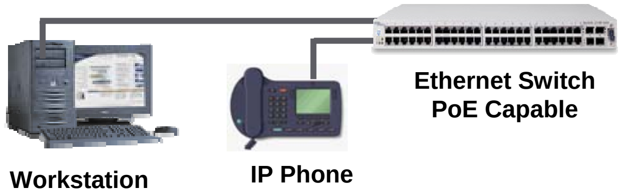


**Figure 2: Workstation/phone separate drops to edge switch**

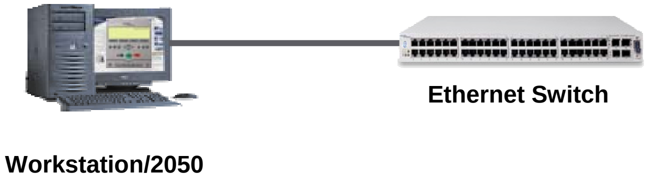


**Figure 3: Workstation using the IP Softphone 2050**

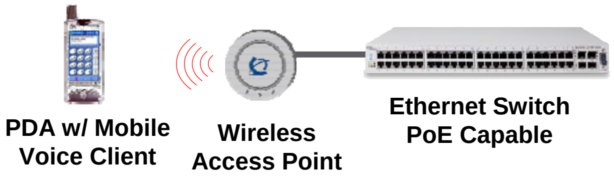


**Figure 4: PDA using the Mobile Voice Client**

Please note that the deployment scenario depicted in Figure 4 is covered in the *Voice over Wireless LAN Technical Solution Guide*.

# 5. Network design considerations

The IP Telephony deployment solution addresses specific areas to consider when designing and deploying IP Telephony Clients on the network infrastructure. This solution is intended to provide optimal network designs and general best practices for implementation and administration. When deploying IP Telephony Clients, you must take into account many design considerations. These can be categorized as follows:

- VLAN separation of voice and data traffic
- IP configuration of the telephony clients
- Quality of Service
- Authentication requirements

Please note that you should review all design recommendations and best practices within this guide against the available features on the Ethernet switching platforms and IP Telephony platforms being deployed and against the release notes for the versions of software being used. As unexpected problems are identified and software fixes are provided, it is imperative to understand the capabilities and limitations of the hardware and software being implemented. Doing so ensures that the design being deployed utilizes the features and functions of the switches to their maximum effectiveness.

## 5.1 VLANs

Since the introduction of IP Telephony from Nortel, the design recommendation has been to segregate the voice traffic from the data traffic using VLANs. There are several advantages to separating this traffic at the edge of the network:

- Simplifies the implementation of QoS for the IP Telephony phonesets. The network administrator can simply enable QoS on a VLAN level – all traffic on the voice VLAN is prioritized over all the other VLANs.
- Isolating the voice traffic provides a level of security for the IP Telephony. Any broadcast or multicast storms that affect the data VLANs will not propagate to the voice VLANs and therefore will not adversely affect the voice traffic.
- Creating separate voice VLANs allows the network administrator to create simple traffic filters that will not allow non-voice traffic on those VLANs – for example, if a user plugged their workstation into the voice VLAN, they would not be able to get anywhere in the network.
- Troubleshooting application level or network level problems is simplified by isolating traffic flows into different VLANs. Understanding that no “normal” data traffic is traversing the voice VLANs eliminates a variable in the troubleshooting process.

The number and size of the voice VLANs will vary depending on the size of the overall network and the number of users on the network. Normally, VLANs have a one-to-one relationship with the IP subnet (VLAN 100 = IP Subnet 10.10.100.0). A recognized practice is to limit the size of the IP subnets to a Class C (254 usable addresses). This helps to minimize the amount of broadcast traffic on the network, improves the efficiency of the network, and helps to isolate areas of the network when troubleshooting.

### 5.1.1 Design recommendation

Implement a multiple VLAN strategy for deployment of IP Telephony Clients, segregating data traffic from VoIP traffic. The only exception is when you use IP Telephony Clients that utilize the

PC as their network device (IP Softphone 2050, MCS client). In this case, it is impossible to segregate the traffic on a VLAN basis.

Create traffic filters on Ethernet switches so non-voice traffic will not be allowed on the voice VLANs.

For IP Telephony traffic, keep the size of the broadcast domains small and manageable. Utilizing a broadcast domain with 254 or 510 usable addresses is deemed a design best practice.

## 5.2 IP configuration of the telephony clients

There are multiple options that you must configure on the Nortel IP Phone in order for it to access the network and register with the call server. Each phone can be configured manually or use Dynamic Host Configuration Protocol (DHCP). The following sections detail these options and provide design recommendations for the deployment of IP Telephony Clients.

### 5.2.1 Accessing configuration menu

There are different ways to access the configuration menu on the various IP Phones. The following table shows ways to access the configuration menu during power-up of the IP Phone.

| IP Phone | # of seconds to Nortel logo after power-up | # of seconds to enter correct key sequence | Key sequence |
|---|---|---|---|
| 2001, 2002, 2004, 1100 series | 4 | 1 | Four feature keys at bottom of display from left to right in sequence |
| 2007 | 4 | 1 | 0 0 7 * in sequence |

**Table 1: Configuration menu access methods for IP Phones**

### 5.2.2 Manual configuration

To configure the IP Phone manually, you must access the configuration section of the phone and enter the IP configuration parameters. See Table 2 on page 17 for descriptions of each of the configuration parameters.

### 5.2.3 Partial DHCP

Partial DHCP configuration uses DHCP to obtain the IP address information for the phone, which includes the IP address, subnet mask, and default gateway. The remaining IP configuration parameters must be manually entered on the phone. See Figure 5 for DHCP packet flow.

### 5.2.4 Full DHCP

Full DHCP configuration uses DHCP to obtain the IP address information for the phone (as described above), along with call server and External Application Server (XAS) configuration information. The VoIP-specific parameters (call server information, XAS information) can be passed to the IP Phones using a DHCP site-specific option – “reserved for site specific use" (DHCP option values 128 to 254). This option must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone to accept these messages as valid. The IP Phone will pull the relevant information out of this DHCP option and use it for configuration. See Figure 5 for DHCP packet flow.

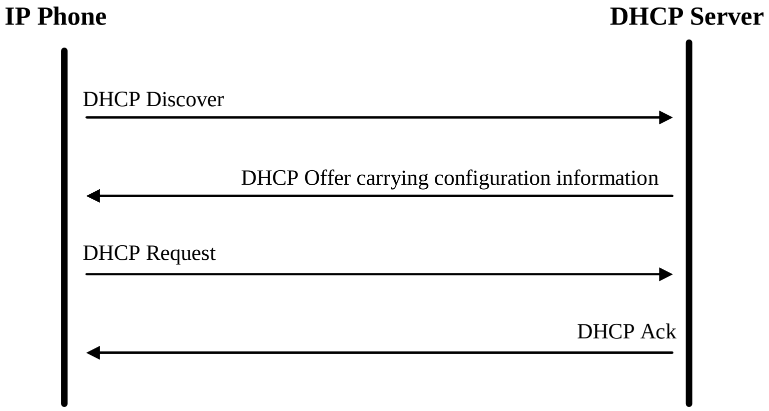


**Figure 5: Standard DHCP packet flow**

The following is detailed information for the DHCP options:

Format of field is: Type, Length, Data

**Type (1 octet)**

Five choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251)

Providing a choice of five types allows the administrator to use any one for the IP Phone. This is beneficial when a type may already be in use for a different application. Pick only one type.

**Length (1 octet)**

Variable – dependent on message content

**Data (variable number octets)**

ASCII based with a format of: “Nortel-i200x-A,w.w.w.w:p,a,r;y.y.y.y:p,a,r;z.z.z.z:p.” where

Nortel-i200x-A uniquely identifies this as the Nortel DHCP VLAN Discovery
x = type of IP Phone (2001, 2002, 2004, 2007, etc.)
-A signifies this version of the phone
w.w.w.w = the IP address of the primary call server
p = UDP port number of the primary call server
a = action code – only valid entry is 1, which is UNIStim hello
r = retry count – valid range from 0 to 255
y.y.y.y = the IP address of the secondary call server
p = UDP port number of the secondary call server
a = action code – only valid entry is 1, which is UNIStim hello
r = retry count – valid range from 0 to 255
z.z.z.z = the IP address of the XAS
p = the UDP port number of the XAS
ASCII comma (,) is used to separate fields.
ASCII semicolon (;) is used to separate server IP information fields.
ASCII colon (:) is used to separate IP address from UDP port number.
ASCII period (.) is used to signal end of structure.

| Configuration Parameter | Manual Config | Partial DHCP | Full DHCP | Comments/Notes |
|---|---|---|---|---|
| IP Address | Required | Provided | Provided | IP address of the IP Phone |
| Subnet Mask | Required | Provided | Provided | Subnet mask of the IP Phone |
| Default Gateway | Required | Provided | Provided | Default gateway for the IP Phone |
| S1 IP Address | Required | No | Provided | IP address of primary call server |
| S1 Port | Required | No | Provided | UDP port number of primary call server |
| S1 Action | Required | No | Provided | Action = 1 is the only valid response |
| S1 Retry Count | Required | No | Provided | Default of 10 |
| S2 IP Address | Optional | No | Optional | IP address of secondary call server (same as S1 if no call server redundancy) |
| S2 Port | Optional | No | Optional | UDP port number of secondary call server (same as S1 if no call server redundancy) |
| S2 Action | Optional | No | Optional | Action = 1 is the only valid response |
| S2 Retry Count | Optional | No | Optional | Default of 10 |
| XAS | Optional | No | Optional | IP address of External Application Server |
| VLAN | Optional | No | Optional | Voice VLAN (0=None, 1=Manual Cfg, 2=Auto) |
| VLAN Filter | Optional | No | Optional | Filters traffic based on 802.1Q tag, only if VLAN is selected |
| Data VLAN | Optional | No | No | Only supported on IP Phones with VLAN-aware 3-port switch |
| Duplex | Optional | No | No | 0=auto is the default for autonegotiation |
| GARP Ignore | Optional | No | No | 0=No is the default (feature to prevent GARP DoS) |

**Table 2: IP Phone configuration parameters**

### 5.2.5 VLAN configuration – Manual/Auto

In addition to Partial or Full DHCP support, the IP Phone provides three different configuration options for voice VLAN usage as detailed below. When using a Data VLAN (VLAN-aware three-port switch on the phone), configure the Data VLAN ID manually on the phone.

- No VLAN

  Use this option in the following design scenario: The IP Phone is connected to an access port of an Ethernet Switch. The port on the Ethernet Switch has only one VLAN configured on it and there is no 802.1Q tagging enabled on that access port. This scenario is typically seen when the phone does not share a port with another device (workstation/PC), and the port on the Ethernet Switch is simply provisioned for the voice VLAN (see Figure 2 on page 13).

- Manual configuration

  Use this option when the phone is connected to an 802.1Q tagged port on the Ethernet Switch. The traffic from the phone must be segregated at the Ethernet Switch. This is done by adding an 802.1Q tag to all the packets being transmitted by the phone to the Ethernet Switch. Conversely, the phone will automatically strip the 802.1Q tag on packets that it receives from the Ethernet Switch. The network administrator must manually configure the VLAN ID on each phone. This VLAN ID becomes the 802.1Q tag appended to the header of each Ethernet packet leaving the IP Phone. The addition of the 802.1Q tag allows traffic from the phone to remain segregated on the voice VLAN. This design scenario is typically deployed when a second device (workstation/PC) is sharing the Ethernet Switch port in the edge closet. Normally, the three-port switch in the phone will be used – one port connecting the workstation/PC, one port connecting the phone (internal), and one port connecting the Ethernet Switch in the closet (see Figure 1 on page 13). With this option, the network administrator must configure the VLAN ID in each IP phone.

