>THIS IS **THE WAY**

>THIS IS NORTEL™

> Converged Campus Technical Solution Guide

Enterprise Solution Engineering
Document Date: September 2005
Document Version: 1.2

Copyright © 2005 Nortel

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. It is solely for the 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 a Converged Campus infrastructure. The document provides an overview of the best design practices to implement a network capable of supporting converged applications and services.

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 a converged campus network design.

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

Revision Control

No	Date	Version	Revised by	Remarks
1	7/28/05	0.5	D. DeBacker	Initial Draft
2	8/16/05	0.8	B. Black	Added TPS Section
3	8/31/05	1.0	D. DeBacker	Edited with feedback from field
4	9/13/05	1.1	JT	Minor Edits – Draft
5	9/15/05	1.2	D. DeBacker	Final Edits

Acknowledgements

Seth Atkins
Brad Black
Andrew Bojak
Fariz Elchamma
John Mead
Ramesh-Babu Puvvada
Terry Singleton
Jean Turgeon
John Vant Erve

Figures and Tables

1. Overview

The Converged Campus solution combines a highly available network infrastructure with proven, feature-rich business telephony and applications. Our solutions provide a strong foundation for innovative converged applications such as IP Telephony and Multimedia. 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, the network must be resilient, reliable, secure, and still provide high performance.

This solution guide highlights various deployment scenarios, with a focus on the infrastructure components required for the converged campus. The solutions ensure 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
- Terabit Switching Cluster
- Flexible deployment options
- QoS capable infrastructure
- Simplified management of all components

1.1 Scope of Document

This document covers the infrastructure components required to design a Converged Campus solution. It highlights the Nortel recommended designs and best practices for implementing a converged solution. 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

- Ethernet Routing Switch 8600
- Ethernet Routing Switch 8300
- Ethernet Routing Switch 5510/5520/5530
- Ethernet Switch 460
- Ethernet Switch 470

Ethernet Switching Hardware Considerations

- Hardware Resiliency (Chassis/Stackable)
- Power Considerations (Redundancy, 802.3af Power over Ethernet)
- Physical Links (GBIC, SFP, CWDM, XFP)

Ethernet Switching Technologies

- Link Detection/Protection (RFI, FEFI, SFFD, LACP, VLACP)
- Link Resiliency (SMLT, RSMLT, VRRP, ECMP, RSTP, LACP)
- Layer 2 and Layer 3 Security (SNMPv3, SSH, DoS Protection, Threat Protection)

- Layer 3 Routing (OSPF, RIP, BGP, DVMRP, PIM-SM)
- Quality of Service (QoS)

This document highlights the applications and services of the converged campus, but does not go into detail on those individual solutions. Those topics are covered in separate solution guides focused on those areas. These applications include:

- IP Telephony/Multimedia
  - Secure Multimedia Zone
  - IP Telephony Deployment
  - Multimedia Communication Server (MCS)
  - IP Video (Surveillance, Conferencing)
- Wireless LAN
  - Wireless VoIP
  - AAA
  - Encryption
  - Roaming
- Secure DMZ
  - Intelligent Traffic Management
  - Threat Protection
  - Switched Firewall
  - VPN Gateway
- Secure/Resilient Data Center
  - Application Switching
  - Threat Protection
  - Fault Tolerant Server Connectivity
  - Switched Firewall

2. Converged Campus Design Solutions

The Converged Campus Solution addresses specific areas to consider when designing the network infrastructure. This solution is intended to provide optimal network designs and general best practices when implementing and administering the network. The end result is a network that can sustain both normal data traffic as well as any converged applications the end user wishes to access. The main topics for discussion include:

Physical Network Components

- Client Connectivity
- Edge Switching
- Uplink Resiliency
- Core Switching

- Threat Protection

Logical Network Components

- VLANs
- Broadcast Domains
- IP Routing
- Security
- Network Management

Please note that all design recommendations and best practices within this guide should be reviewed against the available features on the Ethernet switching platforms being deployed and should also be reviewed against the release notes for the versions of software being used. As bugs are identified and fixed, it is imperative to understand the capabilities and limitations of the switches and software being implemented. This ensures that the design being deployed utilizes the features and functions of the switches to their maximum effectiveness.

2.1 Converged Campus Topology

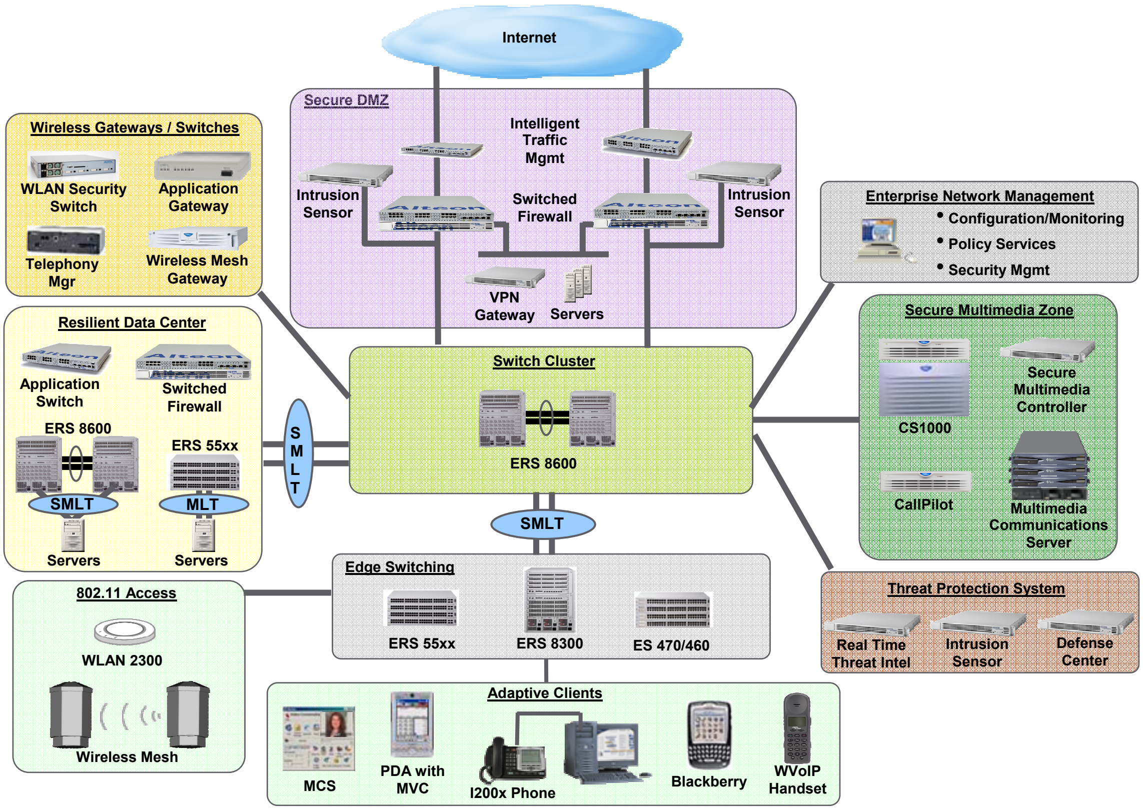


Figure 1: Converged Campus Topology – Overall View

2.2 Network Design

The topology shown in Figure 1 includes all areas of the Converged Campus solution. This guide now focuses on the architecture for edge switching and core switching. There are many permutations of possible designs when deploying infrastructure from Nortel, but this guide highlights the strategic products in each area that are presently available. The ultimate goal of these designs is to provide reliability within the infrastructure so that if a failure occurs, then subsecond seamless failover and recovery prevent any interruption of traffic on the network.

The two major design options are presented in this solution guide: two tier architecture, in which all edge switches terminate into the core of the network, and three tier architecture, in which the edge switches terminate into a distribution layer network. The distribution layer network then terminates into the core. Three tier architecture is usually required when the existing cable plant cannot support a two tier deployment because of fiber distances or layout.

The detailed topology in Figure 2 shows a typical deployment scenario in a two tier architecture design, while Figure 3 shows the same scenario in a three tier architecture design. Both provide for the various edge switching options.

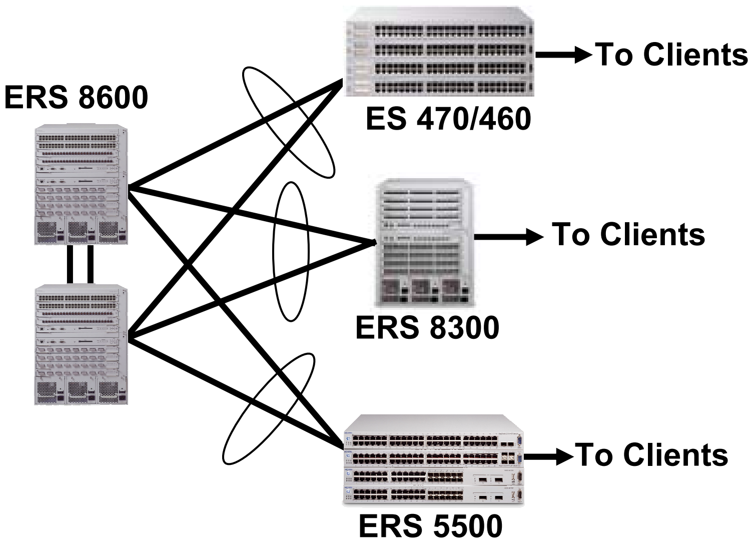


Figure 2: Two Tier Architecture

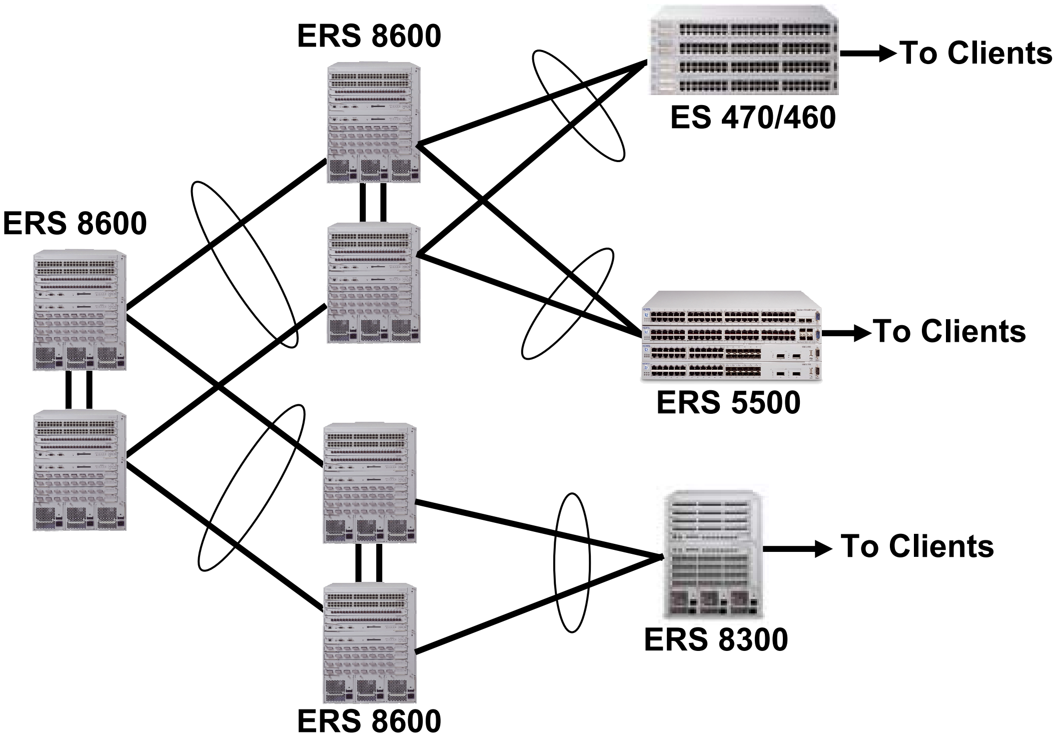


Figure 3: Three Tier Architecture

With both designs, there are several areas of configuration that must be taken into consideration in order to build a truly resilient network. There are also issues to be reviewed regarding the selection of the proper edge switching solution.

From a logical perspective, there are two options for consideration: either Layer 2 at the edge with Layer 3 in the core/distribution, or Layer 3 at the edge with Layer 3 in the core/distribution. Nortel provides Ethernet switching platforms that can provide either design alternative. There is no right answer for all possible designs; however, the Nortel philosophy is always to keep the architecture as simple as possible without compromising resiliency and scalability. This translates into easier management and an overall lower total cost of ownership (TCO) by centralizing routing in the core and distributing intelligence across the network.

2.2.1 Design Recommendation

Deploy a two tier architecture whenever possible. This simplifies the network architecture, reduces the amount of equipment required, and is still very scalable. The two tier architecture can support either Layer 2 or Layer 3 at the edge. As a general rule, If aggregating less than 3000 users into the core, it is desirable to use Layer 2 between the access and core, and if aggregating more than 3000 users, it is better to use Layer 3 between the access and core – this helps to distribute ARP (Address Resolution Protocol) tables, simplify subnet provisioning, and with RSMLT (covered later in this document), allows the extension of Layer 2 VLANs across multiple access switches.

If a three tier architecture is deployed, Nortel recommends using Layer 3 between the distribution and core layers, utilizing RSMLT for these connections. The same rules apply to the connections between the access and distribution layers (for less than 3000 users, use Layer 2; for more than 3000 users, use Layer 3).

With any of these options, it is critical to deploy an end-to-end QoS strategy to ensure that mission-critical applications are able to provide the required quality of experience for the users. A detailed discussion of QoS will be covered in an upcoming section.

2.2.2 Chassis versus Stackable

Several factors come into play when choosing the edge switching solution. Consider the following criteria when selecting the edge product while keeping in mind that the stacking technology continues to evolve and is getting closer and closer to simulating a modular chassis solution.

Switch reliability is a key concern. In the past, modular switches were thought to be more reliable with redundant power supplies, redundant fan trays, and redundant switch fabrics and CPUs. However, the evolution of the stackable switch has reduced the disparity between the two platforms by employing a resilient stacking architecture, supporting external redundant power supplies, and providing features such as auto unit replacement and new unit quick configuration. Both solutions can provide an equally highly reliable edge solution today, although stackable switches require more power outlets in the closet than do chassis switches.

Scalability of the edge switch includes the ability to add ports easily, increase bandwidth out of the closet, and add protocol and features within the closet. A chassis solution typically adds ports by adding new input/output (I/O) modules in the chassis, while stackable switches add ports by adding switches to the existing stack. Both solutions limit the total number of ports supported in a single stack/chassis. The stackable switches provide more flexibility when adding bandwidth out of the closet. A stack can be broken up into two or more stacks, thus increasing bandwidth out of the closet very easily. As stackable switches are added the closet, each one must be powered individually, which uses several outlets in the closet. In contrast, only two to three outlets are usually required for a chassis solution. The same protocols and features are added on both platforms; however, scalability of those protocols is always greater in a chassis solution. It is easier to redeploy stackable switches as a stack or stand-alone unit, whereas the modular chassis requires additional hardware to support the I/O modules.

Serviceability and manageability differences between the two solutions are minimal. With both solutions, you can add ports easily, perform software upgrades, retain multiple configurations, and manage the stack or chassis as a single entity.

Rack space can also be a consideration when selecting the edge switching platform. Typically, a stackable solution takes up less total rack space than a chassis solution in both height and depth. However, stackable switches require rear access for power connections and stacking connections, whereas a chassis solution requires only front access.

The final consideration between the two solutions is price. Usually, a chassis solution is slightly more expensive than a stackable solution due to the additional Switch Fabric/CPU (SF/CPU) needed. In summary, both solutions offer great reliability and scalability. Each customer must decide which provides the optimal solution for their organization.

For a more detailed discussion on this subject, refer to the white paper “Wiring Closet Equality,” document NN108321-052604, available at http://www.nortel.com.

2.2.2.1 Design Recommendation

Regardless of the platform chosen for the edge closet, the following criteria should be taken into consideration:

- Stackable
  - Utilize resilient stacking architecture (always use stacking return cable)
  - Switch redundancy for closet uplinks
  - Power redundancy with external RPSU, preferably on separate electrical circuits
- Chassis
  - N+1 power redundancy, preferably on separate electrical circuits
  - Redundant switch fabrics
  - I/O module redundancy for closet uplinks

2.2.3 Edge Connectivity

After you select the edge switching platform (chassis or stackable), your next decision concerns end station connectivity. This is a very broad subject, but there are a few criteria that need to be reviewed when deciding on the configuration for end stations.

- Spanning Tree
- Virtual LANs (VLAN)
- Autonegotiation
- Quality of Service
- Multicast
- End Station Authentication
- Power over Ethernet

2.2.3.1 Spanning Tree

The IEEE 802.1d Spanning Tree protocol is used to prevent loops in the network. Usually, these loops occur when the design includes redundant connections from the edge to the core, or when multiple wiring closets are inadvertently interconnected. A loop in the network causes severe congestion and eventually renders the network inoperable. Nortel recommends using Split MultiLink Trunking (SMLT) to interconnect closets to the core of the network, thus alleviating the need for the Spanning Tree protocol on uplinks.

When you use SMLT between the edge switch and the core or distribution switch, you can use two or more redundant paths to two separate core/distribution switches without the need for Spanning Tree to prevent loops. Traffic is distributed over all available paths using either MLT or 802.3ad. If one or more of the redundant paths fails, SMLT provides subsecond recovery to an alternative path.

Although there are new Spanning Tree protocols, such as 802.1w Rapid Spanning Tree (RSTP) and 802.1s Multiple Spanning Tree Groups (MSTP), these have limitations. Although RSTP offers faster recovery than normal 802.1d Spanning Tree, it still has the same problem as that of 802.1d: all redundant or looped paths are blocked. MSTP does allow load balancing of VLANs over redundant paths; however, this requires configuration of every switch to assign cost or weight to all available paths for each VLAN. This can lead to administrative difficulties when there are a large number of switches in the network. SMLT removes these requirements – all you have to do is enable SMLT on the core/distribution switches and MLT or LACP on the edge switch. SMLT loads balance traffic without any other user input required.