- Auto configuration

  The auto configuration option uses DHCP to automatically assign the correct VLAN ID for the phone. The design scenario and use of this option are identical to those described for manual configuration. The major difference between the two options is that with auto configuration, the network administrator does not manually configure the VLAN ID on the phone; the configuration comes from the DHCP server. The following section describes in detail the process for Auto VLAN Discovery on the Nortel IP Phones.

### 5.2.6 Auto VLAN Discovery process

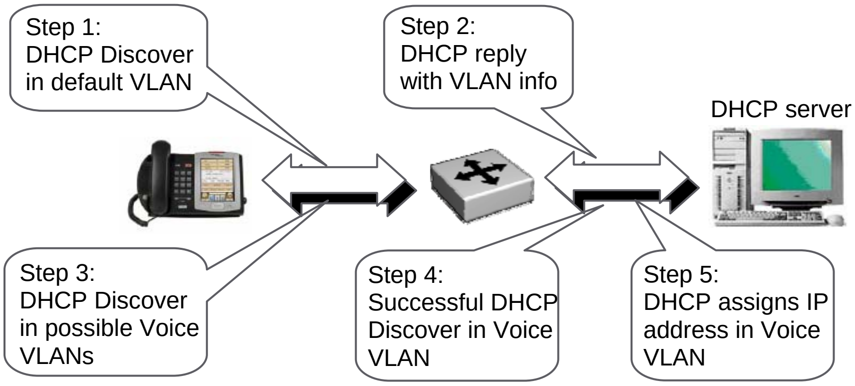

Step 1:
DHCP Discover in default VLAN
Step 2:
DHCP reply with VLAN info
DHCP server
Step 3:
DHCP Discover in possible Voice VLANs
Step 4:
Successful DHCP Discover in Voice VLAN
Step 5:
DHCP assigns IP address in Voice VLAN

**Figure 6: Auto VLAN Discovery process**

When the IP Phone resets, it broadcasts (Layer 2 and Layer 3 broadcast) a DHCP Discover message looking for a DHCP server. Because a VLAN ID has yet to be assigned, the initial Discover packet is sent untagged to the Ethernet edge switch. The edge switch adds the 802.1Q header, tagging the packet with the default VLAN ID for that switch port, and forwards the frame to all ports belonging to the default VLAN.

The DHCP server receives the Discover packet through the network, and responds with a DHCP OFFER message, assigning an IP address consistent with the default VLAN. This is likely to be a temporary address in an Auto VLAN Discovery environment. The server also includes in the DHCP OFFER message a list of the applicable VLAN IDs from which the IP Phone can choose. This list of VLANs is accomplished using DHCP options configured on the DHCP server. The option used to configure VLAN IDs is "reserved for site specific use" (DHCP option values 128 to 254). This option is returned by the DHCP server as part of each DHCP OFFER and ACK message so that the IP Phone accepts these messages as valid. The IP Phone will pull the relevant information out of this option and use it for configuration.

The following is detailed information for the DHCP options:

Format of field is: Type, Length, Data
**Type (1 octet)**
Five choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251)
Providing a choice of five types allows the administrator to use any one for the IP Phone. This is beneficial when a type may already be in use for a different application. Pick only one type.
**Length (1 octet)**
Variable – dependent on message content
**Data (variable number octets)**
ASCII based with a format of: "VLAN-A:XXX+YYY+ZZZ." where
VLAN-A: uniquely identifies this as the Nortel DHCP VLAN Discovery.
Additionally, -A signifies the version of this specification. Future enhancements could use -B, for example.
XXX, YYY, and ZZZ are ASCII-encoded decimal numbers with a range of 0 to 4095. The number is used to identify the VLAN IDs. A maximum of 10 VLAN IDs can be configured in the current version.
String “none” or “NONE” means no VLAN tag.
ASCII plus sign (+) or comma (,) is used to separate fields.
ASCII period (.) is used to signal end of structure.

When it receives the DHCP OFFER with a list of suggested VLANs, the IP Phone accepts the offered IP address (presumably a temporary address) and proceeds with the DHCP negotiations (a DHCP Request sent to the server for the assigned address and a DHCP ACK sent by the server to finalize the assignment).

The IP Phone releases the temporary IP address by sending a DHCP Release to the server. Note that all packets sent by the IP Phone to this point are untagged. The phone then chooses the first VLAN ID included in the previous DHCP OFFER. After releasing the address, the phone now restarts the discovery process, broadcasting another DHCP Discover message, but this time tagging all packets with the selected VLAN ID. The DHCP OFFER, DHCP Request and DHCP ACK continue as before, but now all packets are tagged with a specific VLAN ID.

If the VLAN ID that was selected (first in the list) is not the voice VLAN configured on the edge switch, or if the DHCP server does not have an available address for the requested VLAN and does not respond to the DHCP Discover, the IP Phone resends the Discover broadcast, retrying up to four times and doubling its wait time between each successive attempt (approximately 4, 8, 15, 30 seconds). If the phone still does not receive a response, the IP Phone gives up on that VLAN and broadcasts a new DHCP Discover using the next VLAN from the list. As mentioned previously, up to 10 VLAN IDs can be included in the DHCP OFFER.

Upon success, the IP Phone is configured with the proper IP address and VLAN information for that specific voice VLAN.

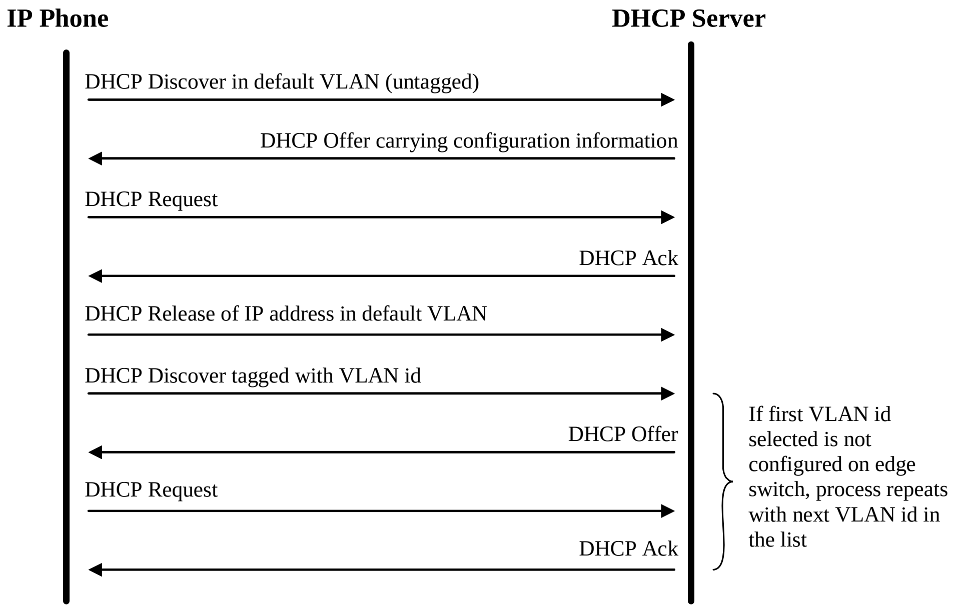

IP Phone
DHCP Server
DHCP Discover in default VLAN (untagged)
DHCP Offer carrying configuration information
DHCP Request
DHCP Ack
DHCP Release of IP address in default VLAN
DHCP Discover tagged with VLAN id
DHCP Offer
DHCP Request
DHCP Ack
If first VLAN id selected is not configured on edge switch, process repeats with next VLAN id in the list

**Figure 7: DHCP packet flow for Auto VLAN Discovery**

### 5.2.7 Design recommendation

Enable the following phone-specific features:

- Full DHCP configuration
- Auto VLAN Discovery
- GARP (Gratuitous ARP) protection – prevents GARP denial of service attack on phone
- VLAN filter (if using VLAN functionality – filters traffic by 802.1Q tag)

## 5.3 IP Phone functionality

Several Nortel IP Phones come equipped with a three-port Ethernet Switch built into the set. The IP Phone 2001 does not have three-port switch functionality, and older versions of the IP Phone 2004 use an external three-port switch. The Phase II and 1100 series phones with the integrated three-port switches also support IEEE 802.3af Power over Ethernet (see Table 3 for details).

The ports on the IP Phone switch are used as follows:

- Ethernet connection for workstation/PC (PC port)
- Ethernet connection for phone (built in, no external port)
- Ethernet connection to the LAN (LAN port)

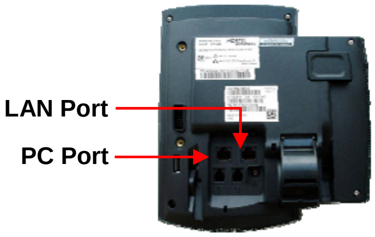


**Figure 8: Rear view of IP Phone (1140E)**

The functionality of the integrated three-port switch differs depending on the IP Phone. The following table indicates the three-port switch functionality and average PSE (power source equipment) power required for each of the Nortel IP Phones.

| IP Phone | Supported Speeds | VLAN Aware | Average Power (PSE) |
|---|---|---|---|
| **Phase 0 Phones** | | | |
| i2004 phone | N/A | N/A | 4.8 watts |
| i2004 phone w/ external 3 port 10/100 switch | 10/100 | No | 13.2 watts |
| **Phase I Phones** | | | |
| i2002 phone w/ integrated 3 port 10/100 switch | 10/100 | No | 4.8 watts |
| i2004 phone w/ integrated 3 port 10/100 switch | 10/100 | No | 4.8 watts |
| **Phase II Phones** | | | |
| IP Phone 2001 w/ integrated 3 port 10/100 switch | 10/100 | Yes | 4.8 watts |
| IP Phone 2002 w/ integrated 3 port 10/100 switch | 10/100 | Yes | 4.8 watts |
| IP Phone 2004 w/ integrated 3 port 10/100 switch | 10/100 | Yes | 5.4 watts |
| IP Phone 2007 w/ integrated 3 port 10/100 switch | 10/100 | Yes | 9.6 watts |
| **1100 Series** | | | |
| 1110 phone w/ integrated 3 port 10/100 switch | 10/100 | Yes | 4.8 watts |
| 1120E phone w/ integrated 3 port 10/100/1000 switch (running 100 Mbps) | 10/100/1000 | Yes | 8.4 watts |
| 1120E phone w/ integrated 3 port 10/100/1000 switch (running 1000Mbps) | 10/100/1000 | Yes | 10.8 watts |
| 1140E phone w/ integrated 3 port 10/100/1000 switch (running 100 Mbps) | 10/100/1000 | Yes | 8.4 watts |
| 1140E phone w/ integrated 3 port 10/100/1000 switch (running 1000Mbps) | 10/100/1000 | Yes | 10.8 watts |
| IP Audio Conference Phone 2033 | N/A | N/A | N/A |

**Table 3: IP Phone three-port switch functionality**

### 5.3.1 Packet forwarding – three-port switch

Packet forwarding of the three-port switch differs between the switches that are VLAN aware and those that are not VLAN aware.

- VLAN aware switch

  Enhanced 802.1p and 802.1Q support on the IP Phone switch improves voice quality by taking advantage of the VLAN filtering available on this hardware. This switch also has two TX (out) queues on each port – High Priority Queue (HPQ) and Low Priority Queue (LPQ).

  If 802.1Q VLAN tagging and VLAN filter are enabled on the IP Phone three-port switch, frames received from the LAN port are filtered first by the VLAN tag and then the MAC address to determine where to forward the packet. Packets addressed to the phone are forwarded to the phone port. Packets addressed to the PC are forwarded to the PC port. Voice traffic is always queued to the HPQ, thereby providing a higher quality of service.