Nortel does recommend using the Spanning Tree protocol on all end station connections in order to safeguard the network from hubs or other devices that could be inserted into the network at the end station. A modification to the normal learning of spanning tree is employed in all Nortel edge switches. This feature is known as Fast Start or Fast Learning, and is the recommended setting for all end station ports.

Under the normal operation of Spanning Tree, a port is first placed into a Blocking state while Bridge Protocol Data Units (BPDU) are exchanged. During this process, the port transitions to Listening and Learning states. While this is happening, no end station data traffic is passed through the port. After it is determined that there are no physical loops in the network, the port is transitioned to a Forwarding state and can now pass end station data.

The process of going from Blocking to Listening to Learning to Forwarding can take as long as 45 seconds. If the end station is using Dynamic Host Configuration Protocol (DHCP) to get an IP address, or has a timeout value on network logon (as does Windows Networking, Novell IPX, and others), the time it takes for Spanning Tree to fully converge can be too long and cause end station connectivity issues (no IP address, no network logon). To overcome this problem, Fast Start assumes there are no network loops and brings the port up in a Forwarding state initially. If there are loops in the network, the port shuts down immediately, preventing network outages.

2.2.3.1.1 Design Recommendation

Enable Spanning Tree Fast Start/Fast Learning on all end station ports. Never enable Fast Start/Learning on any uplink ports; this will cause loops in the network and therefore could have unexpected affects on the entire network. When using Spanning Tree, pay attention to the root bridge. Ensure the root bridge is one of the core switches by configuring the Spanning Tree priority. When using SMLT to connect the edge to the distribution/core, always disable Spanning Tree on the uplink ports/MLT of the edge switch.

2.2.3.2 Virtual LANs (VLAN)

The use of VLANs within a Converged Campus design is quite common. VLANs provide an easy mechanism for traffic separation, a way to minimize the size of broadcast domains, and can help to isolate different protocols from each other. In most cases, the VLAN is considered equal to a broadcast domain; for example, a specific IPv4 subnet is assigned to a single VLAN. From an administrative point of view, VLAN to subnet mapping makes each very easy to identify quickly. The number of VLANs and the type of VLANs deployed can vary greatly from design to design.

Like many other aspects of the Converged Campus design, there is no right and wrong answer, but there are certain design criteria to consider when creating the VLAN design strategy:

- Whether different protocols need to be isolated on the network
- Various VLAN types to be used (port, protocol, MAC, subnet)
- Traffic separation (voice, data, wired, wireless)
- Size of broadcast domain/number of users
- VLANs by geographic area (per closet, per floor, by building)
- VLANs by organizational function (engineering, marketing, etc.)
- Network services required per VLAN (i.e., DHCP)

Another aspect of VLANs is their use as a security mechanism. The implementation of VLANs on the Nortel switching infrastructure makes them extremely secure. There is no possibility of traffic leakage between VLANs at the Layer 2 level. The switches also have the ability to provide a private VLAN edge function that can also assist in an even greater separation of traffic at the host connection. Nortel does not use any VLAN auto discovery protocol such as CDP, thereby preventing a rogue user from connecting a switch to the network and discovering VLANs used on the network.

2.2.3.2.1 Design Recommendation

The following design recommendations are intended to cover a broad range of implementations. Because VLANs are used throughout the network, there is application at the edge and core. These recommendations focus on the edge:

- When implementing Voice over IP (VoIP) it is preferable to deploy a separate VLAN for voice traffic (that is, a VLAN that is dedicated to IP handsets, such as the Nortel i200x). This allows very easy QoS implementation (VLAN prioritization) and helps to isolate the voice traffic from the data traffic. Keeping data traffic (broadcast, multicast, unicast) off the voice network results in improved performance and security.
- When possible, limit the size of a broadcast domain to a single Class C subnet (254 hosts). This is common practice within the industry and also helps to keep broadcast domains small. Having a larger broadcast domain is sometimes necessary, but is not usually recommended.
- Assign general use VLANs by geographic location if possible. The most common practice is to assign VLANs by closet or floor. This practice limits the need to bridge VLANs throughout the network, thus reducing administrative overhead. It also aids in troubleshooting any network or application issues that may arise. An exception to this practice occurs when you create a VLAN for a specific protocol or application that may need to be bridged throughout the network (e.g., IPX, Appletalk, Netbios).
- In most cases, with the advent of a thin Access Point (AP) architecture, there is no longer a need to create a separate wireless VLAN on the wired infrastructure. The APs can generally be connected to any existing VLAN and tunnel their traffic back to a centralized security switch. Details on this application can be found in the *Wireless VoIP Solution Guide*.
- Use DHCP (Dynamic Host Configuration Protocol) to automatically assign IP addresses for those VLANs supporting IP end stations. This eliminates the administrative overhead of statically assigning addresses for each station on the network.
- Always enable 802.1Q VLAN tagging from the edge to the distribution/core. Even if only one VLAN is used at the edge, this enables the addition of more VLANs in the future

without disrupting existing traffic. Enabling 802.1Q VLAN tagging adds a Q tag to every packet on the uplink in order to maintain the VLAN separation across the link. Nortel recommends enabling the Discard Untagged Frames feature on those uplink ports. This causes any packets that are not Q tagged coming into the switch to be dropped.

- Avoid using the default VLAN whenever possible. This helps to minimize the possibility of accidentally creating Layer 2 loops in the network. Because the same default VLAN exists on every switch, it is very easy to incorrectly connect all these VLANs together and create unexpected traffic flows in the network.

2.2.3.3 Autonegotiation

The Autonegotiation standard for Ethernet allows end stations to connect at their most optimal speed and duplex – anything from 10 Mbps half duplex up to 10 Gbps full duplex. This feature allows different end stations with different connectivity capabilities to connect to a single network without the intervention of the network administrator.

Autonegotiation must be enabled on fiber ports to support Remote Fault Identification (RFI) for Gigabit/10 Gigabit and Far End Fault Identification (FEFI) for 100FX connections. These features shut down a port in the case of a single fiber fault at the remote end of the link. A more detailed description is covered in the section on fiber fault detection.

It is critical to verify that both ends of the link are capable of supporting Autonegotiation. If one end is not able to support it, then Autonegotiation must be disabled on both ends of the link. Having Autonegotiation enabled on one end and disabled on the other end is a common configuration error that can cause severe performance degradation of that connection.

In certain situations, it is useful to be able to autonegotiate a specific speed and duplex value by controlling which capabilities are being advertised from the switch. Nortel introduced the Custom Auto-Negotiation Advertisement (CANA) feature to accommodate this need. This feature allows the administrator to control which advertisements are made by the switch. For example, if the switch only advertises a 100 Mbps full duplex capability on a specific link, then the link is only activated if the neighboring device is also capable of autonegotiating a 100 Mbps full duplex capability. This prevents mismatched speed/duplex modes if customers disable Autonegotiation on the neighboring device.

2.2.3.3.1 Design Recommendation

- Enable Autonegotiation on all end station ports, ensuring that all those stations are capable of supporting autonegotiation.
- Where required, use Customized Auto-Negotiation Advertisements (CANA) to control end station connectivity speed and duplex.
- When connecting servers, disable Autonegotiation on both the server and the corresponding switch port. These ports are usually tightly controlled by the administrator and therefore the capabilities of the device connected will not change. Disabling Autonegotiation on these ports eliminates a variable in any troubleshooting activities for server connectivity.
- Disable Autonegotiation on problematic devices. Because the Autonegotiation standard is rather broad, there are some devices that will not connect properly when Autonegotiation is enabled on both ends.
- When using Autonegotiation, always have the most recent Network Interface Card (NIC) driver from the manufacturer.

2.2.3.4 Quality of Service

Differentiated Services (DiffServ) is the industry and Nortel standard for the implementation of Quality of Service (QoS). DiffServ provides QoS on a per hop behavior of the Ethernet switches by marking the header of individual packets with a DiffServ Code Point (DSCP). This DSCP then provides an indication to the Ethernet switch as to the priority of each packet and into which queue the packet should be placed. Please 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.

Whether QoS needs to be deployed in the network depends on the applications and the business-critical nature of those applications. In order to deploy an effective QoS strategy within the Enterprise, it is imperative to understand the types of applications and the traffic patterns. For most installations, QoS is required for an IP Telephony deployment or any other application that is time/delay sensitive (e.g., video conferencing). QoS can also be employed for mission-critical applications such as Enterprise Resource Planning (ERP) tools. It is not necessary to provide QoS for every application on the network, only those that require special treatment. Most applications function fine in a best effort environment.

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 now have the ability to set their own DSCP and thus set their own priority across the network. For example, the i200x phones set their DSCP to Expedited Forwarding, which maps into the Premium Service Class queue.

Care should be taken 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. This can be accomplished 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).

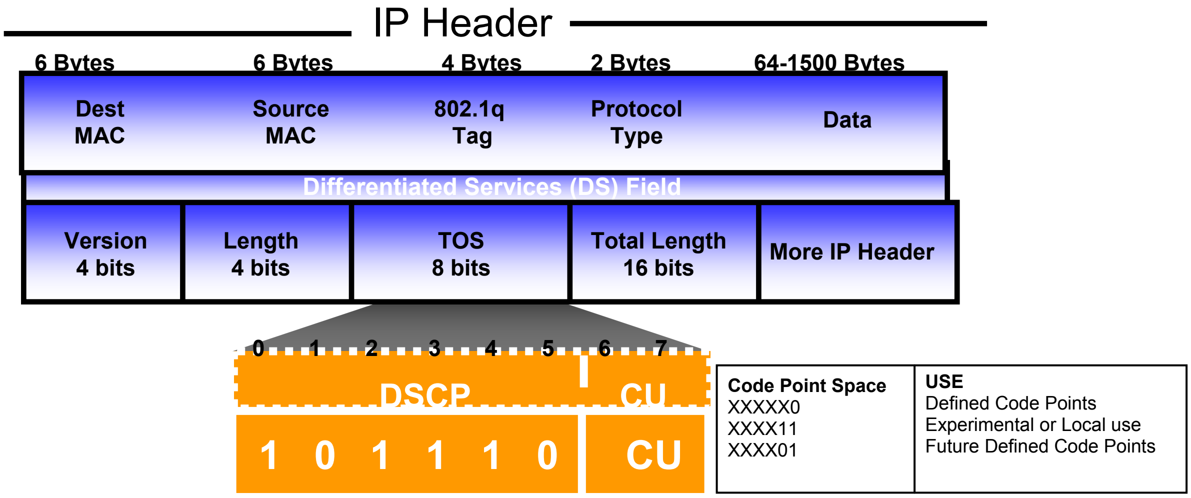
To assist in qualifying these types of applications and the associated QoS levels, Nortel has created a QoS matrix and has standardized Nortel Service Classes across all platforms. This matrix is intended as a guideline for the implementation of QoS:

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 DNS, DHCP, BootP, high priority OAM	Low	Low	N/A
Premium	VoIP, T.38 Fax over IP, Lawful Intercept, CES Real-time VPN service (CIR > 0, EIR = 0)	Very Low	Very Low	Very Low
Platinum	Video Conferencing, Interactive Gaming Real-time VPN service (CIR > 0, EIR > 0)	Low	Low	Low
Gold	Streaming audio, video on demand Broadcast TV, video surveillance	Low-Med	Med-High	High
Silver	SNA terminal to host transactions Credit card transactions, wire transfers Instant Messaging Low Loss/Delay Data VPN service (CIR > 0, EIR > 0)	Low	Low-Med	N/A
Bronze	E-mail Non-time-critical OAM&P	Low	Med-High	N/A
Standard	Best effort applications Best effort VPN (CIR >= 0, EIR > 0)	Med	High	N/A

Table 1: Quality of Service Matrix

The following highlights the IP header/DSCP and the DSCP/ToS/IP precedence mapping to the Nortel Service Classes. There are 64 possible different DSCP markings that can be utilized for QoS in the network, along with four different per hop behaviors:

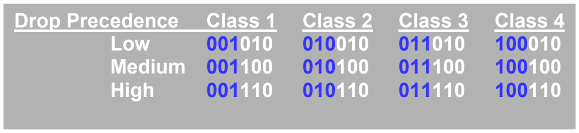
- Expedited Forwarding – voice services
- Assured Forwarding – real-time and non-real-time applications
- Class Selector – used to support legacy routers
- Default Forwarding – best effort



Code Point Space	USE
XXXXX0	Defined Code Points
XXXX11	Experimental or Local use
XXXX01	Future Defined Code Points

DSCP Marking

Differentiated Services Code Point – Six bits of the DS field are used to select the per hop behavior that packet experiences at each node. There are 64 possible code points.



Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
Medium	001100	010100	011100	100100
High	001110	010110	011110	100110

Figure 4: IP Header – DSCP Definition

Table 2 depicts the Nortel mapping of DSCP, Type of Service (ToS), and IP precedence to the Nortel Service Classes, along with their mapping into the DSCP per hop behavior.

DSCP	TOS	IP Precedence	Binary	NNSC	PHB
0x0	0x0	0	000000 **00**	Standard	CS0
0x0	0x0	-	000000 **00**		DE
0x8	0x20	1	001000 **00**	Bronze	CS1
0xA	0x28	-	001010 **00**		AF11
0x10	0x40	2	010000 **00**	Silver	CS2
0x12	0x48	-	010010 **00**		AF21
0x18	0x60	3	011000 **00**	Gold	CS3
0x1A	0x68	-	011010 **00**		AF31
0x20	0x80	4	100000 **00**	Platinum	CS4
0x22	0x88	-	100010 **00**		AF41
0x28	0xA0	5	101000 **00**	Premium	CS5
0x2E	0xB8	-	101110 **00**		EF
0x30	0xC0	6	110000 **00**	Network	CS6
0x38	0xE0	7	111000 **00**	Critical	CS7
DSCP and TOS are in HEX IP Precedence in decimal NNSC: Nortel Networks Service Class					PHB: Per Hop Behavior

Table 2: Default Nortel DSCP/ToS/IP Mapping

2.2.3.4.1 Design Recommendation

- Utilize a consistent QoS implementation end to end in the network.
- The edge switches can either mark or honor the DSCP, and the core of the network strictly honors markings from the edge of the network.
- Do not put multiple applications into the same QoS category, but delineate between applications for priority treatment.
- The switches also have the ability to automatically map 802.1p to Diffserv. This is very beneficial in environments in which there is a mix of equipment and capabilities. Switches that do not support Diffserv, but do support 802.1p, can actively participate in the end-to-end QoS implementation, helping to ensure a consistent QoS deployment.

2.2.3.5 Multicast at Layer 2

The multicast protocol distributes traffic to all subscribers of a multicast group. There are features within the Ethernet switching platforms that make efficient use of the bandwidth available to multicast traffic.

- IGMP Snooping
  The Nortel Ethernet switches can sense IGMP (Internet Group Multicast Protocol) host membership requests for each specific multicast group. Only host ports requesting a multicast stream receive that stream; the switch automatically prunes the other ports and does not send multicast traffic to hosts that did not request it, thus making efficient use of the available bandwidth to each of the hosts on the switch.
- IGMP Proxy
  The Nortel Ethernet switch provides a single proxy report upstream for all members within the same multicast group on the same switch/stack. By consolidating all the IGMP host membership requests into a single request, the switch does not flood the network needlessly with multiple copies of the same request. IGMP Snooping must be enabled for this feature to work.
- IGMP Static Router Port
  This feature allows unknown multicast traffic to be forwarded only to the statically defined multicast router port. The traffic will not be flooded to all ports and will not be sent to dynamically learned multicast router ports. Static router ports have two main purposes: to get (1) multicast traffic and (2) IGMP reports to multicast routers that may not be discoverable through passive detection; for example, when there are two queriers and one is elected and the other becomes silent (per the IGMP standard).

If IGMP Snooping/Proxy is not enabled, multicast traffic is flooded to all ports on the switch that are in the same VLAN.

2.2.3.5.1 Design Recommendation

- If multicast will be used in the network, enable both IGMP Snooping and Proxy on the edge switches.
- If multicast is not being used on the network, disable IGMP Snooping and Proxy on the edge switches.
- Presently, the Nortel Ethernet edge switches support both IGMP v1 and IGMP v2. All devices on the network that are participating in multicast must be running the same version of IGMP.
- Use IGMP Static router ports when multiple IGMP queriers are present and on different ports.

- Flooding unknown multicast traffic is a behavior that is configurable (on or off) on the Ethernet edge switches. The "vlan igmp unknown-mcast-no-flood" command provides this functionality. Turning off flooding ensures that static router ports become the destination of unknown multicast traffic.

2.2.3.6 End Station Authentication

There are several methods for authenticating end stations on the network. The two most popular methods are MAC-based authentication and 802.1x authentication. Both of these methods allow access to the network after authentication has been completed. This helps to ensure only registered users and devices are on the network. A variation of 802.1x allows for the configuration of a guest VLAN, which allows non-authenticated users on the network, but also allows the administrator to control what the guest VLAN users can access.

Authentication Options

- Destination Address (DA) MAC
  - DA provides the ability to drop all packets with a specific destination MAC address.
- MAC Based (Local or Centralized Authentication)
  - Local Authentication

    The MAC Address Security feature allows the administrator to specify a list of MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list.
  - Auto-learning or Static Authentication
    - Auto-learning allows a switch to automatically add a MAC address to the MAC security table without user intervention. You can also limit the number of MAC addresses allowed.
    - Static authentication allows the manual creation of static MAC entries on a per port basis.
  - Centralized Authentication

    This feature functions the same way as local authentication; however, the list of allowed MAC addresses is stored in a RADIUS server. This is a much more manageable approach to MAC security.
- 802.1x Extensible Authentication over LAN (EAPoL)
  - Single Host Single Authentication (SHSA)

    For an EAP-enabled port with SHSA, at any time only one MAC user is authenticated on a 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 for traffic.
  - 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 must complete EAP authentication to enable the port to allow traffic from the corresponding MAC address. Only traffic from the authorized hosts is allowed on that port.

- Multiple Host Single Authentication (MHSA)

  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.

- Guest VLAN

  Allows users connected on EAPoL-enabled ports access to a guest network (with restricted access until the port is authenticated). This feature allows network access to users through the guest VLAN.

2.2.3.6.1 Design Recommendation

There are many different scenarios for the authentication of end users and no one option is necessarily the best. The implementation of end user authentication and the method used is strictly dependent upon the desired level of security on the network, the capabilities of the end stations, and the network access privileges to be granted network users. Table 3 indicates the authentication features and interactions on the various Ethernet switching platforms.

Nortel Supported LAN Switching Security Features

Authentication Features	**ES 460/470**	**ERS 5500**	**ERS 8300**	**ERS 8600**
BaySecure	Yes	Yes	Yes	Yes
RADIUS Authentication	Yes	Yes	Yes	Yes
RADIUS Accounting (CLI and SNMP)	No	No	No	Yes
802.1x Extensible Authentication (EAP) - (SHSA)	Yes	Yes	Yes	Yes
Multiple EAP Authentication per port (MHMA)	Yes	Yes	Yes	POI
Guest Login with EAP enabled on port - (GVLAN-SHSA)	Yes	Yes	Yes	POI
Multiple Host Single EAP Authentication - EAP + GVLAN (MHSA)	POR	POR	POR	POI
MAC based EAP Authentication (Clientless EAP)	POI	POI	Yes	POI
MAC Limitation per port	Yes	POI	Yes	Yes
User Based Policy Support	Yes	Yes	Yes	Yes
Tagged/Untagged				
Per VLAN Egress Tagging	Yes	Yes	Yes	Yes
Tagged and untagged per port	Yes	Yes	Yes	Yes
Tagging with EAP	Yes	Yes	POR	No

Table 3: Supported Authentication Features

2.2.3.7 Power over Ethernet

The use of Power over Ethernet (PoE) has become increasingly popular over the past few years and now has been 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, in which legacy-based (prestandard) PoE devices use a capacitive discovery mechanism. Power can be provided over the used pairs or unused pairs in a UTP copper cable.

When designing a Converged Campus network, it is imperative to understand the PoE requirements in order to provide adequate power to the end devices. The 802.3af standard requires a maximum of 15.4 watts per device, with many devices using only 4 to 8 watts. The standard also defines different classes of detection, as defined in Table 4:

Class	Usage	Maximum power level with 100 m cable of Cat 5 at	
		Output of 8348TX-PWR	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

Table 4: PoE Classes of Power Input/output

- Four classes of DC detection (Classes 0, 1, 2 and 3) per IEEE 802.3af
- Four classes of AC detection (Classes 0, 1, 2 and 3) per IEEE 802.3af
- One class of Capacitive detection (Class 2) for pre-IEEE Nortel IP phones

When designing the network, take into consideration the potential number of end devices requiring PoE and the amount of power each of these devices requires. This will help you decide on the number of PoE-capable ports required in the wiring closet. You can enable or disable power control on a per port/module basis with the Power Management feature, thereby limiting the amount of power per port/module.

Another critical aspect of PoE is redundant power in the wiring closet. When you rely on the Ethernet switches to provide power to the end devices, it becomes even more necessary to have redundant power available in the closet in case of an electrical circuit failure. The addition of redundant power can also be used by the Ethernet switches to add overall power capability and increase the total amount of power available for end devices using PoE.

In all cases, Nortel strongly recommends that you have separate electrical circuits available in the closet for the various AC feeds into the Ethernet switching equipment as well as the Redundant Power Supply Units (if applicable).

2.2.3.7.1 Design Recommendation

The design of a network capable of PoE will have several variations depending on the Ethernet switching equipment that is chosen. The following highlights recommendations based on these different switching options:

- ERS 8300

  This chassis system provides 48 port I/O modules capable of PoE. When utilizing the PoE feature, make sure to engineer the power requirements of the chassis properly. The amount of PoE power required will dictate the type of input power the chassis will require. The ERS 8300 provides various options for input power as indicated in Table 5.

  The amount of PoE per module is configurable up to 800 watts per module, along with the ability to specify port priority for PoE.

Power Supply	Power Supply Rating	# of Power Supplies	Redundancy	PoE Available
8301AC	110-120 VAC 20 Amp 1140 watts	1	No	450 watts
		2	Yes 1+1	450 watts
		3	Yes 2+1	900 watts
	200-240 VAC 20 Amp 1770 watts	1	No	900 watts
		2	Yes 1+1	900 watts
		3	Yes 2+1	1800 watts
8302AC	100-120 VAC 15 Amp 850 watts	1	No	225 watts
		2	Yes 1+1	225 watts
		3	Yes 2+1	450 watts
	200-240 VAC 15 Amp 1400 watts	1	No	450 watts
		2	Yes 1+1	450 watts
		3	Yes 2+1	900 watts

Table 5: ERS 8300 Power over Ethernet Options

- ERS 5520

  This stackable Ethernet switch is available in both a 24-port and a 48-port version. When utilizing the PoE feature, make sure to engineer the power requirements for the switch/stack properly. The ERS 5520 provides up to 320 watts per switch on standard 110 VAC power. To provide more power and redundant power, use the ERS Redundant Power Supply 15 (RPS 15) to augment the ERS 5520. The RPS 15 can support up to three ERS 5520 switches. The available configurations for the various power options are specified in Table 6.

Switch Model	PoE on Standard AC	RPS 15 Power Sharing	RPS 15 RPSU
ERS 5520-24T-PWR	320 watts	370 watts	320 watts
ERS 5520-48T-PWR	320 watts	740 watts	320 watts

Table 6: ERS 5520 Power over Ethernet Options

- ES 460

  This stackable Ethernet switch is available in a 24-port version. When utilizing the PoE feature, make sure to engineer the power requirements for the switch/stack properly. The ES 460 provides up to 200 watts per switch on standard 110 VAC power. To provide more power or redundant power, use the BayStack 10 RPSU to augment the ES 460. The available configurations for the various power options are specified in Table 7.

Switch Model	PoE on Standard AC	BS 10 Power Sharing	BS 10 UPS	BS 10 RPSU
ES 460-24T-PWR	200 watts	235 watts	200 watts for up to 15 minutes	75 watts

Table 7: ES 460 Power over Ethernet Options

- Power over Ethernet Devices

Table 8 highlights the PoE requirements of several Nortel end devices.

PoE Device	Normal Load Power Consumption	Heavy Load Power Consumption
Phase 0 Phones		
i2004 phone	3 watts	3 watts
i2004 phone with external 3 port switch	10 watts	10 watts
Phase I Phones		
i2004 phone	3 watts	3 watts
i2002 phone	3 watts	3 watts
Phase II Phones		
i2001 phone with integrated switch	4.5 watts	8.0 watts
i2002 phone with integrated switch	4.5 watts	8.0 watts
i2004 phone with integrated switch	4.5 watts	8.0 watts
i2007 phone with integrated switch	8.0 watts	13.0 watts
IP Audio Conference Phone 2033	7.4 watts	10.5 watts
WLAN 2230 AP	10 watts	10 watts
WLAN 2330 AP	10 watts	10 watts

Table 8: Power over Ethernet Consumption

2.2.4 Edge Switching – Uplink Resiliency

The previous sections evaluated chassis versus stackable and explored the key features to consider for end station connectivity. This section looks at uplink resiliency from the wiring closet to the core or distribution layer, specifically:

- Layer 2 versus Layer 3 at the Edge
- Use of Distributed MultiLink Trunking on Edge Switching Platforms
- Physical Layer Considerations/Fiber Fault Detection
- Split MultiLink Trunking to the Core/Distribution
- LACP/VLACP

2.2.4.1 Layer 2 versus Layer 3 at the Edge

The process of choosing between Layer 2 and Layer 3 at the edge can take many different twists. When considering the differences between the two, it is imperative to keep in mind the end goal of 99.999 percent network availability. There are several ways to design a Converged Campus network. The goal is to design a network that provides high reliability, fast convergence, and yields the lowest possible total cost of ownership (TCO). The TCO is derived by adding the initial cost of equipment/installation (Capex – Capital Expenditures) and the ongoing administration and support of the network (Opex – Operating Expenditures). Over the long run, the Opex is often higher than the Capex, so our goal is to help reduce Opex by making the network easy to administer and troubleshoot.

The two major areas to consider when deciding between Layer 2 and Layer 3 at the edge are (1) IP routing and (2) intelligence, which can be thought of as operating at Layers 3 to 7. Intelligence can further be defined as the ability to provide traffic management (Qos and content-aware switching) and security, which includes end user authentication and policy enforcement. The goal is to centralize the routing and distribute the intelligence to provide a high-performing and secure network along with easy and simplified management. However, one must also consider the number of users being aggregated. The ability to distribute ARP tables across the network may prove a more efficient design. There are no absolute numbers to tell you whether your network should centralize all routing or distribute the routing, but guidelines are provided in the design recommendations below.

A Layer 2 edge solution, when combined with a strong distributed intelligence features, is easier to implement, administer, and troubleshoot. In addition, subsecond failover and no penalties on performance make Layer 2 the clearly superior choice in the Converged Campus design.

Nortel, however, recognizes that a Layer 2 solution is not always possible or may not fit every network design. The Nortel edge switch portfolio includes products that support a Layer 3 edge into a Layer 3 core/distribution. There are no performance penalties for implementing Layer 3 at the edge. The switches provide outstanding performance whether implemented as Layer 2 or Layer 3. The main difference is seen in the complexity of laying out the Layer 3 design and the ongoing administration and troubleshooting of such a network.

In summary, Nortel provides the flexibility for both approaches. Some customers choose a Layer 3 edge design solution for various reasons – no VLAN propagation, same configuration replicated, smaller broadcast domains, security/access control lists (ACL), for example – and they have the necessary routing expertise to support such a network. Other customers prefer a centralized routing and filtering/ACL approach, which may reduce the overall complexity of the network administration by not distributing Layer 3 throughout the network.

2.2.4.1.1 Design Recommendation

Nortel provides the flexibility to deploy either a Layer 2 or Layer 3 edge solution. As common practice, the recommendation is to deploy Layer 2 at the edge whenever possible. A Layer 2 edge coupled with Quality of Service implemented on a resilient architecture using Split MultiLink trunking and Switch Clustering provides the most resilience, highest performance, and overall lowest TCO possible.

As a general rule, If aggregating less than 3000 users into the core, use Layer 2 between the access and distribution/core, and if aggregating more than 3000 users, use Layer 3 between the access and distribution/core – this will help to distribute ARP tables, simplify subnet provisioning, and, with RSMLT (covered later in this document), allows the extension of Layer 2 VLANs across multiple access switches.

2.2.4.2 Distributed MultiLink Trunking

In order to increase both resiliency and bandwidth from the edge switching platform, Distributed MultiLink Trunking (DMLT) is always a major design consideration. MultiLink Trunking (MLT) itself provides the ability to group multiple physical links into a single logical link (see Table 9 for the specific number of links and groups per switch/stack). This automatically increases bandwidth from the wiring closet by utilizing all the physical links in a logical group. A failure in any of those physical links results in automatic failover of the traffic to the remaining links in subsecond time. After the failed link has been repaired, recovery of that link back into the MLT group is also accomplished in subsecond time.

Switch	Links per Group	Groups per Switch/Stack
ERS 8600	8	32
ERS 8300	4	31*
ERS 5500	4	6
ES 460/470	4	6

* Up to seven Fast Ethernet groups and/or 31 Gigabit groups.

Note: Some of these limitations will change with future software releases.

Table 9: MLT Scaling (links/groups)

By adding the ability to terminate these physical links on different switches within a stack or on different modules within a chassis (known as Distributed Multilink Trunking), we now have increased the resiliency of the uplinks out of the wiring closet. A failure of the switch or module at which one of these physical links terminates will not cut off communication from the wiring closet to the core/distribution.

MLT, DMLT, and SMLT all use a hashing algorithm that distributes traffic across the physical links of the logical trunk. Traffic is distributed on a per session basis, so packets never arrive at the destination out of order. The hashing algorithm does not necessarily have to match on both ends of the link, and therefore, MLT/DMLT/SMLT is interoperable with most third-party vendors (both switches and server NICs). As a general rule, the algorithms are based on source and destination MAC or source and destination IP address. The specific traffic distribution algorithms are as follows:

ERS 8600

- For any bridged packet (except IP), the distribution is based on source and destination MAC:
  - MOD (DestMAC[5:0] XOR SrcMAC[5:0], number of active links)
- For bridged and routed IP or routed IPX, the distribution is based on source and destination IP address:
  - MOD (DestIP(X)[5:0] XOR SrcIP(X)[5:0], number of active links)
- Multicast flow distribution over MLT is based on source-subnet and group addresses. To determine the port for a particular Source, Group (S,G) pair, the number of active ports of the MLT is used to MOD the number generated by the XOR of each byte of the masked group address with the masked source address. This feature was introduced in release

3.5. The feature is not enabled by default and must be enabled in order for IP multicast streams to be distributed.

ERS 8300

- For any bridged packet (except IP), the distribution is based on source and destination MAC:
  - MAC_Hash[6:0] = (MAC_SA[6:0]) XOR (MAC_DA[6:0])
  - L2_Unicast_Trunk_dist_Index[2:0] = The Sum of MAC_Hash bits (MAC_Hash[6] + MAC_Hash[5] + MAC_Hash[4] + MAC_Hash[3] + MAC_Hash[2] + AC_Hash[1] + MAC_Hash[0])
- For bridged and routed IP or routed IPX, the distribution is based on source and destination IP address:
  - If packet is routed and Layer 3 protocol for hash is enabled, then
    - L3_Prot_For_Hash[6:0] <= Pkt's L3 Protocol[6:0]
  - Otherwise
    - L3_Prot_For_Hash[6:0] <= 7'b0
  - L3_Hash[6:0]=(SIP[6:0])XOR(SIP[22:16])XOR(DIP[6:0])XOR(DIP[222:16])XOR (L3_Prot_For_Hash[6:0])
  - L3_Unicast_Trunk_dist_Index[2:0] = The Sum of L3_Hash bits (L3_Hash[6] + L3_Hash[5] + L3_Hash[4] + L3_Hash[3] + L3_Hash[2] + L3Hash[1] + L3_Hash[0])
- For any Layer 2 multicast/unknown unicast/broadcast:
  - V[3:0] = (Unk_V[11:8]) XOR(Unk_V[7:4])XOR(Unk_V[3:0])
  - Unk_Trunk_Dist_Index[3:0] = (Src_Port[3:0])XOR(Src_Dev[3:0])XOR ({1'b0,Src_Dev[6:4]})XOR({Src_Port[5:4],2'd0})XOR(Unk_V[3:0])
- For any registered multicast (source port, source device, VID, VIDX):
  - Reg V[11:0] = VID[11:0] XOR (VIDX[0:11) - (This is VID[11:0]XOR with VIDX[11:0] flipped)
  - V[3:0] = (Reg_V[11:8])XOR (Reg_V[7:4])XOR(Reg_V[3:0])
  - Reg_Trunk_Dist_Index[3:0] = (Src_Port[3:0])XOR(Src_Dev[3:0])XOR ({1'b0,Src_Dev[6:4]})XOR({Src_Port[5:4],2'd0})XOR(Unk_V[3:0])

ERS 5500

- The link selection algorithm uses a combination of the source and destination MACs in assigning traffic to a specific link of the MLT.
  - (Least 3 bits SRC MAC XOR Least 3 bits DST MAC) MOD Active Trunk Links
  - The link selection algorithm is applied to unicast traffic when both source and destination MAC addresses have been learned by the system. For broadcast, unknown unicast, and multicast traffic, only a single link is selected (currently the lowest link) for packet transmission.

ES 460/470

- The distribution of data frames is based on a round robin algorithm. In general, traffic received on a port is directed to the first trunk link. Traffic received on another port is directed to the second trunk link. In order to avoid out-of-order packets, the distribution algorithm always selects the same egress path for all packets coming from the same ingress port.
- Each active port is assigned a port index number from 0 to 3 in the order it comes online. Note that the first active port and the fifth active port share the same port index number.
- In the stack environment, if the ingress port and the trunk port are on the same switch, the local trunk port is selected. If the ingress port and the trunk port are not on the same switch, the selection logic is the same as that of MLT.

2.2.4.2.1 Design Recommendation

The uplinks out of a wiring closet must utilize DMLT whenever possible by terminating each of the separate physical links on different switches within the stack or different modules within the chassis.

- All links in an MLT group must be of the same speed and duplex – Nortel does not support the mixing of different speed links within the same MLT group.
- Nortel recommends that all links within the MLT group be of the same media type (1000BaseT, 1000BaseSX, 1000BaseLX, etc.).
- Nortel recommends that you disable Spanning Tree protocol on the MLT/DMLT group and ports on both the edge and the core/distribution. This is absolutely required when using Split MultiLink Trunking (SMLT) on the core/distribution layer.

2.2.4.3 Physical Layer Considerations/Fiber Fault Detection

Nortel provides several options for uplink connectivity over fiber – this does not necessarily preclude the use of copper for uplink connections; however, due to the distance limitations of copper (100 m), fiber is normally the media of choice. Both ends of a link generally must use the same transceiver type (that is, SX to SX), but they do not necessarily have to be from the same manufacturer or vendor – Nortel GBICs, SFPs, XFPs interoperate with most all third-party vendors' products of the same transceiver type.

Nortel also supports the interoperability of CWDM with both XD and ZX SFPs. More specifically, one end of the link can use a ZX SFP and the other end of the link a CWDM SFP, or one end can use an XD SFP and the other end of the link a CWDM SFP. The following rules apply:

- XD GBIC with 40 Km CWDM SFP
- ZX GBIC with 70 Km CWDM SFP

Table 10 provides a brief description of the various options and distances supported.