  Network broadcast traffic is forwarded to both the phone port and PC port, so both devices see this traffic. Broadcast traffic does not adversely affect the function of the IP Phone.

- Legacy switch (not VLAN aware)

  Packets arriving on the three-port switch from the LAN port are filtered by MAC address to determine where to forward the packet. Packets addressed to the MAC of the phone are forwarded to the phone port, while all other packets are forwarded to the PC port. As discussed previously, broadcast traffic is forwarded to both ports. Traffic leaving the three-port switch out of the LAN port (heading for the network) passes all packets unaltered.

### 5.3.2 Speed and duplex

The three-port switches in IP Phones support 10/100 Mbps or 10/100/1000 Mbps connectivity. By default, the IP Phones have autonegotiation enabled. It is absolutely critical to ensure that there are no duplex mismatch problems between the IP Phone and the edge switch. By setting both ends to autonegotiation, the possibility of a speed/duplex mismatch is virtually eliminated. If the edge switch is not configured for autonegotiation, you must configure the phone to match the exact configuration (speed and duplex) of the edge switch.

### 5.3.3 Power over Ethernet (PoE)

The use of Power over Ethernet (PoE) has become increasingly popular over the past few years and is now standardized by the IEEE with 802.3af. Many end devices, such as wireless access points, security cameras, VoIP phones, and security card readers, now support Power over Ethernet. The 802.3af standard specifies a resistive discovery mechanism, while legacy-based (prestandard) PoE devices use a capacitive discovery mechanism. Power, up to 15.4 watts per device, can be provided over the used pairs or unused pairs in a UTP copper cable. The Nortel implementation of 802.3af utilizes the used pairs for PoE. The standard also defines different classes of detection. Table 4 defines the different classes of PoE along with the wattages at PSE (Power Source Equipment) and PD (Powered Device).

| Class | Usage | Maximum power levels at output of PSE | Maximum power levels at input of PD |
|---|---|---|---|
| 0 | Default | 15.4 watts | 0.44-12.95 watts |
| 1 | Optional | 4.0 watts | 0.44-3.84 watts |
| 2 | Optional | 7.0 watts | 3.84-6.49 watts |
| 3 | Optional | 15.4 watts | 6.49-12.95 watts |
| 4 | Reserved future use | Treat as Class 0 | Reserved future use |

**Table 4: Power classifications – PoE**

Phase 0 and Phase I IP Phones do not have the integrated hardware to support PoE, but require an external power splitter for this functionality, as shown in the following figure.

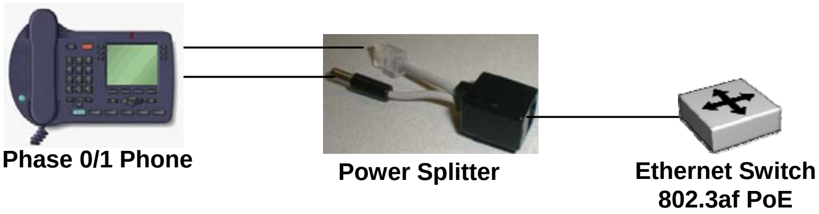


**Figure 9: PoE with power splitter**

Nortel originally provided a splitter that worked with the ES 460 in legacy mode (Nortel part number DY4311015). This splitter will not work with any Nortel Ethernet Switch in 802.3af mode. A new splitter (DY4311046) is required to power the IP Phones and is supported on all Nortel Ethernet PoE-capable switches configured for 802.3af (ES 460, ERS 5520, ERS 8300). The ES 460 supports both legacy and 802.3af PoE, while the ERS 5520 and ERS 8300 support only 802.3af PoE.  The following table lists the splitters and which switches are supported.

| Ethernet Switch | DY4311015 Splitter (Legacy power only) | DY4311046 Splitter (802.3af power only) |
|---|---|---|
| ES 460 | Yes | Yes |
| ERS 5520 | No | Yes |
| ERS 8300 | No | Yes |

**Table 5: Power splitter support**

Phase II phones and the 1100 series phones provide integrated PoE support, which is 802.3af compliant. No power splitter is required for these phones when connecting to the PoE edge switch.

## 5.3.4 Ethernet edge switch configuration options

The configuration and deployment of the IP Telephony Clients will dictate the configuration required on the Ethernet edge switches in the closets. There are several configuration options for the Ethernet edge switches to support IP Telephony. This section covers the basic Ethernet/VLAN configurations for the most common deployment scenarios, while a later section details Quality of Service configuration options.

Scenario 1: IP Phone/PC sharing Ethernet port – only voice traffic tagged

The Ethernet Switch will have two VLANs configured on the port; however, the port will not be configured as a trunk port, but as an access port. The data VLAN will be the untagged member and the PVID (port VLAN identifier) for the port, while the voice VLAN will also be a member of the port. Configure the Ethernet port to Untag PVID only. This ensures that the data traffic headed to the PC will be untagged, while the voice traffic headed to the phone will be tagged.

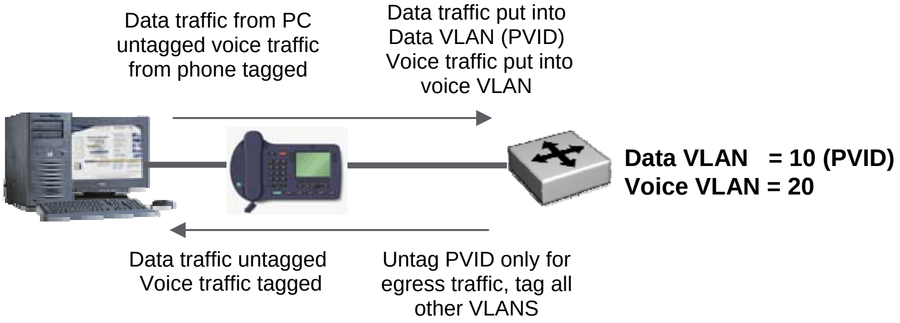


**Figure 10: Ethernet Switch configuration – tag voice traffic only**

Ingress traffic from the three-port switch in the phone to the Ethernet Switch will have tagged traffic from the phone (voice traffic, tagged with the voice VLAN). This traffic will be put into the voice VLAN on the switch, while the untagged traffic from the phone (data traffic from the PC) will be put into the untagged PVID VLAN for that port.

Egress traffic from the Ethernet Switch will have the data traffic (from the PVID VLAN) untagged headed for the PC, while the voice traffic will be tagged with the Voice VLAN headed for the phone. The three-port switch in the phone will send the untagged data traffic to the PC and will send the tagged voice traffic (after stripping the tag) to the phone.

Scenario 2: IP Phone/PC sharing Ethernet port – voice and data traffic tagged

The Ethernet Switch will have two VLANs configured on the port and the port will be configured as a trunk port. Both the data VLAN and the voice VLAN will be a tagged member of the port. Configure the Ethernet port to Tag All for egress traffic. This ensures that both the data traffic headed to the PC and the voice traffic headed to the phone will be tagged. In this case, because the Ethernet switch port is configured as a Trunk port, the PVID on the port does not come into play.

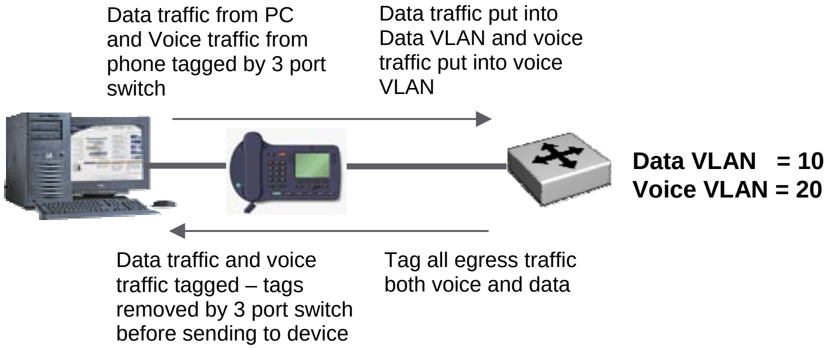

Data traffic from PC and Voice traffic from phone tagged by 3 port switch
Data traffic put into Data VLAN and voice traffic put into voice VLAN
Data VLAN = 10
Voice VLAN = 20
Data traffic and voice traffic tagged – tags removed by 3 port switch before sending to device
Tag all egress traffic both voice and data

**Figure 11: Ethernet Switch configuration – tag voice and data traffic**

Ingress traffic from the three-port switch in the phone to the Ethernet Switch will have all tagged traffic from the three port switch in the phone – voice traffic tagged with the voice VLAN, and data traffic tagged with the data VLAN. The traffic will be put into the proper VLAN on the Ethernet Switch by means of the VLAN tag.

Egress traffic from the Ethernet Switch will have all traffic tagged headed for the three-port switch in the phone. The data traffic headed to the PC will be tagged with the data VLAN, while the voice traffic will be tagged with the Voice VLAN. The three-port switch in the phone will strip the tag before sending the traffic to the appropriate device (phone or PC).

Scenario 3: IP Phone on its own Ethernet port – traffic is untagged

The Ethernet Switch will have one VLAN configured on the port and the port will be configured as an access port. The only VLAN configured here is the voice VLAN, which will be the PVID for the port. Configure the Ethernet port to Untag All for egress traffic. This ensures that the voice traffic headed to the phone will be untagged.

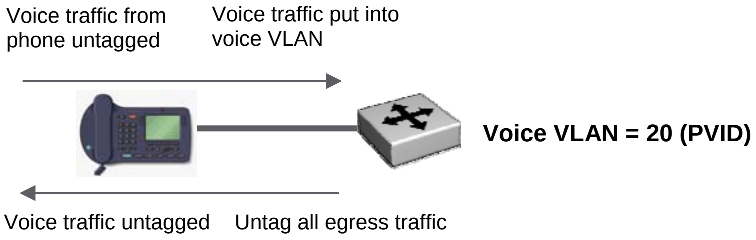


**Figure 12: Ethernet Switch configuration – no tagged traffic**

Ingress traffic from the three-port switch in the phone to the Ethernet Switch will have all untagged traffic. Because there is only voice traffic and one VLAN, all traffic will go into that VLAN on the Ethernet Switch.

Egress traffic from the Ethernet Switch will have all traffic untagged headed for the three-port switch in the phone.

### 5.3.5 Auto Detection Auto Configuration (ADAC)

A feature available on the Ethernet Switch 460/470 Release 3.6 and above provides for the auto detection and configuration of the switch port to support IP Telephony. This feature will be supported in Release 5.0 for the ERS 5500 series. When a Nortel IP Phone is connected to a switch, the switch performs the automatic detection and configuration of the predefined voice VLAN and appropriate QoS parameters on that switch port.

When a Nortel IP Phone is connected to a switch and is powered on, the switch automatically detects the IP Phone and begins the auto configuration of the port. Auto detection of the Nortel IP Phones is performed based on MAC address. When the feature is enabled on a port, the device checks all MAC addresses of received packets on the port. If a received MAC address falls within the range of known Nortel IP Phone MAC addresses, the auto detection feature determines that the specified port is connected to a Nortel IP Phone. The ADAC port participation can be set independently by enabling or disabling ADAC for particular ports on a given switch.