Transceiver	Speed	Fiber Type	Wavelength	Minimum Range	Maximum Suggested Range
1000SX	1 Gigabit	MMF – 62.5µ	850 nm	2-275 m	1.0 km
1000SX	1 Gigabit	MMF – 50µ	850 nm	2-550 m	1.0 km
1000LX *	1 Gigabit	MMF – 62.5µ	1310 nm	2-550 m	8.5 km
1000LX *	1 Gigabit	MMF – 50µ	1310 nm	2-550 m	8.5 km
1000LX	1 Gigabit	SMF – 9µ	1310 nm	2m-10 km	32.0 km
1000XD	1 Gigabit	SMF – 9µ	1550 nm	See Note	50.0 km
1000ZX	1 Gigabit	SMF – 9µ	1550 nm	See Note	70.0 km
CWDM	1 Gigabit	SMF – 9µ	1470-1610 nm	See Note	See Note
10GBase-SR	10 Gigabit	MMF – 62.5µ	850 nm	220 m	220 m
10GBase-SR	10 Gigabit	MMF – 50µ	850 nm	300 m	300 m
10GBase-LR/LW	10 Gigabit	SMF – 9µ	1310 nm	10 km	10 km
10GBase-ER/EW	10 Gigabit	SMF – 9µ	1550 nm	40 km	40 km

* LX over MMF may require mode conditioning patch cables (single mode/multimode hybrid)

Notes:

1000XD GBIC – if range is less than 25 km, use a 5 dB in-line attenuator

1000ZX GBIC – if range is less than 25 km, use a 10 dB in-line attenuator, and if range is less than 50 km, use a 5 dB in-line attenuator

CWDM ranges vary with the SFP or GBIC that is used. Two versions of SFP are available (40 km and 70 km) and one version of GBIC (120 km). Please refer to product documentation for optical specifications and possible maximum ranges for CWDM.

Table 10: GBIC/SFP Specifications

It is imperative to preserve the integrity of the uplinks from the edge closet to the core/distribution layer. In the case of a single fiber fault – either the transmit or the receive – the link must be automatically disabled at both ends. If this does not happen, data could be passed to a port that is not operating properly, and that data would be lost. This issue can cause severe performance degradation and eventually render the network inoperable. To protect the network, it is important to properly enable some form of single fiber fault detection on all uplink ports.

2.2.4.3.1 Design Recommendation

All uplink ports should be configured with a method to detect a single fiber fault and disable the affected ports. There are two options for enabling this feature, depending on the switching platform being utilized at the edge:

- Switches supporting Autonegotiation on the uplink ports (ERS 5500, ERS 8300) should have that feature enabled on both ends of the uplink.

    - On the Gigabit ports, Remote Fault Identification (RFI) is enabled by using Autonegotiation. RFI removes the link from a port in the event of a single fiber fault on the link connected to that port.
    - On 100 Mbps ports, Far End Fault Identification (FEFI) is enabled by using Autonegotiation. FEFI removes the link from a port in the event of a single fiber fault on the link connected to that port.
- Switches that do not support Autonegotiation on the uplink ports (ES 460, ES 470) should have the Single Fiber Fault Detection (SFFD) feature enabled on both ends of the uplink. SFFD was designed to perform the same function as RFI (described above) by removing the link from a port in the event of a single fiber fault – normal failover times for SFFD range from 8 to 60 seconds.

Review the fiber requirements of the network and select the appropriate GBIC/SFP/XFP based on those fiber specifications.

- Utilize CWDM for long haul connections – those that are greater than what is supported by LX.
    - CWDM wavelengths must match on both ends of a link
    - Interoperability between CWDM and XD/ZX is supported (see above rules)

In certain scenarios where the SMLT link may span across a providers LAN extension service, detecting a link failure in the LAN extension core will not work using RFI or even SFFD. RFI/SFFD will not work end to end between a pair of Nortel switches because RFI/SFFD only works between direct connections between a pair of switches. Hence, if there is a failure in the LAN extension core, the link on both Nortel switches will still be running. To solve this problem, enable VLACP on the Nortel switches. The VLACP protocol is forwarded between the Nortel switches. If the switch does not receive any VLACP updates, a link will be declared out-of-service and SMLT will forward traffic through another working link. A detailed discussion of VLACP is covered in an upcoming section. If the intermediate devices are Nortel OpTera 5200s, they will flag far end link failures and disable the local interface without the need for VLACP.

2.2.4.4 Split MultiLink Trunking/Switch Clustering

The Split MultiLink Trunking (SMLT) technology has added industry-leading resiliency to the Converged Campus design. This technology allows for dual homing of multiple links from the edge closet in an N-1 redundancy technique – all links active and passing traffic simultaneously. In the event of a link, switch, or module failure, SMLT provides subsecond failover and recovery. The advent of SMLT makes obsolete the need for Spanning Tree protocol and its complexity.

In SMLT, the aggregation switches (core/distribution) appear as one logical device to the dual homed edge switch. All the intelligence of SMLT rests in these aggregation switches and therefore, SMLT is edge switch agnostic – meaning that any edge switch that supports link aggregation can tie into an SMLT core/distribution. The aggregation switches make use of an Inter Switch Trunk (IST) to exchange topology information, permitting rapid fault detection and forwarding path modification.

There are different configuration options for SMLT, which are covered in the Core Switching section of this document.

2.2.4.4.1 Design Recommendation

All edge closets should be dual homed and use SMLT between the edge and core/distribution. On the edge switch, follow the design recommendation for Distributed Multilink Trunking, as no SMLT-specific configuration is necessary. Note that Spanning Tree must be disabled on the ports participating in the SMLT; failure to do so can cause unexpected traffic behavior.

2.2.4.5 LACP/VLACP

The IEEE 802.3ad is the specification for link aggregation. The major difference between 802.3ad and MLT is that MLT is statically defined, while 802.3ad is dynamic and can provide some additional features. The standard defines the Link Aggregation Control Protocol (LACP), which is used to manage switch ports and their memberships in link aggregation groups.

A function of LACP is to use peer exchanges across the links in an aggregation group to determine, on an ongoing basis, the aggregation capability of the various links, and continuously provide the maximum level of aggregation capability achievable between a pair of switches.

The added functionality of end-to-end checking is a resiliency feature that should be used within a Converged Campus design. Because MLT is statically defined, there is no mechanism for checking between directly connected switches. In the rare event that a switch may become inoperable but the link status remains up, data could be inadvertently sent to that switch, causing it to be lost. A checking mechanism automatically removes that port from the aggregation group, ensuring data is not sent to an inoperable switch, and therefore ensuring no data loss.

There are limitations to the LACP implementation on the ERS 8600 that must be considered:

- LACP was designed to operate between two directly connected switches and will not work in an end-to-end fashion if there are any intermediary devices (Optical ring, Service Provider Network, etc.).
- LACP supports a maximum of 32 link aggregation groups.
- LACP supports up to 32 MLT-based SMLT groups.
- LACP supports up to 32 port-based SMLT groups.

Due to the limitations of LACP, Nortel has developed an extension to LACP called Virtual LACP (VLACP) that provides a true end-to-end failure detection mechanism. This feature now adds a greater level of resiliency and flexibility to the Converged Campus design when used in conjunction with SMLT, especially in the cases in which switches are not directly attached to each other. When comparing LACP to VLACP, there are several differences that may come into play during the network design:

- VLACP was designed to operate end to end, regardless of whether the switches are directly connected or have an intermediary connection between them.
- VLACP supports up to 32 MLT or MLT-based SMLT groups.
- VLACP supports up to 383 port-based SMLT groups.

2.2.4.5.1 Design Recommendation

- The use of LACP or VLACP is dependent upon support of these protocols on the various Ethernet switching platforms. Table 11 highlights scalability of these features and availability within the switching platforms.

Switch Model	802.3ad / LACP Support	VLACP Support	LACP-MLT Scaling	LACP-SMLT Scaling	VLACP-SMLT Scaling
ES 460/470	Release 3.1	Release 3.6	6	N/A	N/A
ERS 5500	Release 4.1	Release 5.0 *	6	N/A	N/A
ERS 8300	Release 3.0 *	Release 3.0 *	31 **	N/A	N/A
ERS 8600	Release 3.7	Release 3.7	32	32	64

* Future software release

** Assumes Gigabit risers, supports a maximum of seven MLTs if Fast Ethernet

Table 11: LACP/VLACP Support and Scaling

- All closet uplinks should enable VLACP to ensure added resiliency in the overall network design. It is preferable to use VLACP where possible because VLACP is a much lighter-weight protocol and provides faster failover than LACP (VLACP is subsecond, LACP is 3 to 4 seconds).
- VLACP is not automatically propagated across the trunk members, but must be manually configured on all ports participating in the trunk.
- In cases in which the Ethernet switching platform does not yet support VLACP, use LACP to provide the added resiliency.
- For LACP/VLACP use short timers for faster convergence.
- Ensure that you match polling timers on both ends of the link. Future software releases will continue to improve/reduce the recovery time.
- Use LACP when interoperating between Nortel and third-party switches.
- Use LACP if you want to take advantage of the standard's standby link capability.
    - LACP supports a maximum of eight active links, all other links (nine and above) are put into standby
    - Active/Standby is defined by ActorPortPriority (higher actor priorty = lower port priority)
    - If actor priority is the same, lower MAC = higher priority
- When using LACP, use the same ID number for the ActorAdmin key and MLT ID.
- It is not necessary to run VLACP on LACP trunks – this takes up added CPU resources and does not provide any added benefit.

2.2.5 Core Switching

This section on core switching is broken into two subsections – the first dealing with a two tier architecture, the second dealing with a three tier architecture. The core switching or distribution layer switching is one of the most critical components of the overall Converged Campus design. The core/distribution must exhibit the following characteristics:

- Highly resilient design with no single point of failure
- Secure architecture built into the switching platform
- Non-blocking architecture to ensure the highest possible performance

- Quality of Service capable with granularity and scalability in filtering

In conjunction with these items, this guide highlights the specific items that must be taken into consideration when designing the Converged Campus – whether the design uses a two tier or three tier architecture, the design considerations remain quite similar:

- Platform redundancy
- Deploy SMLT/RSMLT technology between

  Core and Edge

  Distribution and Edge

  Core and Distribution
- Layer 2 VLANs (port, protocol, subnet)
- Layer 3 (VRRP, ECMP, RIP, OSPF, BGP, DVMRP, PIM-SM)
- Security features
- Quality of service

2.2.5.1 Two Tier versus Three Tier Architecture

To keep the Converged Campus design as simple as possible, the use of a two tier architecture (edge to core) is usually preferred. The ability for the core to handle edge traffic with non-blocking performance allows this simple deployment option. There are certain situations that dictate the use of a three tier architecture, such as when the existing layout of the fiber plant is designed to support a three tier architecture. In the past, a three tier architecture was commonplace to support traffic flow between workgroups. With the advent of centralization, the amount of traffic that remains within a workgroup is substantially less than that which traverses the backbone headed to the data center or Internet/Intranet. This change makes possible the use of the simple two tier architecture.

The immediate benefit from a two tier architecture comes from the reduced amount of equipment to purchase, engineer, deploy, manage, and maintain. The cost differences between the two architectures can be enormous, depending on the size and scope of the Converged Campus design. The simplification of the overall network is another major advantage of having the two tier architecture. Any reductions in the amount of equipment and the complexity of the network lead to a lower TCO in the long run.

2.2.5.1.1 Design Recommendation

Utilize a simple two tier architecture whenever possible. In order to deploy a two tier architecture in the Converged Campus, the core switching platforms must provide:

- The ability to handle traffic at non-blocking rates
- N-1 resiliency for all connections to the core (closets, data center, DMZ, etc.)
- Scalability both in ports and bandwidth
- Platform redundancy and no single point of failure

Nortel highly recommends that you centralize the routing functionality within the core whenever possible, as discussed in the previous section on Layer 2 versus Layer 3 at the edge.

2.2.5.2 Platform Redundancy

The core switching layer is the most critical component of the Converged Campus design. Also, it is imperative to ensure the most redundancy and resiliency possible. The platforms deployed must provide redundancy in hardware components such as power supplies, fan trays, switch fabric/CPUs, and I/O modules. Providing redundancy in the hardware is the basic building block to create the highly resilient core.

From a software perspective, the ERS 8600 supports High Availability (HA) mode when both Switch Fabric/CPU (SSF/CPU) modules are installed. With HA enabled, both CPUs are active. The CPUs exchange topology data, so in the event of an SSF/CPU failure, the functioning SSF/CPU can continue passing traffic with subsecond recovery.

Depending on the protocols and data exchanged (Layer 2, Layer 3, or platform), the CPUs perform different tasks. This ensures that any time there is a failure, the backup CPU can take precedence with the most recently updated topology data.

Protocol and feature support in HA mode is dependent on the software version. Table 12 highlights these releases and their respective protocol/feature support.

Data Synchronized	Release 3.2	Release 3.3	Release 3.5	Release 4.0	Release 3.7
L1/Port Configuration	Yes	Yes	Yes	Yes	Yes
Syslog	Yes	Yes	Yes	Yes	Yes
RMON	No	No	No	No	3.7.1
L2/VLAN Parameters	Yes	Yes	Yes	Yes	Yes
SMLT	Yes	Yes	Yes	Yes	Yes
802.3ad/802.1x	N/A	N/A	N/A	N/A	Yes
ARP Entries	No	Yes	Yes	Yes	Yes
Static/Default Routes	No	Yes	Yes	Yes	Yes
VRRP	No	No	No	No	Yes
RIP	No	No	No	No	Yes
OSPF	No	No	No	No	Yes
BGP	No	No	No	No	No
Filters	No	No	No	No	Yes
L2 Multicast (IGMP)	Yes	Yes	Yes	Yes	Yes
L3 Multicast	No	No	No	No	No

Table 12: ERS 8600 High Availability Feature Support

2.2.5.2.1 Design Recommendation

Deploy a Resilient Terabit Cluster for the core switching and/or distribution layers of the Converged Campus with the following design considerations:

- Provide N+1 power redundancy to all chassis, utilizing separate electrical circuits for each power supply.

- Provide redundant fan trays for each chassis.
- Provide dual active, redundant switching fabrics/CPUs in each chassis.
- Provide the ability to dual home all connections into the Terabit Cluster.
- Ensure that all modules, power supplies, fan trays are hot-swappable.

Enable HA mode when possible to ensure subsecond failover and recovery in the unlikely event of an SSF/CPU failure. Consider the software releases and protocol/feature support in each. For full support of HA/SMLT, ensure that your ERS 8600 software is at least version 3.7.10.

2.2.5.3 SMLT Deployment

Split MultiLink Trunking (SMLT), as described in a previous section, provides industry-leading technology for the resiliency of the Converged Campus design. SMLT provides the ability to perform virtual hitless upgrades of the core switches (cluster). With all connections to the cluster dually attached, a single core switch can be taken out of service without interrupting end user traffic. This switch then can be upgraded and brought back into service. By performing the same function on the other switch, after the upgraded switch is back online, the entire cluster can be upgraded without taking a service outage and without interrupting any traffic flows on the network.

This section focuses on the various implementation options for SMLT within different parts of the network.

2.2.5.3.1 Two Tier Design – Core to Edge

With the basic two tier design, the edge switches connect directly into the core. In the Converged Campus, the core is a Resilient Terabit Cluster consisting of a minimum of two ERS 8600s with sufficient port density to accommodate dual homing all edge switches. An Inter-Switch Trunk (IST) ties the pair of ERS 8600s together to form the Terabit Cluster. The IST is a critical component of the SMLT and therefore must be highly resilient. The architecture of SMLT and the traffic flow through the cluster is such that there is not a high volume of traffic across the IST, so resiliency of the connection is more important than total bandwidth.

There are different design options to be considered with this deployment in regard to SMLT:

- Port-based SMLT

  The port-based SMLT option allows large-scale deployments of SMLT from a single Terabit Cluster. Every port, save at least two for the IST, can be used for SMLT groups terminating into a cluster, with each SMLT group consisting of two uplinks (one per ERS 8600). For most typical deployments, the ability to have two connections per edge switch/stack is more than sufficient bandwidth, and allows a single cluster to handle many environments. The flexibility of the Nortel edge switch solutions allows for uplinks ranging from 10 Mbps to 10 Gbps (uplinks within the same SMLT group must be of the same media type and link speed).

- MLT-based SMLT

  The MLT-based SMLT option allows for increased scaling of the number of links within a single SMLT group. Up to eight links can be combined into a single SMLT group. These eight links can be spread across the Terabit Cluster – usually in an even dispersion, but this is not an absolute requirement. The Terabit Cluster presently supports up to 31 MLT-based SMLT groups. One MLT group must be used to create the IST between the two ERS 8600s.

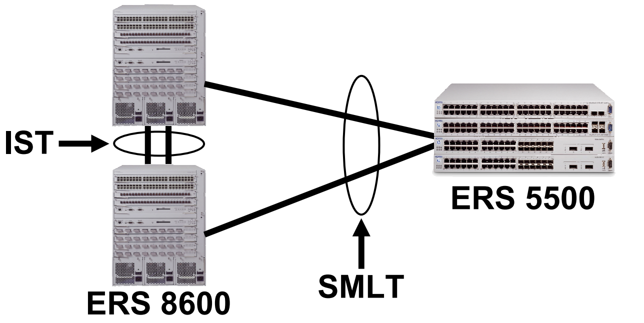


Figure 5: SMLT in a two tier architecture

2.2.5.3.2 Three Tier Design Core to Distribution to Edge

With a three tier design, a distribution layer is inserted between the edge and the core. This is only recommended when the existing fiber plant dictates this requirement. In situations in which three tiers are necessary, we again have options on the deployment of SMLT for resiliency between the layers. The edge to distribution considerations are the same as described in the above section. Between the distribution and core layers, there are different options available based on the architecture deployed:

- Layer 2 between Distribution and Core – SMLT

  In the attempt to centralize routing functionality and distribute the intelligence throughout the network, it is easy to keep a simple Layer 2 architecture between these two layers of the network. In this design, the distribution to core connectivity mimics that of the edge to the core described in the above section. The main difference lies in the ability to fully mesh the distribution to the core. A fully meshed solution provides the highest level of resiliency possible with still maintaining subsecond failover and recovery. A full mesh is not mandatory, but does add resiliency and bandwidth between distribution and core.