ADAC can be configured to apply settings depending on how the Nortel IP Phones are configured to send traffic (tagged or untagged) and depending on the desired complexity level of the auto configuration. The ADAC QoS configurations are applied to traffic coming from the IP Phones, traffic coming from the Call Server port, and traffic coming from the Uplink port. There are three defined ADAC operating modes:

- Untagged-Frames-Basic
  - The IP Phones must be configured to send untagged frames.
  - There is minimal VLAN configuration (tagging must be set to untagged for telephony ports).
  - QoS configuration is applied.
  - Auto configuration occurs when only Nortel IP Phones are detected on a port. You cannot connect a device that is not a Nortel IP Phone to the same port.
- Untagged-Frames-Advanced
  - The IP Phones must be configured to send untagged frames.
  - Both VLAN and QoS configuration are applied.
  - Auto configuration occurs when only Nortel IP Phones are detected on a port. You cannot connect a device that is not a Nortel IP Phone to the same port.
- Tagged-Frames
  - The IP Phone must be configured to send tagged frames with the ID of the voice VLAN.
  - Both VLAN and QoS configuration are applied.
  - Auto configuration occurs when at least one Nortel IP Phone is detected on a port. Other devices that are not Nortel IP Phones can be connected to the same port (for example, by connecting the port to a hub or switch).

Notes

In the ES 460/470 release 3.6, ADAC only supports the MAC address range belonging to the IP Phone 2004 phase II sets.

Presently, when you configure ADAC on an ES 460/470 with operating mode of Tagged, ADAC will configure the switch port as *tagPvidOnly*. Hence, the Nortel IP Phone set cannot be configured for Auto Configuration mode. The reason is that the initial DHCP request from the Nortel IP Phone set will be forwarded untagged, and if the ADAC-enabled port is set for tagging only, the initial DHCP packet will be dropped.

Moving forward, these limitations will be resolved in the 3.7 release for ES 460/470 and added to the 5.0 release for the ERS 5500. With these releases there will be option in ADAC to configure the port for *untagPvidonly* to allow Nortel IP Phones to be configured with the Auto Configuration mode. The capability to add new MAC address ranges will also be added to support additional IP Phone sets.

### 5.3.6 IP Softphone 2050

The IP Softphone 2050 is a Windows-based application that provides voice services for PCs. Designed to work with IP-based phone systems, the IP Softphone 2050 provides Voice over IP services using a telephony server and an enterprise LAN. The IP Softphone 2050 operates on PCs running Windows 98, Windows 98 SE, Windows 2000 Professional, Windows XP Pro, and Windows XP Home.

Because the Softphone is an application running on a PC rather than a traditional phone device, there are different design considerations to take into account before deploying this solution, namely VLANs and QoS.

VLANs

The Nortel recommendation for the deployment of IP Telephony is to create separate VLANs for voice and data traffic. An exception to this recommendation is when using the IP Softphone 2050. Because the Softphone is an application running on the PC, it is impossible to segregate this traffic into a separate VLAN. The voice traffic from the Softphone travels on the same VLAN as the normal data traffic from the PC. Due to this fact, the implementation of QoS becomes even more critical to ensure a consistent and acceptable Quality of Experience for the end user.

QoS

A combination of codec selection, jitter buffer, and packet time, and the use of the network DiffServ Code Point (DSCP) all contribute to the end-to-end QoS. However, the IP Softphone 2050 is an application within the context of the PC operating system (OS), so the OS has an effect on the end-to-end QoS for the IP Softphone 2050. The DSP functionality (such as codec packetization) implemented in DSP hardware on the IP Softphone 2050 and Voice Gateway Media Card runs as part of the application code on the PC CPU. If the CPU is busy with other tasks, voice quality can be negatively affected. You can adjust the number of buffers used for audio data between the application and PC audio hardware device driver from the Configuration Tool. Using fewer buffers reduces the audio path delay but increases the chances of dropouts and choppy speech, depending on the speed and utilization of the PC CPU.

The IP Softphone 2050 uses DSCP settings assigned by the Terminal Proxy Server (TPS). The IP Softphone 2050 supports DSCP on Window 98, Windows 98 SE, Windows 2000 Professional, and Windows XP. The IP Softphone 2050 can also use 802.1p (priority) settings assigned by the TPS. The IP Softphone 2050 supports 802.1p on Windows 2000 Professional and Windows XP. This requires the installation of Nortel IP Softphone 2050 QoS Service. The DSCP values assigned from TPS 802.1Q operation can be enabled or disabled from the QoS tab in the Configuration Utility. The service can be installed from the Softphone 2050 CD-ROM. If you install the IP Softphone 2050 with Administrator access, then this service is installed automatically.

Note that the IP Softphone 2050 does not support VLANs (the VLAN ID in 802.1Q).

Not all operating systems allow assignment of all QoS settings. The Configuration Utility allows settings only applicable to specific operating systems to be assigned. The only possible assignments in Windows 2000 Professional are 802.1Q and DiffServ. Note that Administrator privileges are required to set 802.1Q and DiffServ and a prerequisite for this is installation of the QoS Packet Scheduler within the OS.

## 5.4 Quality of Service

Many considerations must be evaluated before you install IP Telephony on a converged infrastructure. Simply deploying IP Telephony Clients on a best-effort IP network will not provide the desired results for users. Because IP networks are by nature best effort – meaning that all traffic is treated equally – there will exist differing amounts of delay, jitter, and packet loss. These situations will have an adverse effect on delay-sensitive converged applications such as IP Telephony. This environment will produce undesirable characteristics such as clipping, speech breakup, and echo.

### 5.4.1 QoS considerations

In order to accommodate IP Telephony, the converged infrastructure must employ Quality of Service (QoS). Many networks have more than sufficient bandwidth to accommodate this type of traffic and many people believe QoS is not an absolute requirement. Even though there is bandwidth available, QoS guarantees a consistent delay and jitter (which are critical to provide high quality Voice over IP) – this becomes important in times of network congestion. There are different mechanisms to deploy QoS, and this document discusses them at a high level. For a detailed description of QoS for VoIP networks, refer to Appendix A, the Nortel whitepaper “QoS Recommendations for VoIP” by Ralph Santitoro.

### 5.4.2 Differentiated Services and 802.1p

Differentiated Services (DiffServ) is the industry and Nortel standard for the implementation of Quality of Service. DiffServ provides QoS on a per-hop behavior of the Ethernet Switches by marking the header of individual packets with a DiffServ Code Point. This DSCP then indicates to the Ethernet Switch the priority of each packet and into which queue the packet is to be placed. Note that the network infrastructure must support QoS end to end. Without a full end-to-end deployment, QoS cannot provide the necessary actions to ensure priority through every hop of the network. By default, the edge switches remark all QoS bits to zero and do not honor any markings.

Not all Ethernet Switch equipment may be DiffServ capable. In that case, 802.1p priority can be used to provide QoS. The 802.1p priority is part of the 802.1Q VLAN tag header in the IP packet. This provides a Layer 2 user priority on a physical Ethernet port basis – available priorities range from 0 to 7, with 7 being the highest. Ethernet Switches that support DiffServ can map 802.1p into DiffServ and DiffServ into 802.1p and therefore can still support a true end-to-end QoS implementation.

The Nortel Ethernet PoE switches (ES 460, ES 470, ERS 5520, ERS 8300) all support both Diffserv and 802.1p. These switches have the capability to honor, re-mark, or ignore the marking of the packets.

### 5.4.3 QoS strategy

There are various strategies for deploying QoS throughout the infrastructure, and Nortel provides several tools to streamline the implementation. The Ethernet Switches have the ability to either mark or honor the DSCP within each Ethernet packet. Many end devices have the ability to set their own DSCP and thus set their own priority across the network. For example, the Nortel IP Phones can set their DSCP to Expedited Forwarding, which maps into the Premium Service Class queue. The IP Phones can also mark their 802.1p priority (priority level of 6) if 802.1Q tagging is enabled on the phone. This priority also maps into the Premium Service Class queue.

Take care when simply honoring the markings from end stations. Windows XP can also mark DSCP, and therefore savvy users could prioritize their traffic on the network that honors the DSCP marking. It is a better practice for the edge switch to re-mark the DSCP to one that is controlled by the network administrator. You can accomplish this by using VLAN prioritization, which marks all packets in a specific VLAN with the same priority (prioritizing the voice VLAN), or by using the filtering capabilities of the Ethernet Switches to mark packets individually based on filtering criteria established by the network administrator (an application that uses a specific TCP port number can be given priority).

To assist in qualifying these types of applications and the associated QoS levels, Nortel created a QoS matrix and standardized Nortel Service Classes across all platforms. This matrix is intended as a guideline for the implementation of QoS.

| Nortel Service Class | Target Applications and Services | Tolerance to: | | |
|---|---|---|---|---|
| | | Loss | Delay | Jitter |
| Critical | Super user Telnet, critical heartbeats between routers/switches | Very Low | Very Low | N/A |
| Network | ICMP, OSPF, BGP, RIP, ISIS, COPS, RSVP<br>DNS, DHCP, BootP, high priority OAM | Low | Low | N/A |
| Premium | VoIP, T.38 Fax over IP, Lawful Intercept, CES<br>Real-time VPN service (CIR > 0, EIR = 0) | Very Low | Very Low | Very Low |
| Platinum | Video Conferencing, Interactive Gaming<br>Real-time VPN service (CIR > 0, EIR > 0) | Low | Low | Low |
| Gold | Streaming audio, video on demand<br>Broadcast TV, video surveillance | Low-Med | Med-High | High |
| Silver | SNA terminal to host transactions<br>Credit card transactions, wire transfers<br>Instant Messaging<br>Low Loss/Delay Data VPN service (CIR > 0, EIR > 0) | Low | Low-Med | N/A |
| Bronze | E-mail<br>Non-time-critical OAM&P | Low | Med-High | N/A |
| Standard | Best effort applications<br>Best effort VPN (CIR >= 0, EIR > 0) | Med | High | N/A |

**Table 6: Quality of Service matrix**

The implementation of QoS on a converged infrastructure varies greatly from network to network. There is no one correct solution or simple cookbook for deploying QoS. It is best to understand the overall network and the applications that are deemed critical in order to design a QoS strategy.

### 5.4.4 QoS deployment

After documenting the QoS strategy, the configuration and deployment of QoS is straightforward. It is imperative that QoS is deployed end-to-end throughout the network in order to provide an acceptable Quality of Experience for the users. If there are areas of the network that are not configured for QoS, it effectively returns the network to a best effort environment and defeats the overall purpose of QoS. Nortel provides several options for configuration and deployment of QoS throughout the network infrastructure:

- Manual configuration on a switch by switch basis – network administrators can implement QoS on a per switch basis using a web GUI (graphical user interface) or through CLI (command line interface).
- Centralized configuration can be accomplished using Enterprise Policy Manager. This network management tool can create QoS and security policies that can be quickly and easily deployed to the Ethernet Switches throughout the network.

Each of the Nortel Ethernet switching products has substantial documentation about the actual configuration steps to deploy QoS – refer to these documents, which can be found on the support site of www.nortel.com, for this information.

### 5.4.5 Design recommendation

Nortel recommends the implementation of a consistent QoS policy across the network, ensuring an acceptable IP Telephony Quality of Experience for the end user. The following points highlight this recommendation:

- Implement Differentiated Services for QoS.
- Create a QoS strategy based on the application requirements of the network. IP Telephony should be regarded as a premium service.
- Be aware that simply honoring all Diffserv markings can result in unexpected network performance if other devices (such as PCs) are marking their traffic into a premium service class – to avoid this situation, do not honor markings from the edge, but instead create VLAN prioritization or filters on the edge switches to identify voice traffic and mark its priority accordingly.
- Utilize Enterprise Policy Manager to create and deploy consistent QoS across the network infrastructure.

# 6. Authentication options

Several design options are available for IP Telephony in regard to authentication. Requirements for authentication can be for the PC only, the phone only, or any combination thereof. The following sections describe the common scenarios, and Table 7 on page 33 highlights the various capabilities of the Ethernet Switches to accommodate the authentication requirements.