- Layer 3 between Distribution and Core – Routed SMLT

  If routing is desired between the distribution and core layers, deploy routed SMLT to maintain subsecond failover and recovery while running a routing protocol such as RIP or OSPF. Routed SMLT builds on the SMLT technology by providing an active-active router concept to SMLT networks with routing enabled on the core VLANs. In the case of a routing switch failure, RSMLT takes care of packet forwarding at Layer 2 while the routing protocol converges at the Layer 3 level. This allows the non-stop forwarding of traffic in the event of any failure with no disruption to the user. Another huge advantage of RSMLT is the ability to extend Layer 2 subnets – something that is not possible if strictly using Layer 3 routing between the core and distribution.

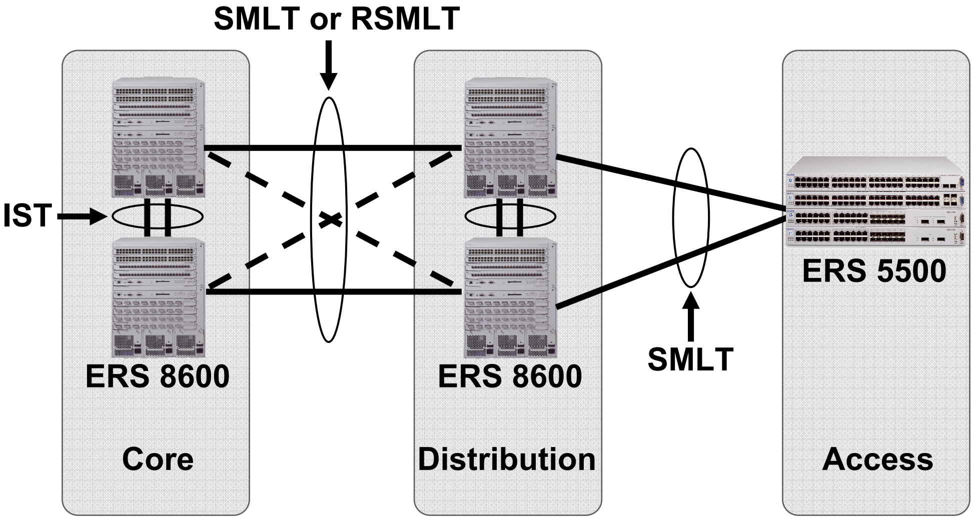


Figure 6: SMLT/RSMLT in a Three Tier Architecture

2.2.5.3.2.1 Design Recommendation

There are several design recommendations when deploying SMLT/RSMLT, whether in a two or three tier architecture. The following design aspects and switch features should be reviewed:

- SMLT automatically disables STP on the participating ERS 8600 ports – make sure to disable STP on the edge switch uplinks.
- For added resiliency, utilize VLACP or LACP on SMLT links whenever possible – do not use LACP on the IST ports.
- Always enable VLACP if there is a LAN extension service used between the core and distribution layer or between the distribution and access layer.
- Make sure that the VLACP timers are set to the same value on both ends of the link. At this time, the lowest common value supported by all platforms is 500 ms when connecting ERS 8600 to ES 460/470. ERS 8600 to ERS 8600 can support lower timer values (400 ms).
- Set LACP/VLACP to use short timers for faster convergence.
- If using MLT-based SMLT, it is a good practice to use the same ID number for the MLT group and the corresponding SMLT group – this is not mandatory for configuration, but it simplifies operation and troubleshooting.
- When configuring an SMLT square (SMLT between two pairs of ERS 8600s), use the same SMLT ID number on both sides of the square – again, for operational simplification.
- Although it is possible to overlap the ID numbers when using MLT-based SMLT and port-based SMLT, Nortel recommends that you avoid this – start port-based SMLT ID numbers at 33, reserving 1 to 32 for MLT-based SMLT.
- Distribute IST connections between different modules in the chassis and utilize lowest port numbers whenever possible – this provides a quicker initialization of the IST between the core switches.
- Create a separate VLAN for the IST and do not enable any Layer 3 protocols on this VLAN.

- Ports assigned to an MLT (IST) are indexed by a number starting at zero (0). The lowest port position (slot 1 port 1 being the lowest) in the chassis for an MLT link is assigned an index of zero. The next MLT link in the second lowest position gets an index of one (1). This index is used by the MLT algorithm to assign a flow over a particular MLT link. Therefore, Nortel recommends that you mate the lowest port position of one MLT link in one chassis with the lowest port position of the corresponding chassis. Mate the second MLT link in the next lowest position in the chassis with the second lowest position in the other chassis. Follow this rule for all successive MLT links. This will help to ensure that the MLT algorithm always resolves a flow over the same link between the two chassis.

- Utilize CP-limit as follows:
  - Enable on all SMLT ports in the distribution/core.
  - Disable for all ports in the IST – ports participating in the IST should never be shut down under any circumstance.
  - In multi-tiered core environments, Nortel recommends that edge closet switches have CP-limit values less than the values used on the core links. This way, if an offending device does transmit malicious traffic, the edge switches will get triggered because of lower values, thus preventing the important core links from shutting down. This will also aid in isolating problems.
  - For edge and server connected ports, if the connected device is determined to produce traffic to the levels for which CP-limit is configured, the connected port will be disabled when it starts transmitting. Thus the traffic must be baselined so that the default values can be adjusted to the required needs. Refer to Table 13 for recommended values.

Recommended CP-Limit Values		
	Broadcast	Multicast
Severe		
Workstation	1000	1000
Server	2500	2500
Non-IST Interconnection	7500	7500
Moderate		
Workstation	2500	2500
Server	5000	5000
Non-IST Interconnection	9000	9000
Relaxed		
Workstation	4000	4000
Server	7000	7000
Non-IST Interconnection	10000	10000

Table 13: CP-Limit Recommended Values

CAUTION - Altering CP-limit values from their defaults during normal network operation can cause the links to become disabled. Nortel strongly recommends that you get a baseline of the network traffic across the uplinks, choose the right value, and apply.

- Enable Loop Detect on SMLT ports for added protection – do not enable Loop Detect on the IST ports. Be sure to enable Loop Detect with the action of port down as opposed to the action of VLAN down. This feature disables the port where a MAC incorrectly shows up (looping port) due to MAC flapping between the correct port and the looping port.

- If the uplinks are 802.1Q tagged, ensure that Discard Untagged Frames is enabled on those uplink ports in the ERS 8600. This prevents inadvertent connections to the core that could potentially cause loops or unexpected traffic flows.
- Verify that all VLANs tagged on one end of the IST and SMLT are also available and configured on the other end of the IST.
- Although it is not recommended, the ERS 8600 supports SMLT while using a single Switch Fabric/CPU module in the chassis. If this configuration is required, ensure that the hardware I/O modules are at the correct hardware revision to support this and enable the single CPU SMLT feature in the software. This disables SMLT ports on the I/O modules if the Switch Fabric/CPU module fails or is removed from the chassis.
- Enable High Availability mode on the ERS 8600 when using SMLT for optimal failover and recovery. Please note to check the release notes for the software releases to ensure full support for HA/SMLT, and also note the protocol/feature support in each of the software releases before trying to implement HA/SMLT.
- The single CPU SMLT feature can be implemented in dual SSF/CPU chassis. This provides a very similar redundancy capability as HA in an SMLT environment. The advantage of this feature is that there are no protocol restrictions as there are in HA mode. This feature is fully supported on R-modules. For support on other modules, consult your Nortel representative.
- RSMLT
    - Based on SMLT, so all SMLT rules apply.
    - Configured on a per VLAN basis.
    - VLAN must be routable and part of the SMLT links and IST link.
    - If possible, ensure that destination networks are directly accessible from each of the switches participating in RSMLT. This guarantees subsecond failover in case of a failure.
    - Leave the hold down timer at 60 seconds. An exception: For very large OSPF networks where convergence times are greater than normal, increase the timer to slightly longer than the expected convergence time.

2.2.5.4 Layer 2 VLANs

VLANs and their use are described in the edge connectivity section above. The use of VLANs within the core and/or distribution layer are dependent on the VLAN architecture for the edge. At a minimum, within the Converged Campus, there will be VLANs configured for both data and voice at the edge. VLANs are created in the core for specific network services, backbone connections, and any other areas of the network that should be isolated through Layer 2. The Terabit Cluster switches have the flexibility the employ various types of VLANs, including port, protocol, subnet, and MAC.

2.2.5.4.1 Design Recommendation

The use of VLANs within the core/distribution layers is very beneficial for isolating traffic and controlling traffic flow, along with easing the implementation of QoS. Assess the following criteria when implementing VLANs in the core/distribution:

- Order of precedence for identifying packets ingressing the ERS 8600
    - 802.1Q tagged packet
    - Subnet-based VLAN

    - Protocol-based VLAN
    - MAC-based VLAN
    - Port-based VLAN

- Create a separate port-based VLAN that is strictly used for the IST between ERS 8600 pairs. Do not enable any Layer 3 protocols on this VLAN, and add only the IST ports to this VLAN.
- Avoid using brouter ports (ports with an IP address assigned directly) – instead, use single port VLANs, which will provide much more flexibility and consistency in the configuration of the ERS 8600.
- Use subnet-based VLANs to emulate multi-netting (separation of multiple IP subnets ingressing the same link to the ERS 8600) – DHCP will not work in this configuration to assign different IP addresses to different subnets on the same link, unless IP addresses are statically defined within the DHCP server.
- Do not use subnet-based VLANs as transient VLANs – this configuration is not supported by the ERS 8600.
- By default, VLAN 1 is created and all ports are members – this VLAN cannot be deleted. It is a best practice to not use this VLAN for any type of production traffic. Use this VLAN only as a repository for unused ports within the Terabit Cluster. When modules are added to the chassis, all of those new ports will automatically be configured for VLAN 1. Therefore, to avoid any possible misconfigurations or inadvertent connections, it is best not to use this for production traffic.
- Leave Forwarding Database (FDB) timers at default value of 300 seconds.

2.2.5.5 Layer 3 Routing

The design philosophy of the Converged Campus is to centralize the routing functionality within the core and distribute the intelligence (QoS, traffic management, security/authentication) across the network. Within the core, there are many Layer 3 routing options to be taken into consideration. Evaluate all of the following during the design phase:

- IP routing protocol – OSPF/RIP/BGP

  The ERS 8600 switch supports a variety of Layer 3 routing protocols, including RIP v1/v2, OSPF and BGP. The selection of the correct routing protocol for the Converged Campus design is dependent on the requirements for size and scalability. The RIP protocol is much easier to implement, but is not nearly as efficient as OSPF, both in convergence times, and the amount of control traffic across the network. Normal convergence times for RIP are approximately 30 to 60 seconds; in contrast, OSPF usually converges in approximately 15 to 25 seconds. For large, complex networks, OSPF is the preferred choice of routing protocol because it is more efficient and scalable.

  Border Gateway Patrol (BGP) is an exterior gateway protocol designed to exchange network reachability information with other BGP systems in other autonomous systems, or within the same autonomous system (AS). This network reachability information includes information on the AS list that reachability information traverses. This information is sufficient to construct a graph of AS connectivity from which you may prune routing loops and enforce some policy decisions at the AS level.

  BGP4 provides you with a new set of mechanisms for supporting classless inter-domain routing. These mechanisms include support for advertising an IP prefix and eliminate the concept of network class within BGP. BGP4 also introduces mechanisms that allow you to aggregate routes, including aggregating AS paths. BGP is usually used to connect an Enterprise network to the Internet.

- IP multicast routing protocol – PIM/DVMRP

  Either DVMRP or Protocol Independent Multicast (PIM) routing can be used to distribute multicast traffic within the network. With this method, you must distribute sources of multicast traffic on different IP subnets and design routing metrics so that traffic from different sources flows on different paths to the destination groups. The ERS 8600 is uniquely designed to support multicast traffic flows in a very efficient manner – at ingress, the packet is classified in hardware and only replicated where needed.

  DVMRP (Distance Vector Multicast Routing Protocol) is a flood-and-prune technology in which the multicast streams are sent throughout the network and then pruned back to only those areas needing the multicast. This technology works very well where there are large groups of users requesting the same multicast stream.

  PIM only sends multicast to areas of the network that have specifically requested the multicast stream. This is a much more efficient use of the available bandwidth in the network. PIM is usually the protocol of choice when there are a sparse number of users requesting the multicast stream. The ERS 8600 supports both PIM-SM (sparse mode) and PIM-SSM (source specific mode). PIM-SSM is usually the protocol of choice for applications such as TV distribution or applications that require transmission acknowledgement. PIM uses the underlying routing table of the unicast routing protocol for its route table – for large scale networks, it is best to use OSPF as this protocol.

- Equal Multicast for Layer 3 link load balancing

  ECMP provides the ability to load balance Layer 3 links and provide redundancy for routing in situations where there are at least two equal paths from the source to the destination network.

- Dynamic Host Configuration Protocol (DHCP)

  DHCP provides a mechanism to automatically provision IP address information to end stations on the network. This is the predominant method used throughout most Enterprise environments because of the ease of implementation. From the network point of view, enabling DHCP relay on the switches allows a single DHCP server to provide IP addresses across many VLANs/subnets.

- Virtual Router Redundancy Protocol (VRRP) for default gateway resiliency

  VRRP provides redundancy for end user's default gateway. This adds another layer of resiliency to the Converged Campus design and should be utilized for each VLAN configured to host end stations. In the event of an uplink failure or switch failure, there is no interruption for end user traffic attempting to go off their local subnet.

  Nortel has created an extension to VRRP that allows for local processing of traffic that would otherwise have to take an extra hop to get to the default gateway. VRRP Backup Master allows both ERS 8600 switches to forward and route traffic, creating an active-active environment for routing. This feature is extremely beneficial when implemented in conjunction with SMLT.

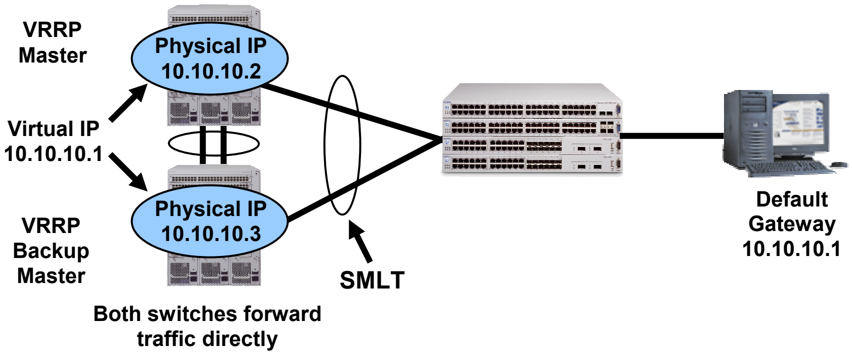


Figure 7: VRRP Default Gateway Resiliency

- VRRP versus RSMLT for default gateway resiliency

  Both VRRP and RSMLT can provide resiliency for the end station's default gateway. The configurations of these features are different in regard to the ERS 8600. However, to the end station, both provide the same end result and are transparent to the end station.

  To reduce the convergence time of VRRP, the VRRP Fast features allow the modification of VRRP timers to achieve subsecond failover of VRRP. Without VRRP Fast, normal convergence time is approximately 3 seconds. Take care when implementing VRRP Fast as this creates additional control traffic on the network and also creates a greater load on the CPU.

  Implementing RSMLT instead of VRRP can provide several advantages:

  - RSMLT is only limited by the number of IP interfaces on the ERS 8600.
    - VRRP is limited to 250 instances.
  - RSMLT requires significantly less control traffic.
  - RSMLT is much less intensive on CPU resources.

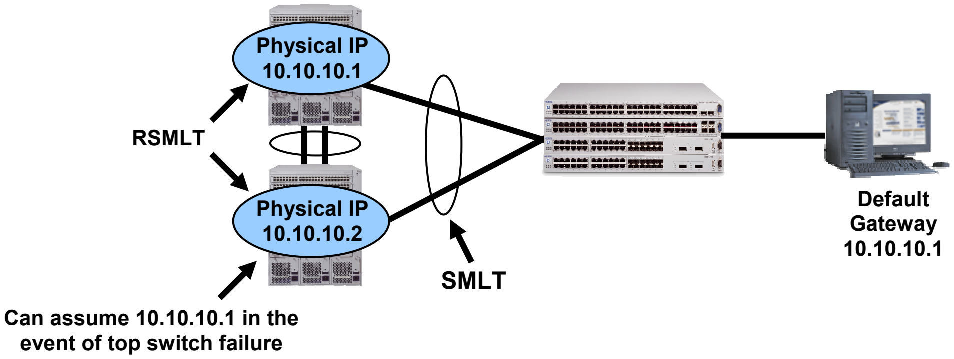


Figure 8: RSMLT Default Gateway Resiliency

2.2.5.5.1 Design Recommendation

The following details the design limitations and scalability numbers that must be evaluated during the design process. Please note that the scalability numbers provided are software-version dependent (check the software release notes). Scalability numbers will improve with future software releases.

- The default route preferences within the ERS 8600 should be left at default – only change route preferences when necessary, especially when using BGP and RIP. The defaults are as follows:
    1. Local
    2. Static
    3. OSPF Internal
    4. EBGP
    5. RIP
    6. OSPF External
    7. IBGP
- OSPF
    - Five areas per switch
    - 80 adjacencies per switch
    - 15 000 routes per switch
    - Timers must be consistent across the entire network – use default values
    - Configure core switches as designated routers
        - Higher rtrpriority is designated router
        - Configure rtrpriority in increments of 10 for future flexibility
        - Configure any Layer 3 closet switches with a priority of 0 so they can never become the designated router
    - Configure OSPF global router ID the same as the CLIP address for operational simplicity – CLIP address is the circuitless IP address
    - Must enable ASBdrRtr to utilize route redistribution
    - Use MD5 authentication on any untrusted OSPF links
    - Use OSPF area summarization to reduce routing table sizes
    - Use OSPF passive interfaces to reduce the number of active neighbor adjacencies – use passive interfaces on all user VLANs.
    - Use OSPF active interfaces only on intended route paths. Typically, you should configure wiring closet subnets as OSPF passive interfaces unless they form a legitimate routing path for other routes.
    - Limit the number of OSPF areas per switch to as few as possible to avoid excessive shortest path calculations. Be aware that the switch has to execute the Djikstra algorithm for each area separately.
    - Ensure that the OSPF dead interval is at least four times the OSPF hello interval
- RIP
    - 2500 routes per switch

    - For user VLANs where RIP is enabled, disable default supply and listen to reduce the amount of broadcast traffic on those VLANs

- DVMRP
    - Up to 1980 interfaces can be configured for DVMRP, with a maximum of 80 active
    - Interfaces should be configured as passive
    - Scaling up to 2500 routes when used in conjunction with RIP, OSPF, IPX/RIP
    - Supports up to 2000 S,G pairs
    - Number of source subnets times receiver groups should not exceed 500
- PIM-SM
    - Up to 1980 interfaces can be configured for PIM
    - Up to 80 active interfaces, with 10 active in large scale networks with greater than 500 VLANs
    - Interfaces should be configured as passive
    - Scaling up to total number of routes supported by unicast routing protocol – recommendation is to use OSPF in large scale networks
    - Supports up to 2000 S,G pairs
    - Number of source subnets times receiver groups should not exceed 500
- DHCP
    - Enable DHCP relay on every VLAN that requires DHCP address provisioning
    - Enable both DHCP and Bootp modes
    - Ensure the agent mode is consistent with the VLAN mode – DHCP is enabled on a global basis as well as on individual VLANs
    - By default, the hop is set to 4 – in most cases, this is sufficient, but if the DHCP server is greater than four hops away, be sure to modify this parameter
- VRRP
    - Supports a maximum of 250 instances per switch and cluster
    - Do not configure the virtual address as a physical interface that is used on any of the routing switches – use a third address, for example:
        - Physical IP address of VLAN a on Switch 1 = x.x.x.2
        - Physical IP address of VLAN a on Switch 2 = x.x.x.3
        - Virtual IP address of VLAN a = x.x.x.1
    - Leave the VRRP hold down timer at 60 seconds. For very large networks with higher than normal convergence times, this timer can be increased.
    - Implement VRRP Backup Master for an active-active configuration.
    - Backup Master works across multiple switches participating in the same VRRP domain.
    - Always set the VRRP priority on the master switch higher than the default of 100.

- RSMLT for edge connectivity
  - Based on SMLT, so all SMLT rules apply
  - Configured on a per VLAN basis
  - VLAN must be routable and part of the SMLT links and IST link
  - Hold up timer must be increased to 9999 (meaning infinity) so that the functioning switch is able to forward traffic indefinitely for a failed peer

2.2.5.6 Security Features

The security of the Converged Campus is of paramount importance to the overall design. Nortel offers a variety of security mechanisms, both within the Ethernet switching platforms and without, that work in conjunction to provide the highest level of security possible. This section focuses on features built into the Resilient Terabit Cluster that guard against attacks on the network.

- Broadcast and Multicast Rate Limiting

  To protect the ERS 8600 switch and other stations from a high number of broadcasts, the switch has the ability to limit the broadcast/multicast rate. This feature can be configured on a per-port basis. By default, this feature is disabled, and should only be enabled when the overall rates of broadcast and multicast traffic exceed normal levels.

- Directed broadcast suppression

  The ERS 8600 provides the ability to enable or disable forwarding for directed broadcast traffic on an IP-interface basis. A directed broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. When you disable or suppress directed broadcasts on an interface, all frames that are sent to the subnet broadcast address for a local router interface are dropped. Directed broadcast suppression protects hosts from possible Denial of Service (DoS) attacks.

- Prioritization of control traffic

  ERS 8600 uses a very sophisticated prioritization scheme for scheduling received control packets (BPDUs, OSPF Hellos, etc.) on physical ports. This scheme involves two levels with both hardware and software queues and guarantees proper handling of these control packets regardless of the load on the switch. In turn, this guarantees the stability of the network. More specifically, it guarantees that the applications that heavily use broadcasts (typically IPX) are handled with a lower priority. Note that you cannot use the CLI to view, configure, or modify these queues. Setting the queues and determining the type of packets entering each queue is Nortel confidential.

- ARP limitation

  The ARP request threshold limits the ability of the ERS 8600 to source ARP requests for workstation IP addresses it has not learned within its ARP table. The default setting for this function is 500 ARP requests per second. To help customers experiencing excessive amounts of subnet scanning caused by a virus (such as Welchia), Nortel recommends that you change the ARP request threshold to a value between 100 and 50. This will help protect the CPU from causing excessive ARP requests, help protect the network, and lessen the spread of the virus to other PCs.

- Multicast learning limitation

  This feature protects the CPU from multicast data packet bursts generated by malicious applications such as viruses. Specifically, it protects against those viruses that cause the CPU to reach 100 percent utilization or that prevent the CPU from processing any protocol packets or management requests. If more than a certain number of multicast streams enter the CPU through a port during a sampling interval, the port is shut down until the user or administrator takes appropriate action.

- High Secure Mode

  To protect the ERS 8600 against IP packets with an illegal source address of 255.255.255.255 from being routed (per RFC 1812 Section 4.2.2.11 and RFC 971 Section 3.2), the ERS 8600 supports a configurable flag, called *high secure*. By default, this flag is disabled. Note that when you enable this flag, the desired behavior (not routing source packets with an IP address of 255.255.255.255) is applied on all ports belonging to the same Octapid (group of eight 10/100 ports [8648], 1 Gig port [8608], or 2 Gig ports [8616]).

- Access Policies – ERS 8600 and ERS 8300

  Access policies let you control management access by setting policies for services to prevent or allow access to the switch. You can specify which hosts or networks can access the switch through FTP, http, rlogin/rsh, SSH, Telnet, and TFTP. You can set the access level (ro|rw|rwa).

- Configurable Software Daemons

  The ERS 8300 and ERS 8600 provide the ability to enable or disable various access methods. On the ERS 8600, you enable or disable ftp, tftp, telnet, rlogin, SSH, or SNMP. The ERS 8300 allows you to enable or disable ftp, tftp, telnet, rlogin, or SSH. The ERS 8600 also has a High Secure Mode in which all daemons are disabled; i.e., telnet, ftp, tftp, rlogin, and SNMP are disabled.

  For the ES 460/470 and ERS 55xx, HTTP, telnet, and SNMP can be enabled or disabled through standard configuration.

- Router Policies

  The ERS 8600 supports IP RIP/OSPF accept/announce policies. This provides extra security by either blocking specific subnets or selecting to announce specific subnets. The ERS8600 also support IPX RIP/SAP polices.

  The ERS 8300 in release 2.2 supports RIP announce/accept polices.

- Port Lock Feature

  This feature lets you lock a port or prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is unlocked.

- Out-of-band Management

  Each Switch Fabric on the ERS 8300 and ERS 8600 provides an Out-of-band Management port. Traffic on this port is completely separated from the user traffic and provides a high secure network for management.

- Access Security

  The following features are supported for access to an ES or ERS switch.

  - RADIUS authentication
  - SSH
  - SSL (ES 460/470 and ERS 5510)
  - Password security and CLI logging

- Stopping IP Spoofed Packets

  Spoofed IP packets are stopped by configuring the ERS 8600 to ensure that IP packets are forwarded only if they contain the correct source IP address of your network. A spoofed packet is one that comes from the Internet into your network with a source address equal to one of the subnet addresses used on your network. Its source address belongs to one of the address blocks or subnets used on your network. With anti-spoofing protection, you have a filter rule/configuration assigned to the external interface, which examines the source address of all outside packets crossing that interface. If that address belongs to internal network or firewall itself, the packet is dropped. The correct source IP addresses consist of the IP network addresses that have been assigned to the site/domain. It is particularly important that you do this throughout your network, especially at the external connections to the existing Internet/upstream provider. By denying all invalid source IP addresses, you minimize the chances that your network will be the source of a spoofed DoS attack.

  This will not stop DoS attacks coming from your network with valid source addresses, however. In order to prevent this, you need to know which IP network blocks are in use. You then create a generic filter that:

  - Permits your sites' valid source addresses
  - Denies all other source addresses

2.2.5.6.1 Design Recommendation

The following summarizes the guidelines for implementing security features within the Resilient Terabit Cluster.

- Broadcast and Multicast Rate Limiting
  - Default:
  - Severe: Workstation=1000, Server=2500, Interconnect=7500
  - Moderate: Workstation=2500, Server=5000, Interconnect=9000
  - Relaxed: Workstation=4000, Server=7000, Interconnect=10000
- ARP limitation guidelines
  - Default: 500
  - Severe Conditions: 50
  - Continuous scanning conditions: 100
  - Moderate: 200
  - Relaxed: 500
- Directed broadcast suppression
  - Default is enabled and should be left as such
- High Secure Mode
  - Default is disabled and should be enabled for an increased level of security – this feature will disable all daemons such as telnet, ftp, tftp, rlogin, and SNMP.

- Create ingress filters to prevent IP spoofed packets. If you do not know all the addresses from which spoofed packets are sent, it is important to at least deny Private (See RFC1918) and Reserved Source IP addresses:

0.0.0.0/8	Historical Broadcast
10.0.0.0/8	RFC1918 Private Network
127.0.0.0/8	Loopback
169.254.0.0/16	Link Local Networks
172.16.0.0/12	RFC1918 Private Network
192.0.2.0/24	TEST-NET
192.168.0.0/16	RFC1918 Private Network
224.0.0.0/4	Class D Multicast
240.0.0.0/5	Class E Reserved
248.0.0.0/5	Unallocated
255.255.255.255/32	Broadcast

2.2.6 Filter Features on ES and ERS switches

	Feature	ES460/470	ERS55xx	ERS8300	ERS8600	R-Modules
Layer 2	Ingress/Egress	Ingress	Ingress	Ingress	Ingress	Both
	VLAN	Yes	Yes	Yes	No	Yes, in and out
	VLAN Tag	Yes	Yes	Yes	No	Yes
	EtherType	Yes	Yes	Yes	No	Yes
	802.1p	Yes	Yes	Yes	No	Yes
	src/dst MAC	No	Yes	Yes	No	Yes
Layer 3/4	Ingress/Egress	Ingress	Ingress	Ingress	Ingress	Both
	src/dst IP	Yes	Yes	Yes	Yes	Yes
	DSCP	Yes	Yes	Yes	Yes	Yes
	Protocol Type	Yes	Yes	Yes	Yes	Yes
	src/dst Port	Yes	Yes	Yes	Yes	Yes
	ARP	No	No	No	No	Yes
	IP Fragmentation	No	No	Yes	Yes	Yes
	TCP Flags	No	No	Yes	No	Yes
	IPv6	No	Yes	No	No	Yes, 4.1
Filter Actions	Remark DSCP	Yes	Yes	Yes	Yes	Yes
	Remark 802.1p	Yes	Yes	Yes	Yes	Yes
	Manual Select Egress Queue	No	No	No	No	Yes
	Permit/deny	Yes	Yes	Yes	Yes	Yes
	Filter Count/Stats	No	Yes	Yes	Yes	Yes
	Mirror	No	No	Yes	Yes	Yes
	Fwd-next-hop	No	No	Yes	Yes - dst filter only	Yes
Police/Shape	Police Traffic	Yes	Yes	Yes	Yes	Yes
	Shaper/port	Yes	Yes	Yes, 10M/port	No	Yes
	Shaper/queue	No	No	Yes, 10M/queue	No	Yes
Off-set Filters		No	Yes	No	No	Yes

Table 14: Filter Features – ES/ERS

2.2.7 Threat Protection

2.2.7.1 Overview

The Nortel Layered Defense approach to network security provides comprehensive protection for all aspects of the Converged Campus. Within the Core Switching and Edge Switching elements (see Figure 1), a key focus is to provide awareness of malicious traffic and protect clients and servers from falling victim to or launching network-based attacks. These attacks can include:

- Unauthorized Access or Failed Access Attempts
- Denial Of Service Attacks
- Policy Violations
- Network Probing/Scanning
- Virus/Worm/Trojan Activity

The Threat Protection System (TPS) provides the following features and benefits:

- Detects known threats through deep-packet inspection: Exposes defense weaknesses and enables administrators to take corrective actions.
- Detects unknown threats through rules-based anomaly detection: Gives early warning against emerging threats or malicious internal activity.
- Passively scans network traffic to gain real-time awareness of network hosts (as a client or as a server) including host Operating System, Network Services and Vulnerability.
- Keeps up to date on new threats and vulnerabilities through the Snort™ community and a dedicated team of security experts: Helps to maintain the most effective security posture possible.
- Queries and reports on threats and event data: Lets you gain a better understanding of the network environment and prioritize vulnerabilities.
- Traps and traces traffic associated with any attack: Lets you analyze all critical information to formulate response to generic or specialized attacks.
- Correlates network threats to target vulnerability to reduce false positives, prioritize positives, and provide context for intrusion response.
- Actively blocks threat traffic whether deployed in-line or through enforcing access control policies on other network devices, including firewalls, application switches, and routers.

Key components of the TPS solution include:

- Intrusion Sensors – monitor network traffic, validate protocol compliance, ensure communication flow, and prepare the data for inspection against the rules data base. The rules database alerts on a match of known threat signatures and traffic anomalies.
- Real-Time Threat Intelligence (RTI) Sensors – passively collect network traffic in order to develop and refine host profiles, which house Operating System (OS), network service, and vulnerability information for all hosts on the network.
- Defense Center – acts as a centralized management station for all other sensors on the network and provides configuration control, reporting database, policy management, data correlation and threat response management.
- Remediation Application Programming Interface (API) – provides a flexible architecture for dynamically updating firewall policies, application switch filters, and other extensible actions, such as initiating Nessus host scans.

Sensor Types

There are currently six sensor models with the following capabilities and network interfaces:

- Out of Path Intrusion Sensors
  - 2050-IS: 100 Mbps capacity, 3 x 10/100/1000 TX Sensing NICs, 1 x 10/100/1000 Management NIC
  - 2070-IS: 1.2Gbps capacity, 3 x 10/100/1000 TX Sensing NICs, 1 x 10/100/1000 Management NIC
- In-line Intrusion Sensors
  - 2150-IS: 100 Mbps capacity, 3 x 10/100/1000 sensing interfaces – one bypass 2 port NIC for in-line operation, 1 x 10/100/1000 Management NIC
  - 2170-IS: 1Gbps capacity, 3 x 10/100/1000 sensing interfaces – one bypass 2 port NIC for in-line operation, 1 x 10/100/1000 Management NIC
- RTI Sensors
  - 2050-TI: 100 Mbps capacity, 3 x 10/100/1000 TX Sensing NICs, 1 x 10/100/1000 Management NIC
  - 2070-TI: 1 Gbps capacity, 3 x 10/100/1000 TX Sensing NICs, 1 x 10/100/1000 Management NIC

2.2.7.2 Design Considerations

Consider these guidelines when designing a Threat Protection System for your network.

2.2.7.2.1 General Recommendations and Requirements

- Place sensors as close as possible to the hosts that they are intended to protect. Sensors are often placed within the DMZ and Data Center to monitor traffic to and from those critical network zones. Within the core and edge switching zones, it is desirable to place sensors as close as possible to the end-hosts that they are protecting in order to provide more accurate RTI host profiles, more granular detection (including peer-to-peer desktop threats), and to reduce the aggregate bandwidth that must be handled by the sensors. In practice, there is always a trade-off with regard to the number of sensors that can be distributed in terms of cost versus the benefits provided. Given the goal to analyze traffic to and from all hosts and maximize the scope of RTI host inventories, it is ideal to deploy sensors that monitor all of the lowest-tier uplinks, shown in Figure 3. This can be done by collecting traffic from one or more SMLT uplink sets to each Intrusion sensor. This places sensors at the core switching in a two tier architecture (Figure 2) and the distribution tier (middle tier) in a three tier architecture.
- Sensors must be able to collect and analyze both client to server and server to client communication flows to function properly. When using port mirrors, take care to direct both ingress and egress port traffic to the Intrusion or RTI sensor. When using network taps, transmit signals from both directions must be directed to the sensor.
- Take care in deployments where there is possibility of asymmetric traffic flow. Links that use various load-balancing techniques (SMLT, 802.3ad, ECMP) or for which the ingress path is different than the egress gateway must be carefully considered for IDS monitoring. For example, client to server traffic may follow one SMLT uplink while the server to client response traffic may follow another link. In this case, multiple ports must be mirrored or tapped to the same sensor.

- In general, the aggregate traffic must not exceed the sensor capacity. In practical terms there is a trade-off of peak traffic demands and sensor capacity, depending on sensor location and traffic patterns.
- Although TPS supports an in-line mode for sensor deployment, this mode is not typically used within Edge and Core Switching zones due to the requirement to support SMLT asymmetry, and because the current single fail-open NIC provides in-line support for a single link.
- RTI and Intrusion sensors need to monitor traffic from the same hosts so that the RTI capability can provide target vulnerability information for the threats monitored by the IS (Intrusion sensor). Generally the goal of Intrusion sensors is to monitor as much traffic as possible (client/Internet, client/Data Center, client/WAN, client/client), whereas the goal of RTI sensors is to identify as many hosts and services as possible. To capture host profiles for as many clients as possible, one option is to place RTI sensors in front of servers to which all clients must communicate, such as DNS, DHCP and e-mail servers. In many cases, placing RTI sensors between the Edge Switching zone and the Data Center accomplishes this.