## 6.1 MAC security

MAC address filtering can provide a basic level of authentication for the device connected to the Ethernet Switch port in the closet. All Ethernet Switches and Ethernet Routing Switches support local MAC filtering in which the valid MAC addresses must be entered into the edge switch. In this manner, the network administrator can lock down to which ports which MAC addresses are allowed. This is an administrative function, and if MAC addresses change due to a new device being added to the network, administrative intervention is required on that particular edge switch to add the MAC.

To make this option scale better, the Centralized MAC Authentication feature has been introduced to several of the Nortel Ethernet Switches. This feature allows the valid MAC addresses to be entered in a centralized RADIUS server. Each of the edge switches points to this server to authenticate their local MAC addresses. This enables valid MAC addresses to move throughout the infrastructure without administrative intervention.

With centralized MAC authentication, RADIUS VLAN assignment is not supported. In this case, the VLAN must already be provisioned on the Ethernet Switch port and cannot be altered through the authentication process.

## 6.2 802.1x Extensible Authentication Protocol (EAP)

IEEE 802.1x provides a transport for the authentication of end devices. Defined within 802.1x are the following roles:

- Supplicant – End device, such as an IP Phone, that requires access to the network.
- Authenticator – The network entry point to which the supplicant physically connects (typically a Layer 2/3 switch). The authenticator acts as the proxy between the supplicant and the authentication server. The authenticator controls access to the network based on the authentication status of the supplicant.
- Authentication Server – Provides authentication of the supplicant.

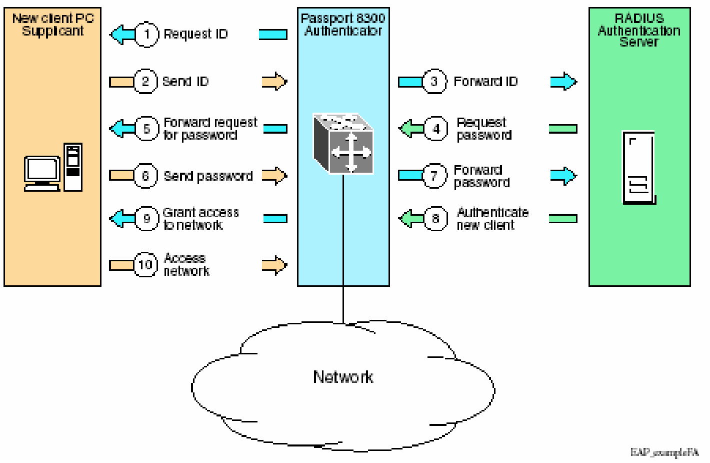


**Figure 13: EAP authentication packet flow**

Extensible Authentication Protocol (EAP) supports multiple authentication methods – MD5, TLS, TTLS, PEAP – that use the underlying 802.1x transport. The supplicant and authentication server must be using the same EAP method in order to successfully authenticate the end device.

802.1x authentication has been available for quite some time on PCs and workstations. For example, it is built into the Windows XP operating system and needs simply to be enabled for use. On older legacy operating systems you may need to install a third-party application in order to support authentication. In most cases, this type of authentication is used to authenticate the user of the device and not necessarily the device itself.

Nortel IP Phones now support 802.1x authentication. This authentication is designed to authenticate the device (the IP Phone set) and not the user of the device. The Nortel IP Phones use EAP-MD5 for authentication of the device. A device ID and password must be validated by the RADIUS server before the IP Phone is permitted on the network. The device ID and password must be provisioned on the IP Phone and corresponding entries must be present in the RADIUS server. This feature is intended to prevent rogue devices from attaching to the network. Theoretically, the phones could be programmed with all the same device ID and password, thus requiring only one entry in the RADIUS server. On the other hand, every single phone could be programmed with a unique device ID and password if so desired. This would require an entry in the RADIUS server for every single phone. The more device IDs, theoretically the more secure the deployment, but at the cost of additional administration. It is a tradeoff between security and administrative overhead.

## 6.3 Guest VLAN

A Guest VLAN provides restricted access to the network for those devices that are not able to authenticate. The most common scenario for use of the Guest VLAN feature is to accommodate guest users on the network. Registered users are able to authenticate through EAP and have full network access, while guest users can get on the network without EAP authentication but may have their access restricted to certain areas of the network or just the Internet. Guest access is determined by the network administrator and is based on the filters and Access Control Lists (ACL) set up on the network equipment. Rules for the Guest VLAN are as follows:

- Must be a port-based VLAN
- Is configured per switch or stack
- Access to the Guest VLAN is configurable per port
- Affects ports in EAP-Auto state
- Does not affect ports in force-authorized or force-unauthorized

## 6.4 Single Host Single Authentication (SHSA)

For an EAP-enabled Ethernet Switch port with SHSA, at any time, only one MAC address is authenticated on that port, which is assigned to only one port-based VLAN. Only a particular device or a user who completes EAP negotiations on the port is allowed access to that port to pass traffic. Two or more devices are not allowed to share the same Ethernet switch port. The RADIUS server can also pass back VLAN information and 802.1p port priority to the Ethernet edge switch (Authenticator). The VLAN must exist on the Ethernet edge switch in order to dynamically move the port into that specific VLAN. Note that the dynamic VLAN assignment is not stored in NVRAM.

To enable dynamic VLAN assignment and 802.1p port priority, the following return list attributes must be configured in the RADIUS server:

- VLAN membership attributes
    - Tunnel-Type: value 13, Tunnel-Type-VLAN
    - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
    - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes
    - Vendor ID: value 562, Nortel vendor ID
    - Attribute Number: value 1, Port Priority
    - Attribute Value: value 0 to 7 (this value is used to indicate the port priority value assigned to the specified user)

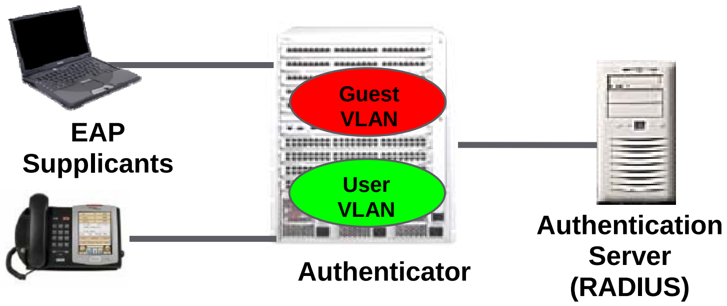


**Figure 14: Single Host Single Authentication**

In the example shown in Figure 14, the ports on the Ethernet Switch (Authenticator) are placed in the Guest VLAN. Upon a successful EAP authentication, the ports are dynamically assigned to the correct VLAN (as passed back from the RADIUS server). Those devices that are unable to successfully authenticate are left in the Guest VLAN. Network access and privileges for the Guest VLAN are determined by the network administrator.

## 6.5 Multiple Host Single Authentication (MHSA)

The MHSA feature accommodates multiple devices sharing a single Ethernet Switch port in the closet (PC and IP Phone) while still allowing EAP authentication of one of those devices. For an EAP-enabled port with MHSA, a finite number of users or devices with unique MAC addresses are allowed access to a port. In this case, both a single EAP user and multiple non-EAP users can access the port. A single EAP user has to complete EAP authentication to allow traffic from the corresponding MAC address. The other non-EAP users must have their MACs preconfigured on the switch port or use centralized MAC authentication for access to the port. Dynamic VLAN assignment is not supported for non-EAP authenticated devices. The Guest VLAN feature is not supported with MHSA.

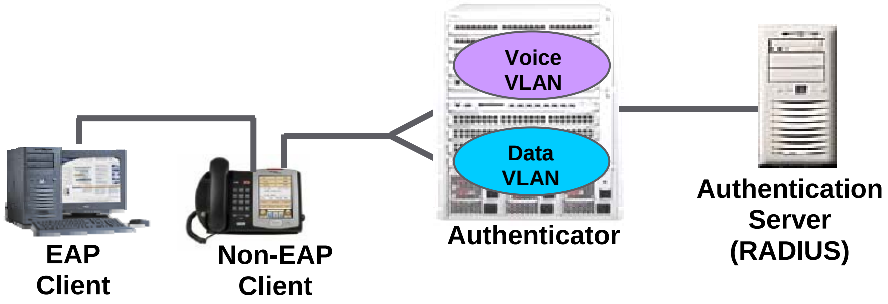


**Figure 15: Multiple Host Single Authentication**

In the example shown in Figure 15, the PC would be authenticated through EAP and the VLAN for that PC could be dynamically assigned from the RADIUS server (VLAN must already exist on the Ethernet Switch – Authenticator). The non-EAP client would be authenticated through a MAC address that was configured on the switch locally or in the RADIUS server if centralized MAC authentication was enabled. The VLAN cannot be dynamically assigned, so the port must be a member of the correct VLAN (voice VLAN in this example). Refer to the section about Ethernet edge switch configuration for details about the various options for 802.1Q tagging on the three-port phone switch and Ethernet edge switch.

## 6.6 Multiple Host Multiple Authentication (MHMA)

For an EAP-enabled port with MHMA, a finite number of users or devices with unique MAC addresses are allowed access to a port. Each user has to complete EAP authentication so as to enable the port to allow traffic from the corresponding MAC address. Only traffic from the authorized hosts is allowed on that port.

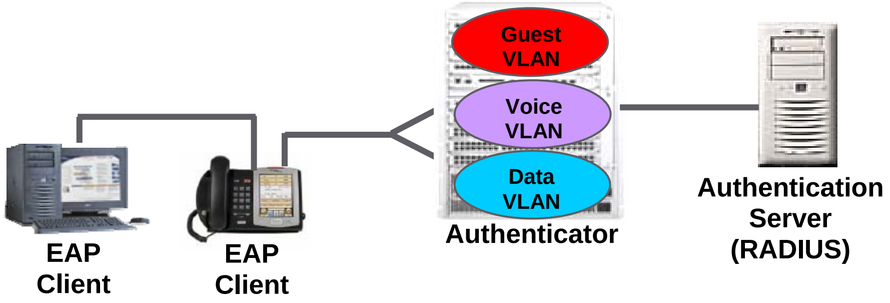


**Figure 16: Multiple Host Multiple Authentication**

In the example shown in Figure 16, both devices are authenticated through EAP. Dynamic VLAN assignment is not supported in MHMA mode, so both VLANs would need to be configured on the Ethernet Switch port.

The following table indicates the various authentication features and corresponding support on the Nortel Ethernet Switches.

**Nortel Supported LAN Switching Security Features**

| **Authentication Features** | **ES 460/470** | **ERS 5500** | **ERS 8300** |
|---|---|---|---|
| Local MAC Security | Yes | Yes | Yes |
| Centralized MAC Security | POR | POR | Yes |
| Guest VLAN | Yes | Yes | Yes |
| Single Host Single Authentication (SHSA) - 802.1x EAP | Yes | Yes | Yes |
| Multiple Host Single Authentication (MHSA) - 802.1x EAP | POR | POR | Yes |
| Multiple Host Multiple Authentication (MHMA) - 802.1x EAP | Yes | Yes | Yes |
| SHSA with Guest VLAN | Yes | Yes | Yes |
| MHSA with Guest VLAN | POI | POI | POI |
| MHMA with Guest VLAN | POI | Yes | POI |
| **Tagged/Untagged** | | | |
| Per VLAN Egress Tagging | Yes | Yes | Yes |
| Tagged and untagged per port | Yes | Yes | Yes |
| Tagging with EAP | Yes | Yes | Yes |

POR = Plan of Record – feature set and timeline established for specific release
POI = Plan of Intent – feature set and timeline subject to change

**Table 7: Nortel supported LAN switching security features**

# 7. Futures

Nortel is developing several key features and functionalities that will enhance the deployment of IP Telephony Clients in regard to configuration and security.