2.2.7.2.2 Port Mirroring Design Matrix

Table 15 highlights mirroring capabilities and limitations.

Ethernet Switch	Egress Mirroring Ports	Ingress Mirroring Ports	Monitor Ports	Notes
ERS 8600 E/M Modules	383	383	64	Ports from same Octapid must be mirrored to same destination
ERS 8600 R-Modules	1/Lane	1/Lane	64	See Table 16 for module/port/lane assignments
ERS 8300	8	383	1	Ingress/Egress supported on same port
ERS 5500	383	383	1	Must use Release 4.2 or later for many to one port mirroring
ES 460/470	2	2	1	See below for configuration parameters
AAS 2000/3000	Many	Many	1	All ports on a switch can be mirrored, less the monitor port

Table 15: Port Mirroring Capabilities

ERS 8600

- Must use E/M/R Modules for egress mirroring support
- Can mirror multiple ports to a single destination (see Table 16)
- Can mirror different speed ports and different physical media
    - 10/100 to Gig – no issues
    - Gig to 10/100 – may not see all packets if exceeding 100 Mbps on the Gig link
    - Copper to Fiber – no issues
    - Fiber to Copper – no issues

- Cannot mirror a single port to multiple destinations
- Number of mirroring ports plus mirror ports cannot exceed 384
- VLAN mirroring supported with R modules

ERS 5500

- Monitor port must belong to the same VLAN as mirror ports
- If mirror port is tagged, monitor port must also have tagging enabled
- If mirroring an MLT port, MLT must be disabled

ES 460/470

- Monitor port must belong to the same VLAN as mirror ports
- If mirror port is tagged, monitor port must also have tagging enabled
- If mirroring an MLT port, MLT must be disabled

AAS 2000/3000

- Supports 1:1 and M:1 port mirroring
- Supports 1:1 and M:1 VLAN mirroring
- Support for IDS load balancing
    - VIP or Filter based SLB processing must be ON
    - 1 to 255 monitoring devices – SIP/DIP hashed
    - 1:M , or M:M IDS flooding supported
    - 1:M service based IDS groups
    - Stealth mode health checks – link and SNMP
    - 802.1Q for downstream IDS supported

Table 16 highlights the assignments of ports within an ERS 8600 switch to the Octapids (for E/M modules) and Lanes (for R modules). Note that ports belonging to the same Octapid group must be mirrored to the same destination port.

ERS 8600 Modules	Ports per Octapid	Port Assignments per Octapid (8 Octapids/Module)
8608 (GBE, GTE, SXE) 8608 (GBM, GTM)	1	1, 2, 3, 4, 5, 6, 7, 8
8616 (SXE, GTE)	2	1-2, 3-4, 5-6, 7-8, 9-10, 11-12, 13-14, 15-16
8624FXE	8	1-8, 9-16, 17-24
8632TXE 8632TXM	8 per copper 1 per GBIC	1-8, 9-16, 17-24, 25-32, 33 (GBIC), 34 (GBIC)
8648TXE 8648TXM	8	1-8, 9-16, 17-24, 25-32, 33-40, 41-48
8672ATME 8672ATMM	4 with OC3 2 with DS3 1 with OC12	1-4, 5-8 with OC3 1-2, 3-4 with DS3 1,2 with OC12
8683POSM	2 with OC3 1 with OC12	1-2, 3-4, 5-6 with OC3 1, 2, 3 with OC12
8681XLR 8681XLW	1 port uses all 8 Octapids	1
ERS 8600 Modules	**Ports per Lane**	**Port Assignments per Lane (3 Lanes/Module)**
8630GBR	10	1-10, 11-20, 21-30
8648GTR	24	1-24, 25-48
8683XLR	1	1, 2, 3

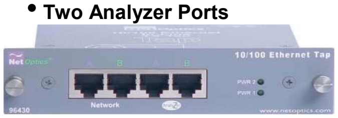
Table 16: ERS 8600 I/O Module Assignments for Port Mirroring

2.2.7.2.3 Taps

The following information provides details on network taps currently available from Nortel.

10/100 Passive Tap

- **Full Duplex 10/100 operation**
- **Redundant Power**
- **Two Monitor Ports**
- **Two Analyzer Ports**



Gig E Passive Tap

- **Full Duplex Gig E operation**
- **Redundant Power**
- **Two Monitor Ports**
- **Two Analyzer Ports**

Key Benefits:

- **Taps are left in-line and create a permanent access point without degrading performance**
- **Taps are non-intrusive, and pass on traffic from all network layers**
- **Taps enable Monitoring at full duplex**
- **Taps are "transmit-only" to the monitoring device- Stealth Monitoring.**
- **Taps "fail-open" with complete power failure.**

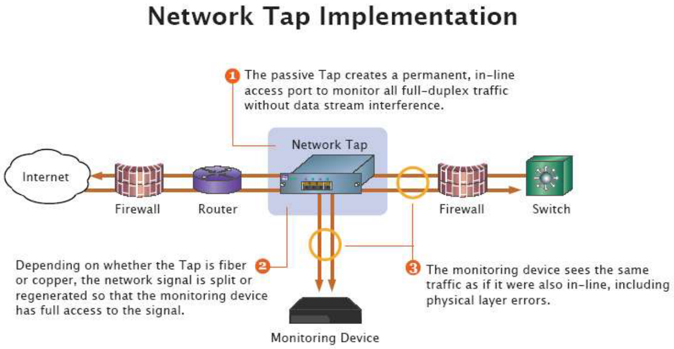

Network Tap Implementation
1 The passive Tap creates a permanent, in-line access port to monitor all full-duplex traffic without data stream interference.
Network Tap
Internet
Firewall
Router
Firewall
Switch
Depending on whether the Tap is fiber or copper, the network signal is split or regenerated so that the monitoring device has full access to the signal. 2
3 The monitoring device sees the same traffic as if it were also in-line, including physical layer errors.
Monitoring Device

Figure 9 shows the data flow through a standard passive copper tap. Note that two sensor ports are required to capture transmit signals from each direction.

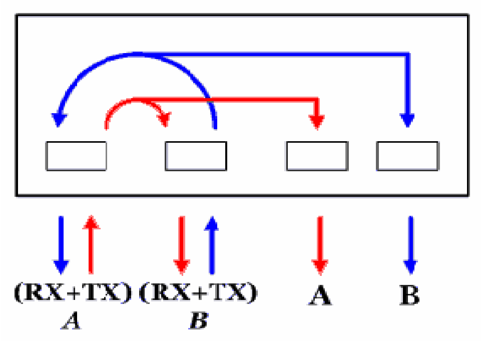


Figure 9: Copper Passive Tap Data Flow

2.2.7.2.4 Design Recommendations and Rationale

Figure 10 illustrates the use of ingress and egress port mirrors to direct traffic to an Intrusion sensor within a two tier architecture. The application in a three tier model is identical with the sensor connected at the distribution layer.

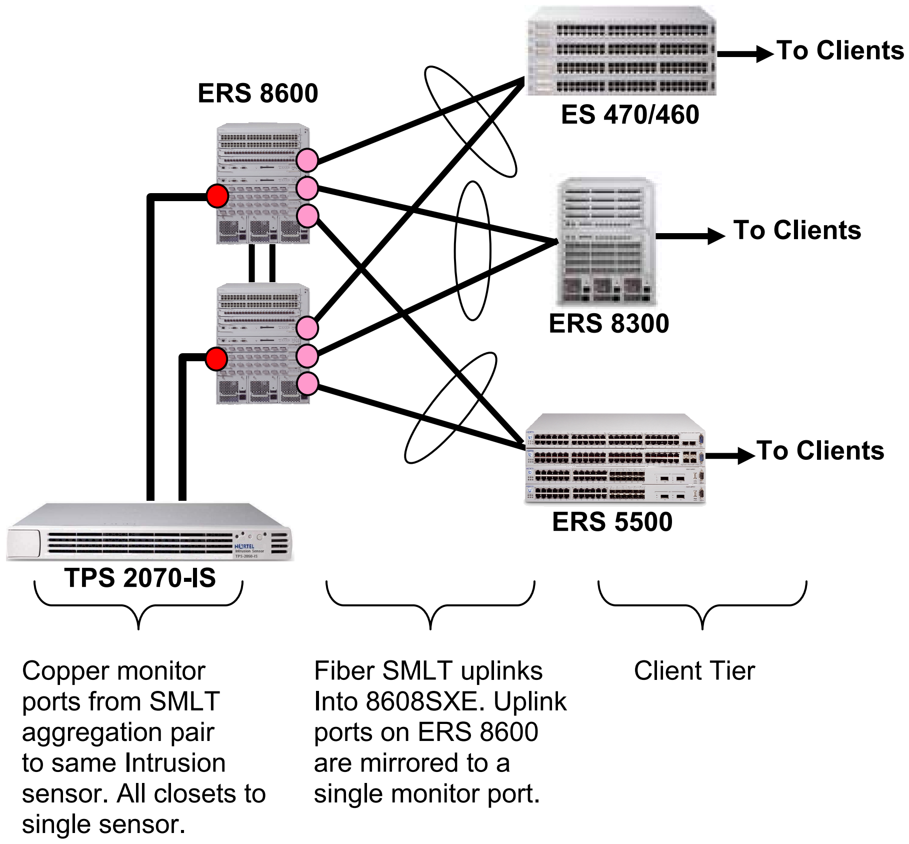
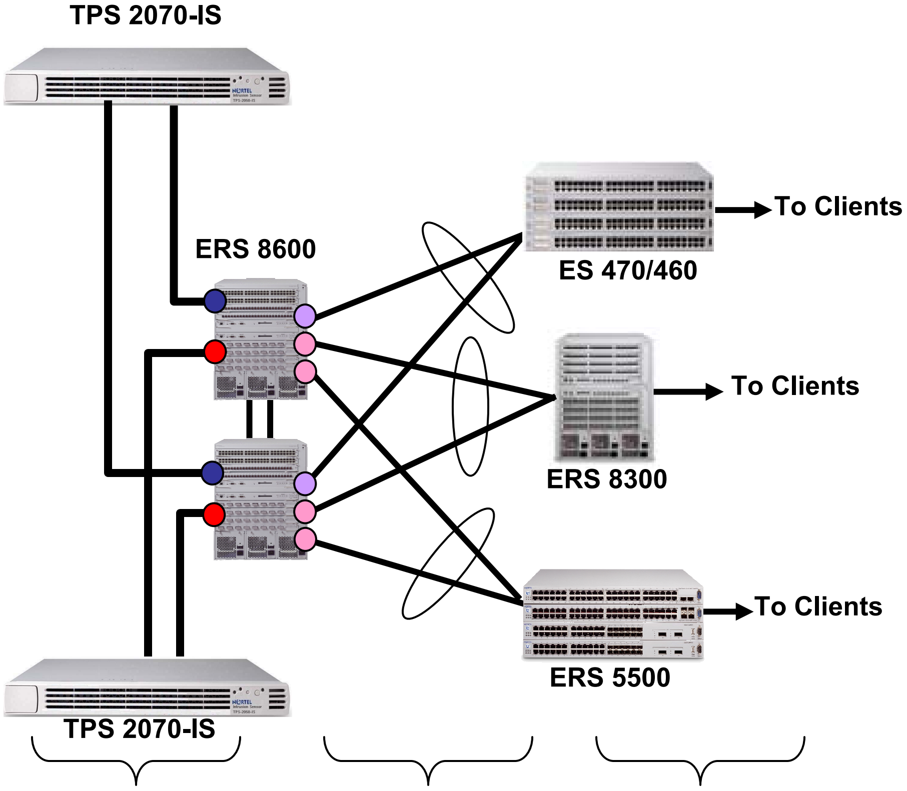

ERS 8600
ES 470/460
To Clients
ERS 8300
To Clients
ERS 5500
To Clients
TPS 2070-IS
Copper monitor ports from SMLT aggregation pair to same Intrusion sensor. All closets to single sensor.
Fiber SMLT uplinks Into 8608SXE. Uplink ports on ERS 8600 are mirrored to a single monitor port.
Client Tier

Figure 10: TPS Architecture – Port Mirroring

Figure 11 illustrates adding additional Intrusion sensors to scale the TPS application. In this case, sets of SMLT uplinks can be grouped together and mirrored to a monitor port connected to the sensor. Adding sensors in this fashion ensures that an individual sensor does not become overloaded from the aggregate bandwidth.



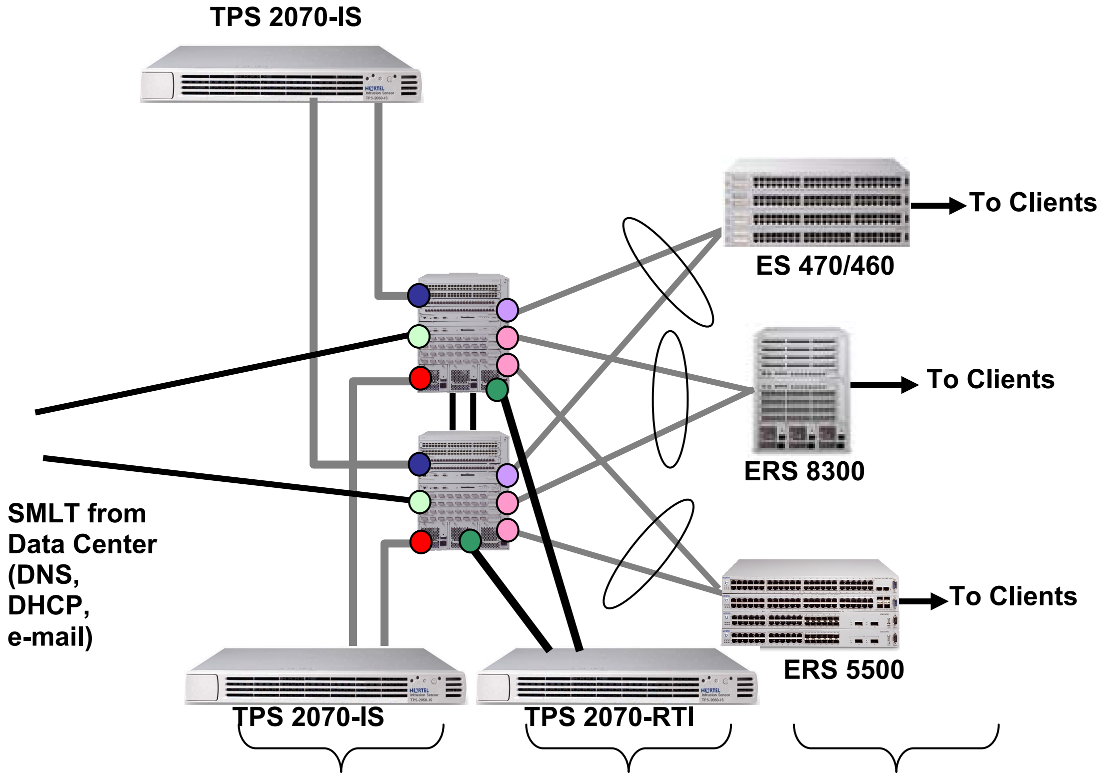
Copper monitor ports from SMLT aggregation pto same Intrusion sensor. Scale by distributing closet's mirror ports across multiple sensors.

Fiber SMLT uplinks Into 8608SXE uplink ports on ERS 8600 are mirrored. Top stack is mirrored to a different sensor than the bottom two closets.

Client Tier

Figure 11: TPS Architecture – Scaling Intrusion Sensors

Figure 12 adds an RTI sensor, which monitors the uplink ports to the Data Center. Additionally, the same monitor ports can monitor traffic to the DMZ (Internet) and WAN. The goal of RTI is primarily to gain visibility to all client hosts on the network to profile host type, OS and vulnerability information, which is correlated by the Defense Center to set threat impact flags on events.



Copper monitor ports from SMLT aggregation pair to same IS. Scale by distributing closet's mirror ports across multiple sensors.

RTI sensors monitor SMLT uplink ports from Data Center, DMZ and WAN zones. DNS, DHCP and e-mail traffic ensure wide coverage of LAN hosts for RTI host profiling.

Client Tier

Figure 12: TPS Architecture – RTI Sensors

2.2.7.3 Remediation – Responding to Threat Traffic

Using the TPS Policy and Response mechanism, high impact and priority threats can be actively blocked by configuring enforcement points within the network with filters or rules to block sessions, source addresses or destination addresses. Current remediation modules support the Nortel Application Switch, Nortel Switched Firewall, Third-Party OPSEC Firewalls, and Cisco PIX Firewalls and CISCO IOS routers. Any such enforcement device in the threat traffic path can be used to actively block traffic. Within the Edge and Core Switching environment these enforcement points typically reside between zones (Data Center, DMZ, WLAN, etc.) but can also be used to isolate VLAN traffic within the Core or Edge Switching zones.

2.2.8 Network Management

Nortel provides a comprehensive set of solutions and tools to enable a system-wide life cycle management approach dedicated to delivering convergence solutions that reduce total cost of ownership and enhance the end-user experience by managing real-time system and application performance, security, and reliability.

This section details the design and capabilities of our existing Convergence Management Solutions, highlighting key areas of importance.

In a converged network environment, maintaining availability, reliability, performance and protecting the network become significantly more important. Absence of any of these conditions is much less tolerable in a converged network environment when compared with a data network environment only. This is due to the fact that these conditions are constantly and immediately noticeable for the end user experience in a large community of users. Data packets may get constantly retransmitted and transactions eventually succeed, making the problem difficult to notice without sophisticated Flow Based Management tools (discussed later in this section). Problem conditions become immediately apparent to end users of VOIP, often long before the central administrator is able to detect them. In this case, the administrator needs a solution such as Proactive Voice Quality Management (PVQM), which is discussed later in this section.