The IEEE 802.1AB standard will provide configuration information from the IP Phones and Ethernet Switches to simplify the deployment in regard to management and configuration. Support for 802.1AB on Nortel IP Phones and Nortel ES/ERS products is expected during 2006.

From a security perspective, the Nortel Secure Network Access (NSNA) architecture provides consistent security and policy enforcement across the network, whether wired, wireless, local, or remote.

## 7.1 802.1AB

The IEEE 802.1AB standard defines the Link Layer Discovery Protocol (LLDP), which is a neighbor discovery protocol. It defines a standard method for Ethernet network devices such as switches, routers, and IP Phones to advertise information about themselves to other nodes on the network and store the information they discover.

The 802.1AB standard specifies the necessary protocol (LLDP) to:

- Facilitate multivendor interoperability and the use of standard network tools to discover and make available physical topology information for network management
- Make it possible for network management to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers
- Provide information to assign network management in making resource or configuration changes that correct configuration inconsistencies or malfunctions

The LLDP lets network management systems accurately discover and model physical network topologies. As LLDP devices transmit and receive advertisements, the devices will store information they discover about their neighbors. Details such as device configuration, device capabilities, and device identification can be advertised using this protocol.

It is expected that LLDP will be a useful management tool – particularly for heterogeneous networks – by providing accurate network mapping, inventory data and network troubleshooting information. Because LANs currently support a high density of heterogeneous devices with multiple applications, a harmonious operation among these devices requires correct configuration of their supporting protocols. LLDP enables LAN devices to inform each other about their configurations.

Providing LLDP support in the IP Phone allows the exchange of information between the phone and the Layer 2/Layer 3 Ethernet edge switch. This allows the devices to exchange capabilities and for a network administrator to have a more complete view of the network infrastructure. In the case of convergence, this protocol can be used to:

- Discover duplex mismatches between an IP Phone and the Ethernet edge switch to which it connects
- Help identify Nortel IP Phones and assign some specific QoS, VLAN, or any other specific configuration parameters
- Help locate an IP Phone (e911)

## 7.2 Nortel Secure Network Access

Nortel Secure Network Access (NSNA) is the endpoint security and policy compliance solution designed to inspect, assess, ensure compliance to policy, and remediate at the network endpoint source, prior to network access. The NSNA solution dramatically simplifies the complexity of enterprise network access architectures with a ubiquitous, open solution guaranteeing endpoint security with seamless device quarantine and containment, remediation and repair for LAN users and remote users (IPsec/SSL), with both fixed and mobile connectivity devices. The Nortel Secure Network Access solution delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, user identity and session context.

Running NSNA with Nortel Ethernet Switches enables a highly integrated endpoint security solution from a management and ease of use perspective. With NSNA, the enterprise can define, deploy, and enforce a robust and consistent security policy across its varied network segments with trusted role-based access enablement premised on user identity and session context. NSNA can ensure that devices meet the corporate security policy before they are granted network access, and reduce the risk of virus infections or misconfigured systems being added to the network. Verifying compliance and blocking connections from non-compliant systems can guarantee 100 percent compliance with corporate policy 100 percent of the time.

Nortel IP Phones have the same checks in place as the Ethernet Routing Switches. In dynamic mode, the Ethernet Routing Switch checks for a Nortel signature in the DHCP packet. In static mode, the NSNA switch and Ethernet Routing Switch check for MAC authentication. Additionally, the NSNA switch tracks and displays all supported IP Phones in the network.

### Contact us

For product support and sales information, visit the Nortel web site at:

**www.nortel.com**

In North America, dial toll-free 1-800-4Nortel, outside North America dial 987-288-3700.

# Appendix A

# QoS Recommendations for VoIP

Ralph Santitoro

## Introduction

Many considerations need to be made before installing a VoIP system on an existing best-effort IP network infrastructure. This document provides an overview of the different QoS systems and makes recommendations about how they should be used.

## Quality of Service Systems

### *Why do you need QoS Systems?*

Most IP networks treat all traffic the same and are referred to as "best-effort" networks. Because of this, the traffic may experience different amounts of packet delay, loss or jitter at any given time. These types of traffic "impairments" result in the quality of the voice signal that the user will hear such as:

> Speech Breakup. This causes the speech to sound distorted, like the speech experienced on a digital cell phone when the signal is getting out of range.
>
> Speech Clipping. This causes parts of words to get cut off.
>
> Pops and clicks. This is caused when voice packets are dropped.
>
> Echo. This is caused by your voice getting reflected back to you from the remote end.

In today's TDM-based voice systems, the voice traffic experiences a fixed amount of delay and essentially no packet loss due to the structure of the circuit-switched telephone network resulting in very high quality voice. For VoIP systems, a QoS system is needed because voice over IP networks do not traverse along dedicated circuits with a small, constant amount of delay and no packet loss as in circuit-switched telephone networks.

IP networks are "connectionless," i.e., the voice traffic can take different paths from source (caller) to destination (called party) and the voice traffic also shares those paths with other types of traffic. QoS systems are required to ensure that voice traffic also experiences the high quality transmission needed to meet current user expectations.

Some data networks may be over-provisioned such that there is plenty of unused bandwidth available. While this may provide sufficient QoS for VoIP some of the time, it cannot provide QoS consistently during times of congestion or during transmission peaks of bursty data traffic. A QoS system eliminates these events that can impair the voice quality.

### *TOS and DiffServ: What's the Difference?*

The second byte of the IP packet header contains an 8-bit field used for IP QoS. The original definition of that field was referred to as the TOS (Type of Service). In 1999, the IETF (Internet Engineering Task Force) that is responsible for IP standards created a new QoS system and has redefined this byte to now be called the DiffServ (Differentiated) Service Field.

#### TOS

The TOS byte is broken down into 2 sub-fields, namely, the 3-bit IP Precedence field and the 4-bit TOS field. The least significant bit of the field is always set to zero. Figure 1 illustrates the different sub-fields.

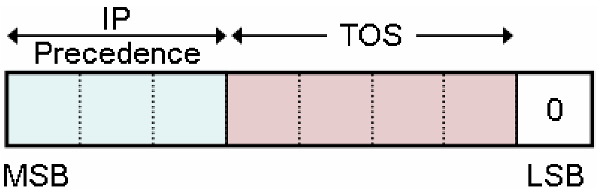


**Figure 2: TOS Byte**

Of these 2 sub-fields, the IP Precedence sub-field is used almost exclusively and the TOS sub-field has seen limited use. Legacy routers that do support IP QoS typically support only the IP Precedence field. These 3 bits result in 8 classes of service. Unfortunately, many people refer to a router supporting TOS when they really mean IP Precedence.

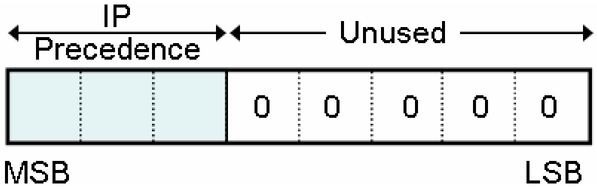


**Figure 3: IP Precedence field in TOS Byte**

## DiffServ

In 1999, the IETF created IP Differentiated Services (DiffServ) to replace the older IP QoS definitions of the TOS byte. The DiffServ field uses the same TOS byte but the definition of the bits and purpose of them is now quite different. The most-significant 6 bits are used while the last 2 bits are used for a capability known as Explicit Congestion Notification (ECN), which can be used by routers supporting ECN to inform neighboring nodes of congestion. The 6-bit value is referred to as the DiffServ Code Point (DSCP).

The value of the DSCP is used to define the DiffServ class to which the traffic belongs and the type of treatment the traffic will receive. Out of the 64 possible values for the DSCP, only 32 are currently available for public use while the other 32 are currently defined for experimental or local use.

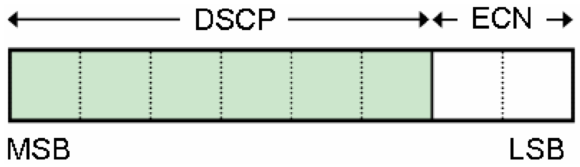


**Figure 4: DiffServ use of the TOS field**

Twenty-one of the 32 DSCPs have been standardized by the IETF, leaving 11 DSCPs that can be used for user-defined purposes.

## *IP QoS through DiffServ*

DiffServ defines a number of different services classes and QoS mechanisms that are applied (called Per-Hop Behaviors or PHBs) to packets in those service classes. These PHBs each have an IETF-standardized DSCP associated with them so that packets marked with these DSCPs can be determined to be in the respective DiffServ class. Different types of applications have different traffic characteristics and require different types of QoS behaviors to be applied to them.

### Class Selector DiffServ class

The Class Selector (CS) DiffServ PHB is represented by eight classes and uses the same bit positions as the IP Precedence field in TOS. Traditionally, the CS7 ('111000') and CS6 ('110000') DSCPs have been used for network control traffic and the CS0 ('000000') DSCP has been used for best effort traffic. The Class Selector PHB allows CS DSCPs to inherit the behavior of other PHBs. The significance of this will become apparent later in this paper.

| CS Code Point Name | CS Code Point Value |
|---|---|
| CS7 | '111000' |
| CS6 | '110000' |
| CS5 | '101000' |
| CS4 | '100000' |
| CS3 | '011000' |
| CS2 | '010000' |
| CS1 | '001000' |
| CS0 | '000000' |

**Table 1: Class Selector Code Points**

### Expedited Forwarding DiffServ class

The Expedited Forwarding (EF) DiffServ behavior provides a low-latency, high-priority service that is ideally suited for VoIP. The EF DSCP is represented by the binary value '101110.' Note that the term EF is not a hexadecimal value but an abbreviation of Expedited Forwarding.

### Assured Forwarding DiffServ Class

The Assured Forwarding (AF) DiffServ behavior consists of four different service classes, each with three different discard-priority levels.

Each AF class has three different discard priority (drop precedence) levels resulting in 12 different DSCP values. Routers use these drop precedence values to determine the discard priority of packets under network congestion. Note that the term AF is not a hexadecimal value but an abbreviation of Assured Forwarding.

| Discard Priority | AF Class | | | |
|---|---|---|---|---|
| | Class 1 | Class 2 | Class 3 | Class 4 |
| **Low** | '001010' (AF11) | '010010' (AF21) | '011010' (AF31) | '100010' (AF41) |
| **Medium** | '001100' (AF12) | '010100' (AF22) | '011100' (AF32) | '100100' (AF42) |
| **High** | '001110' (AF13) | '010110' (AF23) | '011110' (AF33) | '100110' (AF43) |

**Table 2: Assured Forwarding DiffServ Classes**

## *Configuring DiffServ*

When configuring DiffServ values (DSCP) with which to mark packets, be careful about how the device implements the DSCP. While the DiffServ field is an 8-bit value, the DSCP is only a 6-bit value. Some devices require you to configure an 8-bit value (DSCP + 00). Some devices require you to configure only the actual 6-bit DSCP value. In this case, the devices would pad this 6-bit value with 2 zeros to offer 64 contiguous values. For example, the 6-bit DSCP value for Expedited Forwarding (EF) is '101110' (binary), 2E (hexadecimal) or 46 (decimal). The 8-bit DiffServ field value for Expedited Forwarding (DSCP+00) is '10111000' (binary), B8 (hexadecimal) and 184 (decimal). Note that you would see this 8-bit value instead of the 6-bit DSCP if you used a network analyzer to look at the DiffServ byte.

## *DiffServ for VoIP*

If you currently have a best-effort IP data network and are just adding VoIP, the simplest approach is to construct your network QoS such that there are only 3 levels of traffic priorities. One priority is for VoIP media (bearer) traffic. The second priority is for VoIP signaling traffic. The third priority is for you best-effort IP data traffic. Routers connected to low-bandwidth interfaces must separate voice media and voice signaling packets to minimize voice jitter that would be introduced by the signaling packets to the voice media packets. This jitter would occur if the packets were not separated and placed in the same queue. This will be discussed in more detail in the section entitled "VoIP over Low-Bandwidth Connections".

**RECOMMENDATION**: Use DiffServ traffic classes as indicated in the following table:

| Traffic Type | DiffServ Class | DSCP (binary) | DSCP (decimal) |
|---|---|---|---|
| Voice media | Expedited Forwardin g | '101110' | 46 |
| Voice signaling | Class Selector 5 | '101000' | 40 |
| Data traffic | Default | '000000' | 0 |

## Ethernet IEEE 802.1Q

This is an IEEE Ethernet standard that adds 4 additional bytes to the standard 802.3 Ethernet frame for Ethernet QoS and Virtual LAN (VLAN) support. Most Ethernet switches support the 802.1Q standard with the exception of the lowest cost ones found at consumer electronics stores.

### *Ethernet 802.1p*

The Ethernet QoS is accomplished via the three 802.1p User Priority bits.

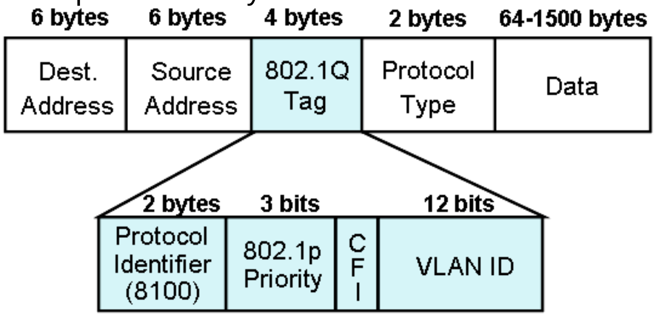


**Figure 5: 802.1p Priority bits in the 802.1Q Tag**

The 802.1p User Priority bits are used to create 8 classes of service for packets traversing Ethernet networks. Table 3 includes the definitions for each of the 802.1Q fields.

| 802.1Q Field | Description |
|---|---|
| 3-bit priority field (802.1p) | Value from 0-7 representing user priority levels (7 is the highest) |
| Canonical Field Identifier | Always set to 0 |
| 12-bit 802.1Q VLAN ID | VLAN identification number |

**Table 3: 802.1Q Field Definitions**

**RECOMMENDATION**: Use 802.1p user priorities indicated in the following table:

| Traffic Type | 802.1p (binary) | 802.1p (decimal) |
|---|---|---|
| Voice media and signaling | '110' | 6 |
| Data traffic | '000' | 0 |

## Making QoS Simple

After reading through this document, you will quickly conclude that QoS is quite a complicated topic and there are many different technologies, standards and implementations to consider. Furthermore, there is no single QoS technology or standard that can be used across your network. How can QoS be simplified?

Nortel Networks has embarked upon simplifying QoS by creating standardized, default QoS configurations and behaviors for its product in the form of end-to-end network service classes. These are called Nortel's Network Service Classes (NSC). The NSCs have been defined based upon the most common types of applications. The NSCs provide default mapping between DiffServ and different link layer QoS technologies that a particular interface uses, e.g., 802.1p for an Ethernet interface. The NSCs also provide default mapping of these QoS technologies to a specific queue on an interface.

| Traffic Category | Example Application | Network Service Class |
|---|---|---|
| Network Control | Critical Alarms | Critical |
| | Routing, Billing, Critical OAM | Network |
| Interactive | IP Telephony | Premium |
| | Video Conferencing, Interactive Gaming | Platinum |
| Responsive | Streaming audio/video | Gold |
| | Client/Server Transactions | Silver |
| Timely | Email, non-critical OAM | Bronze |
| | Best Effort | Standard |

**Table 4: Nortel's Network Service Classes (NSCs)**

NSCs provide the following default QoS settings for the following:

DiffServ Code Point
Link layer QoS, e.g., Ethernet 802.1p User Priority
Queue in which traffic is placed
Traffic Management Parameters
Traffic Schedulers

NSCs can also be created in other non-Nortel products through device configuration or QoS policy management systems.
Nortel has defined the Premium NSC to be used for IP Telephony applications such as VoIP. Table 5 outlines some of the default attributes of the Premium NSC. Note that the link layer QoS attributes will be specific for a given interface type. For example, an Ethernet interface will use 802.1p while an ATM interface will not.

| QoS Attribute | Premium NSC default setting (4 queue system example) |
|---|---|
| DSCP | Voice Media - Expedited Forwarding |
| | Voice Signaling Class Selector 5 |
| Link Layer QoS | 802.1p User Priority 6 |
| | ATM CoS = CBR or rt-VBR |
| | PPP Class Number 3 |
| Scheduler | Priority |
| Policer | Drop packets exceeding configured rate |

**Table 5: Default Premium NSC settings-4 queue system**

## *How do NSCs simplify QoS?*

The best way to illustrate this is by an example. Suppose you are deploying VoIP services over an existing best-effort IP data network in your facility. Before you introduce the VoIP service, you need to QoS-enable your network.

### VoIP Gateways and IP Phone Configuration

Your VoIP gateways and IP phones would be configured to pre-mark the VoIP packets for the Premium NSC, i.e., voice media packets marked with the 'EF' DSCP and voice signaling packets marked with the 'CS5' DSCP. Note that you could bypass this step with some Nortel Networks products that already provide you with these default settings.

### IP Routers and L2/L3 switches Configuration

You need to QoS-enable your networking devices and configure them to place the VoIP traffic into the Premium NSC. This is accomplished by configuring your data networking equipment to provide Premium NSC treatment to all 'Premium-marked' packets. Some Nortel Networks products already perform this by default when QoS is enabled on a particular interface. Otherwise, you will have to configure all of the many configuration settings (e.g., priority scheduler, tail drop policer, link layer QoS setting, etc.) that the Premium NSC would automatically provide for you by default.

## Other methods to achieve QoS

Depending upon the application, different and often simpler, QoS mechanisms can be applied. DiffServ is used to provide IP QoS services across the network. However, 802.1p may not be necessary to provide QoS for your VoIP traffic for your layer 2 Ethernet switches. QoS could be achieved by methods described below.

### *Port Prioritization*

If you are adding a VoIP gateway, it will connect to a specific port on your Ethernet L2 switch so you would configure the L2 switch to prioritize all traffic coming from the port. Refer to Figure 6. In this case 802.1p is not required because you are prioritizing all traffic coming in on this port.

If the device attached to the L2 switch port is an IP phone, then port prioritization is not recommended since IP phones may be unplugged and moved. If a PC were connected to a port configured to use port prioritization, then all of the PC's traffic would be given high priority treatment.

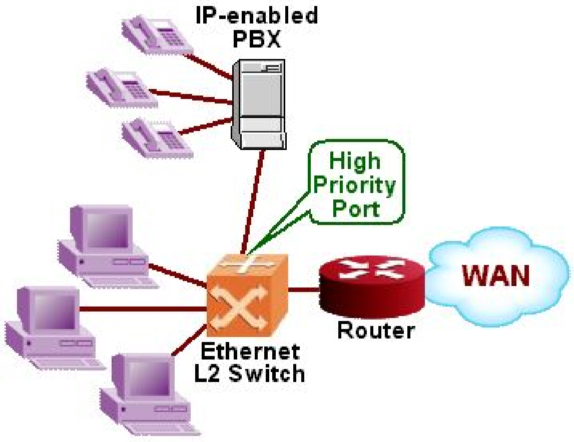


**Figure 6: Port-based prioritization example**

### *Traffic Separation using VLANs*

All voice traffic can be placed into one VLAN and all other data traffic into another VLAN. Refer to Figure 7. The "Voice" VLAN traffic can be prioritized over the "Data" VLAN traffic. In some cases, this may be the easiest method if all Ethernet switches support the 802.1Q standard for VLANs. VLANs can also be used to separate traffic for security purposes.

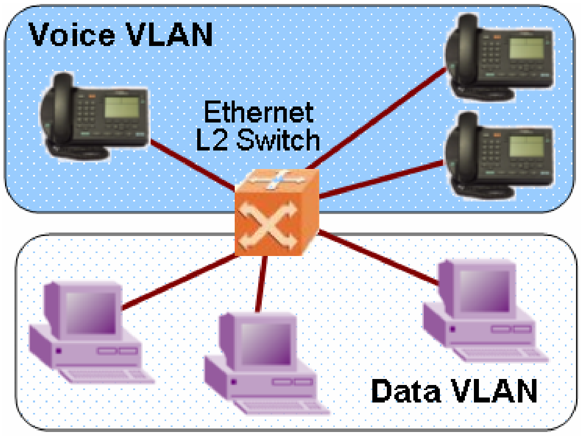


**Figure 7: Voice and Data VLAN example**

### *IP Address Prioritization*

VoIP traffic can also be prioritized by its IP address. Refer to Figure 8. This approach is ideal for devices with statically assigned IP addresses that rarely, if ever, change. IP PBXs, VoIP gateways and call servers are VoIP devices that would have their IP addresses statically assigned. A network administrator can configure the routers to filter (classify) and prioritize all packets originating from these IP addresses and know they are from VoIP devices.

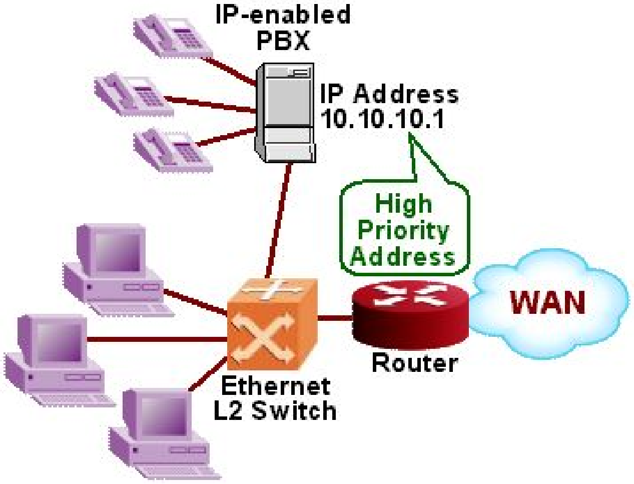


**Figure 8: IP address-based prioritization example**

In Figure 8, any traffic entering the router from IP address 10.10.10.1 will get priority over any other traffic.

**RECOMMENDATION**: For stationary IP telephony devices such as VoIP gateways, use port prioritization on the Ethernet switch port that connects to the device.

## Other Considerations

There may be other items to consider when setting up your QoS enabled network. For example, do you "trust" your network connections or VoIP devices connected to your network? If the network is under your complete administrative control, e.g., private IP network, then you may have control over and hence trust the VoIP devices attached to your network. It is possible for VoIP devices, e.g., IP phones and gateways, to generate packets that are pre-marked with QoS settings (DiffServ DSCP or Ethernet 802.1p) that you have provisioned. Can you trust those devices to mark their VoIP packets with the appropriate QoS markings?

### *Packet Marking for QoS*

Some VoIP devices such as IP phones and gateways can pre-mark packets with QoS settings prior to transmitting them to the network. These devices could mark the DiffServ Code Point (DSCP) and perhaps also the Ethernet 802.1p user priority. If the VoIP devices cannot provide pre-mark packets, then you have to rely on the routers or policy switches to perform this marking. Some products such as the Nortel Networks Business Policy Switch and Passport 8600 can classify, mark and prioritize based on both DSCP and Ethernet 802.1p.

**RECOMMENDATION**: Use DiffServ packet marking unless other routers or L3 switches in your network only support IP Precedence. Also use Ethernet 802.1p user priorities to tag your VoIP packets if your voice devices support this capability.

### *VoIP Packet Scheduling*

It is important that all VoIP packets be queued in a router or switch using a strict priority scheduler whereby VoIP packets will receive priority treatment over all other packets. This is required to minimize voice traffic delay but more importantly, minimize the delay variation (jitter) introduced to the voice traffic. Because a strict priority scheduler can "starve" the servicing of all other traffic queues, you need to set a threshold to limit the maximum amount of bandwidth that the VoIP traffic can consume. Most products allow you to set this and it is often called "rate limiting."

Other "weighted" schedulers such as Weighted Round Robin (WRR) or Weighted Fair Queuing (WFQ) are NOT RECOMMENDED. If your 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 percent. If you cannot configure a 100 percent weight due to some product limitation, then you should consider replacing the product because it will cause unpredictable voice quality.

**RECOMMENDATION**: Use a strict priority scheduler for VoIP.

## VoIP over Low-Bandwidth Connections

There are a number of items to consider when using routers with low-bandwidth WAN and access network connections such as xDSL and

Packet Cable. This section will specifically discuss WAN connections but the techniques and recommendations described also apply to other low-bandwidth access network connections such as xDSL and Packet Cable.

## Per call bandwidth

The amount of bandwidth a VoIP call uses depends on whether the voice signal is compressed and what link layer protocol the VoIP packet uses for transport. It is desirable to compress your voice signals when using VoIP over a low-bandwidth connection. There are several possible choices for voice compression. The ITU G.729 codec provides the lowest bandwidth yet highest voice quality. G.729 compresses the voice call from 64kbps down to 8 kbps. This 8kbps is the "raw voice" bandwidth and needs to be encapsulated into other protocols before it becomes VoIP and can be transported over an IP network. The link layer protocol to transport the IP packet could be PPP, Frame Relay or ATM. The additional overhead added by these protocols increases bandwidth required for VoIP packets to 24kbps. (Note that the 24kbps is based on 20ms voice samples.)

Voice compression is not required over high bandwidth, Ethernet connections. This uncompressed voice is encoded using the ITU G.711 codec resulting in 64kbps of "raw voice" bandwidth. The voice gets encapsulated into IP and Ethernet to create a VoIP packet which requires 80kbps of total bandwidth. (Note that the 80 kbps is based on 20 ms voice samples.)

### Bandwidth Example

One of the main attractions of VoIP is the ability to use an existing WAN data network infrastructure 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, the routers are typically configured to reduce the data traffic throughput by the amount of bandwidth for the VoIP call, e.g., 24kbps per call over a PPP connection. This will reduce the data traffic throughput to perhaps an unacceptable level. Adding VoIP to the existing WAN data network may require the WAN bandwidth to be increased.

Example: A company has two sites that are connected via a leased line WAN connection operating at 128kbps. This bandwidth is sufficient for the current data requirements. The company believes that it only needs 70-80kbps most of the time with occasional traffic peaks up to the full 128kbps. The company wants to support up to four simultaneous voice calls over the IP WAN network between the sites. If all four calls were simultaneously active, this would require 96kbps (using a G.729 codec) of the available 128kbps of the connection leaving only 32kbps remaining for the data traffic. This is not sufficient based on the company's business needs.

Solution: Upgrade the WAN connection bandwidth.

**RECOMMENDATION**: Use G.729 codec to compress voice traffic over low-bandwidth connections. Budget 24kbps of bandwidth for each simultaneous G.729 call.

Do not use any voice compression over high bandwidth connections. Budget 80kbps of bandwidth for each simultaneous G.711 (uncompressed) call.

## Delay/Latency

The overall "delay budget" for a voice call from the time you speak to the time the receiver hears your voice should typically be no longer than 200ms for good quality voice over landline connections. (The amount of delay is often longer but unavoidable for satellite and other types of wireless connections.) Studies have shown that as the 200 ms delay budget is exceeded, most users tend to perceive the delay, resulting in more dissatisfaction with voice quality. Every time a VoIP packet passes through a device or network connection, delay is introduced. A significant amount of delay can be introduced over low-bandwidth connections.

## Reducing Delay Through Packet Fragmentation

In mixed voice/data IP networks, packets must be fragmented prior to traversing bandwidth-limited (<1Mbps) connections to minimize voice delay and jitter. There are several different protocols that can be used to fragment packets. For Frame Relay connections, you can use the FRF.12 standard for fragmenting packets. ATM natively provides fragmentation since all packets are fragmented into 53-byte ATM cells. Both of these fragmentation techniques are acceptable. However, there are two types of fragmentation that are more universal and not limited to a specific link layer technology such as ATM or Frame Relay. These methods are via the PPP protocol and via IP fragmentation.

### 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 queuing and transmission. PPP fragmentation allows higher-priority VoIP packets to interrupt and transmit ahead of the remainder of larger, lower-priority packets that have already been queued. The packets may be interleaved so the maximum delay a voice packet will experience is one 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 begins to get transmitted as the first fragment. Next, the first fragment of the data packet is transmitted. Next, the second voice packet is transmitted. Finally, the second fragment of the data packet is transmitted. If no more packets enter the router, then the data packet fragments will continue to be transmitted until the entire data packet is transmitted.

### IP Fragmentation

All routers support IP fragmentation whereby all IP packets are configured to a size determined by the MTU (Maximum Transmission Unit). Most routers use a default maximum packet size of 1500 bytes, which can take a considerable amount of time to transmit over a low-bandwidth connection. Consider a 1500-byte data packet being transmitted over a 64kbps connection. It would take 188ms to transmit this data packet out of the router onto the 64kbps connection. This same queuing delay is added again as the packet is queued in at the far-end router on the other side of the connection. In general, a desirable end-to-end delay for a voice packet to achieve high quality is less than 200ms. So you can see that this data packet uses up almost the entire delay budget for the voice traffic before the first voice packet is ever transmitted!

Over bandwidth-limited connections (<1Mbps), if PPP fragmentation is not used, the router must be configured to transmit smaller packets by adjusting the MTU size for the IP packets. The MTU size is adjusted to achieve a maximum delay of 20ms over the different connection speeds. Therefore, a higher bandwidth connection will have a larger MTU size than a lower bandwidth connection.

**RECOMMENDATION**: PPP is the preferred method for packet fragmentation. IP fragmentation can also be used if your router does not support PPP fragmentation.

The following table provides the recommended maximum MTU sizes for different connection speeds when using IP fragmentation:

| | **Connection Rate (kbps)** | | | | |
|---|---|---|---|---|---|
| | **56** | **64** | **128** | **256** | **512** |
| Maximum MTU (bytes) | 128 | 128 | 256 | 512 | 1024 |

## Link Utilization for VoIP Traffic

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.

**RECOMMENDATION**: For low-bandwidth (<1Mbps) connections, you can use up to 50 percent of the available bandwidth for voice traffic. For connections > 1Mbps, you can use up to 85 percent of the available bandwidth for voice traffic.

## *Packet Reordering*

In some cases there may be multiple paths for a VoIP packet to take when traveling from its source to its destination. If all VoIP packets do not take the same path then packets could 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.

Example: If two locations are connected using two Frame Relay PVCs, you must ensure that all voice traffic for a specific call traverses the same PVC. The routers can be configured to direct voice packets from the same source/destination IP address to traverse the same VC. Another approach is to configure the router to send all voice traffic over only one of the PVCs.

# VoIP over Ethernet Networks

Ethernet networks require less sophisticated QoS mechanisms than low-bandwidth WAN connections because the bandwidth is much higher, resulting in significantly lower queuing and network delay. However, network congestion, even for short periods of time and bursty, TCP-based Internet traffic can cause significant voice quality problems if QoS were not applied.

Only switched-media Ethernet networks should be used with VoIP. Shared-media Ethernet hubs must never be used. QoS mechanisms described earlier, such as 802.1p, VLANs and Port prioritization can be used for VoIP traffic over Ethernet networks. If the Ethernet switches support layer 3 capabilities, then QoS mechanisms such as DiffServ, IP Address prioritization can also be used.

# Summary

VoIP requires QoS systems to be implemented in your IP network to ensure predictable and acceptable performance. You now are armed with a basic understanding of the different QoS technologies to consider when deploying VoIP.

# References

"Introduction to Quality of Service (QoS)," http://qos.ca.nortel.com/Whitepapers/WP-QoS-GEN-01.pdf

RFC 3246, "An Expedited Forwarding PHB," http://www.ietf.org/rfc/rfc3246.txt

RFC 2597, "Assured Forwarding PHB Group," http://www.ietf.org/rfc/rfc2597.txt

RFC 791, "Internet Protocol" (includes TOS field definition), http://www.ietf.org/rfc/rfc0791.txt

RFC 2475, "An Architecture for Differentiated Services," http://www.ietf.org/rfc/rfc2475.txt

RFC 2474, "Definition of Differentiated Services Field (DS Field) in IPv4 and IPv6 Headers," http://www.ietf.org/rfc/rfc2474.txt

RFC 2686, "Multi-Class Extensions to Multi-Link PPP," http://www.ietf.org/rfc/rfc2686.txt

RFC 1990, "PPP Multilink Protocol (MP)," http://www.ietf.org/rfc/rfc1990.txt

ATM Forum Traffic Management Specification v4.1 ftp://ftp.atmforum.com/pub/approved-specs/af-tm-0121.000.pdf

IEEE 802.1Q, "Virtual Bridged Local Area Networks," http://standards.ieee.org/reading/ieee/std/lanman/802.1Q-1998.pdf

# About the Author

Ralph Santitoro, Director of network architecture at Nortel, provides best practice guidelines for network/service architecture, triple play services, QoS, and traffic management for Ethernet, IP, MPLS, and broadband access networks. Mr. Santitoro chairs Nortel's QoS Core Team which defines the QoS technology requirements and strategy for Nortel's enterprise and carrier product portfolios. Mr. Santitoro is co-author of Nortel's "The Essentials of Real-Time Networking" book published in December 2004.
Mr. Santitoro can be reached at rsantito@nortel.com or +1 805-527-3024

# Acknowledgements

The author would like to thank John Hagerty, who provided significant contributions to the initial version of this paper.

## Nortel Locations

| | |
|---|---|
| In the United States: | In Europe: |
| Nortel | Nortel |
| 35 Davis Drive | Maidenhead Office Park |
| Research Triangle Park,<br>NC 27709  USA | Westacott Way<br>Maidenhead Berkshire SL6 3QH<br>UK |
| | |
| In Canada: | In Asia Pacific: |
| Nortel | Nortel |
| 8200 Dixie Road, Suite 100<br>Brampton, Ontario L6T 5P6 | Nortel Networks Centre<br>1 Innovation Drive |
| Canada | Macquarie University Research Park Macquarie Park NSW 2109 Australia |
| In Greater China: | Tel: +61 2 8870 5000 |
| Nortel | |
| Sun Dong An Plaza, | In Caribbean and Latin America: |
| 138 Wang Fu | Nortel |
| Jing Street | 1500 Concorde Terrace |
| Beijing 100006, China | Sunrise, FL  33323  USA |
| Tel: (86) 10 6528 8877 | |

## About Nortel

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both enterprise and service provider customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband,
Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the web at http://www.nortel.com.

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

This is the Way, This is Nortel, Nortel, the Nortel logo, the Globemark, Alteon, BayStack, Passport and Contivity are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.