To gain insight on how to effectively manage a converged network, think of a reference model to network management that specifies types or levels of network management solutions and categories of network management functionality within those levels.

Following the lead of the OSI layered protocol model, the ITU-T TMN Network Management Model provides an organization of management services in the form of a five-layer hierarchy of services. For each TMN layer, this document highlights Nortel solutions that provide the classic FCAPS (Fault, Configuration, Accounting, Performance, Security) capabilities within these solutions. The services provided by the TMN layers include:

Business Management

Nortel offers a comprehensive business life cycle management comprised of several solutions that allow customers to manage the converged network through a closed loop process of design/readiness. This flows to ongoing Service Management, which is linked back to solutions that make it easy to manage configuration and policies in order to configure and address network performance.

Service Management

Manage Converged Services and subscribers to those services. Are we effectively delivering a quality end-user experience? How and where is the network being used by what applications?

Proactive Voice Quality Management — PVQM provides real-time, proactive notification and problem resolution of emerging voice quality problems while a call is ongoing, without end-user involvement or awareness.

Enterprise Policy Manager — Easily and quickly takes action based on information received from PVQM to effect changes QoS policies, Security/Filter policies, and Policies to control Admission to the network.

Enterprise Subscriber Manager — Easily handles moves, adds, and changes of subscribers to converged services across different service types and call servers.

Opsware Network Automation System — Handles configuration control for security and compliance purposes. Manage password and SNMP community string changes across many different type of enterprise device types.– designed for use in large enterprise environments.

Nusecure — Security Event Management. – Aggregates and corroborates multiple dissimilar logs and traps looking for potential security events.

NetQoS — Leverage IPFIX Flow Based Management information down to the port level embedded into specific Nortel switches.

Network Management

Managing the voice and data networks as a converged whole, the Network Management layer with Nortel's solution provides for discovery, visualization, fault and troubleshooting for the Converged Campus.

Enterprise Network Management System – Discovery and Visualization of Call Servers, Phones, Data Network Switches, Secure Router/VPN tunnels, wireless and Optical in a single platform. Use as a consolidator and platform from which to launch to the Element Management layer applications. Converge Events from PVQM, Data Network Devices (SNMP/Syslog), and the Telephony Manager solution into a single display in Enterprise Network Management System.

Enterprise IP Address Domain Manager – The Nortel IP Address Domain Manager software solution provides automated IP Address, DHCP and DNS server management to increase IP network performance, availability and reduce costs associated with IP network management. IP Address Domain Manager minimizes downtime by streamlining IP address management. In addition, the software supplies innovative tools to simplify Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) management.

Element Management

Nortel provides best in class element management systems with industry-leading SNMPv3 support.

Enterprise Switch Manager – Multi-Element-Configuration Management System supporting SNMP v1/v2/v3 MD5/DES/AES

- VLAN Manager
- Security Manager
- Configuration File Backup and Restore
- Operation Image Upgrades
- Single Element Manager for Ethernet Switching platforms:
  - Ethernet Routing Switch 8600
  - Ethernet Routing Switch 8300
  - Ethernet Routing Switch 5510/5520/5530
  - Ethernet Switch 460/470

Telephony Manager – Multi-Element-Configuration and Performance Management System for CS1k:

- Element configuration and monitoring, forward alarms and events to Enterprise Network Management System

Network Element

Value added features for the Network Element in the areas of security, service monitoring and management.

SNMPv3 – With MD5 Auth, DES Privacy, AES Encryption – Full Support in Element Management Layer with Device Manager and Enterprise Switch Manager, as well as the Network Management Layer in Enterprise Network Management System

Topology Support – Topology data provides down to physical level connectivity. Visualization information helps to feed QoS/Filter/Network Provisioning. Will provide standards based 802.1ab support with future software releases:

- Ethernet Routing Switch 8600
- Ethernet Routing Switch 8300
- Ethernet Routing Switch 5510/5520/5530
- Ethernet Switch 460/470

IPFIX – Provides flow based monitoring beyond just up and down status on a per-port basis in certain devices, such as ERS5510 and ERS8600PR, without the need for expensive and complex external probes

2.2.8.1 Business Management

Nortel offers a closed loop Convergence Business Management life cycle. Some companies refer to this as PDIO or Plan-Design-Implement-Optimize. It is referred to as closed loop because the process involves a repeated cycle or “loop around” from the Optimize phase back into the Planning phase, continuously keeping the network in top condition. It is a significant challenge to do this without the proper solutions and tools, as well as enhanced features in the network devices themselves, such as those provided by Nortel.

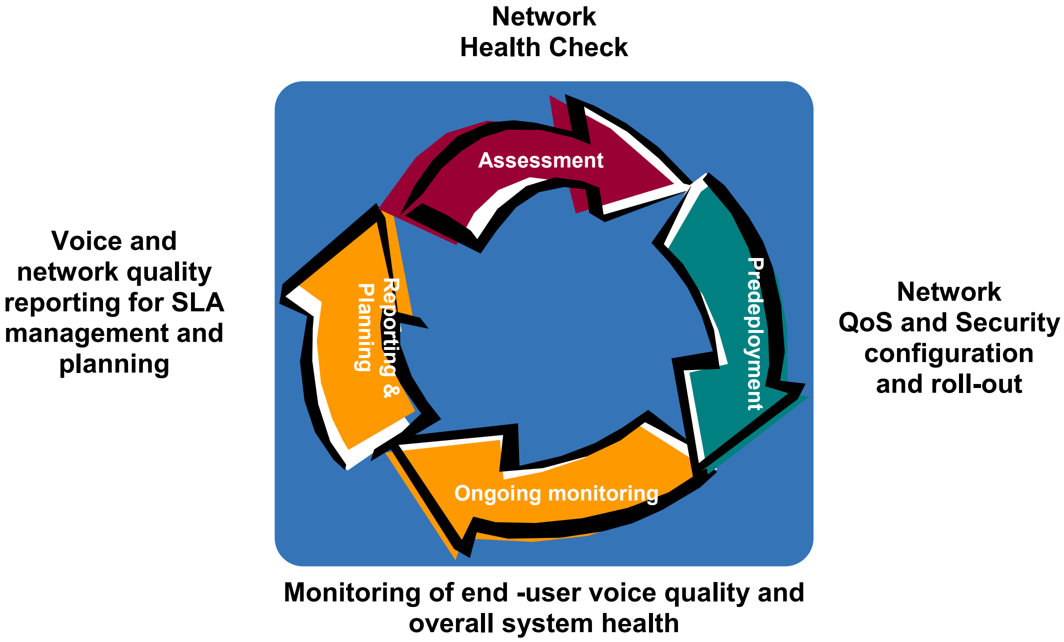

Network
Health Check
Assessment
Voice and network quality reporting for SLA management and planning
Reporting & Planning
Predeployment
Network QoS and Security configuration and roll-out
Ongoing monitoring
Monitoring of end -user voice quality and overall system health

Figure 13: Closed Loop Management

2.2.8.1.1 Health Check/Assessment Phase

Ensure the success and readiness of the network to support a converged environment prior to deployment. The health check and assessment will indicate where changes need to be made and where QoS policies need to be implemented, saving time and money. NetIQ Vivinet Assessor is the solution in this category. For detailed current information, see the *Nortel Alliance Partner Reference Sales Guide*.

2.2.8.1.2 Network QoS and Security Configuration/Predeployment Phase

Many converged networks today do not provide “dial tone” level reliability due to lack of proper security and QoS configuration. Additionally, improper configuration opens the door to Denial of Service (DoS) from accidents, broadcast storms, or malicious activity. For example, perhaps users may unintentionally perform a backup during key business hours.

Information from the Network Management Layer using solutions such as Enterprise Network Management System can be used to understand the topology of the network. Then, you can use Enterprise Policy Manger to enable (down to the network device physical port level) QoS and rate-limiting policies as well as TCP/UDP-level port filters to protect the network from Service Affecting situations. In network locations where there are visitors or less-supervised access to the network, or for all locations in companies where a high level of security is necessary, Enterprise Policy Manager can be used in conjunction with network elements from Nortel that support

EAP/UBP as a prerequisite for access to the network. Managers using Enterprise Policy Manager can even show who is authenticated to a slot/port using EPM.

The combination of Enterprise Network Management System and Enterprise Policy Manager allows customers to visualize the network and its components, and rapidly configure multiple types of Nortel equipment in the network for QoS, filters, and secure access to the Network using EAP/UBP.

2.2.8.1.3 Ongoing Monitoring (out to the end user quality of experience) Phase

Ongoing Voice Quality monitoring is often overlooked. Many companies put the bulk of their effort and investment into the readiness and initial configuration phases of their business process, only to have the network evolve and need constant reconfiguring to meet business needs. Few networks ever stay completely static. As a result, voice quality often suffers, and it is very difficult to monitor voice quality down to an individual user's quality of experience on a real-time basis.

Proactive Voice Quality Monitoring (PVQM) measures voice quality in real time from an end-user perspective using standards-based technology, and explains why you are experiencing reduced call quality. Reports allow you to monitor service levels, call quality, overall performance, usage trends and capacity planning. Most importantly, it allows you to know about and fix problems before they impact service.

2.2.8.1.4 Reporting, Troubleshooting, Planning Phase

Information obtained during the previous phases can be used in conjunction with information from the Network Management Layer to troubleshoot, isolate and actually address and fix problems. Using the solutions from Nortel makes this easy. Topology and visualization information, as well as real-time statistics from Enterprise Network Management System, can be used to assess where to make changes with Enterprise Policy Manager. NetiQ Vivinet Diagnostics can be used along with Vivinet Manager to isolate problems. Voice quality alerts from PVQM can be sent to the Enterprise Network Management System in combination with events from Telephony Manager for a truly converged alert/event system. Service Level Agreement (SLA) trends can be used to determine impacts of changes and past performance, which can be used to plan future changes to the converged network, or to determine the effectiveness of moving equipment to obtain better performance.

2.2.8.2 Service Management

Service Management of a converged network can be used in conjunction with information obtained from the lower layers, such as the Network Management Layer using the Enterprise Network Management System. Therefore, the first step in truly understanding a converged network is to discover and visualize the data network, and discover and visualize the location of the Call Servers, Media Gateways, and End Phones.

Use Enteprise Network Management System 10.4 to visualize and troubleshoot the converged network.

When you understand the system down to the physical slot/port connectivity of the network and the location of the various elements, you have a much better frame of reference for using complementary solutions such as PVQM to monitor end-user quality of experience and to implement policies through Enterprise Policy Manager to configure QoS on these network links. This knowledge also helps you implement policies to protect access to the network and the data that is transported over the network with significant speed and ease of use.

2.2.8.2.1 Proactive Voice Quality Management (PVQM)

Proactive Voice Quality Management (PVQM) is a solution Nortel has codeveloped with NetIQ. It gives the network manager the capability to ensure the overall quality of IP telephony deployments. PVQM continuously and passively measures the user quality of experience (QoE) for all IP Telephony communications, conducts system health checks for IP Telephony servers, and provides troubleshooting and resolution for any performance degradation or fault conditions. PVQM provides real-time, proactive notification and problem resolution of emerging voice quality problems while a call is ongoing, without end-user involvement or awareness.

Figure 14 is an example of a PVQM Solution Flow in an Ethernet Switching and CS 1000 v4.0 Environment.

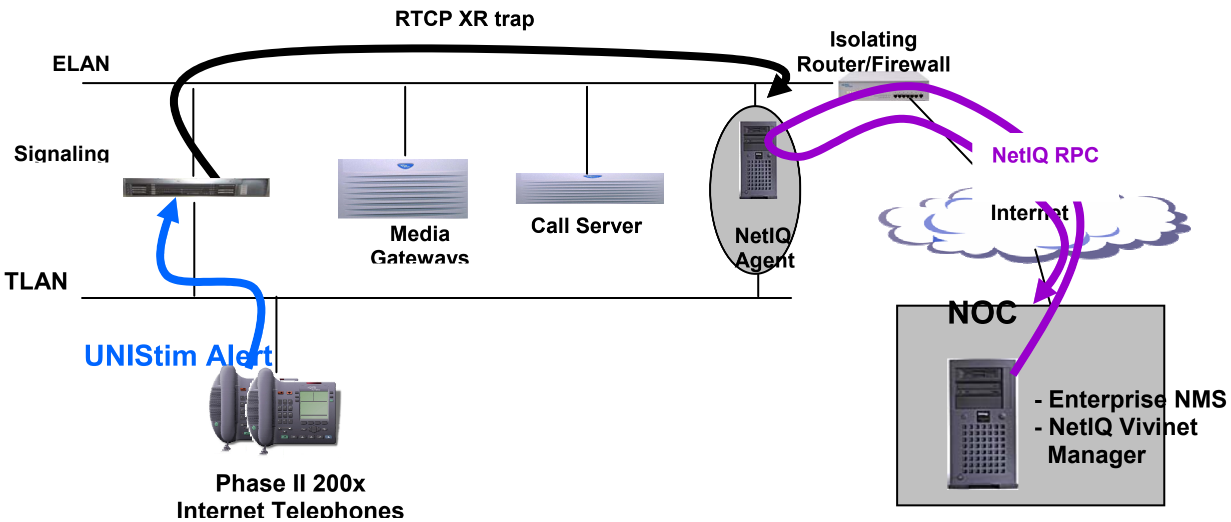


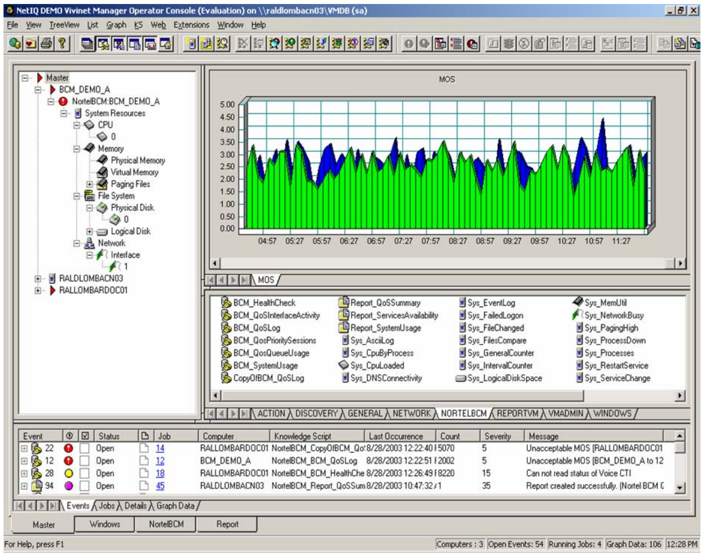
Figure 14: PVQM Solution Flow

- RTCP XR SNMP Trap into ENMS identifies Source/Destination Address of the originating/terminating media endpoints
- RTCP XR metrics indicate a network problem
- Low Discards with High Packet Loss indicates a network packet loss problem
- Isolate the path between the two endpoints using ENMS
- Create a performance view monitoring discards on each interface along the path to isolate where the packet loss is occurring

Standards Related to PVQM:

- ITU
  - H.323 (H.460.9 Annex B)
  - H.248 (H.248.30 – RTCP XR package)
- IETF
  - SIP RTCP XR
  - RTCP XR MIB
  - RTCP Video Extensions

NetIQ Vivinet App Manager as part of PVQM Solution – Ongoing Service Level Monitoring of end user Quality of Experience (MOS scores shown below)



```
Master
  BCM_DEMO_A
    NortelBCM:BCM_DEMO_A
      System Resources
        CPU
          0
        Memory
          Physical Memory
          Virtual Memory
          Paging Files
        File System
          Physical Disk
            0
          Logical Disk
        Network
          Interface
            1
  RALDLOMBACN03
  RALLOMBARDOC01
```

```
BCM_HealthCheck            Report_QoSSummary            Sys_EventLog            Sys_MemUtil
BCM_QoSInterfaceActivity   Report_ServicesAvailability  Sys_FailedLogon         Sys_NetworkBusy
BCM_QoSLog                 Report_SystemUsage           Sys_FileChanged         Sys_PagingHigh
BCM_QosPrioritySessions    Sys_AsciiLog                 Sys_FilesCompare        Sys_ProcessDown
BCM_QosQueueUsage          Sys_CpuByProcess             Sys_GeneralCounter      Sys_Processes
BCM_SystemUsage            Sys_CpuLoaded                Sys_IntervalCounter     Sys_RestartService
CopyOfBCM_QoSLog           Sys_DNSConnectivity          Sys_LogicalDiskSpace    Sys_ServiceChange
```

Event		☑	Status		Job	Computer	Knowledge Script	Last Occurrence	Count	Severity	Message
22	●	□	Open		14	RALLOMBARDOC01	NortelBCM_CopyOfBCM_Qo:	8/28/2003 12:22:40 I	5070	5	Unacceptable MOS [RALLOMBARDOC01
12	●	□	Open		12	BCM_DEMO_A	NortelBCM_BCM_QoSLog	8/28/2003 12:22:51 I	2002	5	Unacceptable MOS [BCM_DEMO_A to 12
28	●	□	Open		18	RALLOMBARDOC01	NortelBCM_BCM_HealthChe	8/28/2003 12:26:49 I	8220	15	Can not read status of Voice CTI
94	●	□	Open		45	RALDLOMBACN03	NortelBCM_Report_QoSSum	8/28/2003 10:47:32 /	1	35	Report created successfully. (Nortel BCM C

For Help, press F1 | Computers : 3 | Open Events: 54 | Running Jobs: 4 | Graph Data: 106 | 12:28 PM

Figure 15: NetIQ Vivinet App Manager

2.2.8.2.2 Nortel Enterprise Policy Manager (EPM)

Nortel Enterprise Policy Manager (EPM) is a single network-level application that allows administrators to manage network bandwidth, prioritize traffic streams and set network access policies. Nortel Enterprise Policy Manager is part of a comprehensive Nortel Management solution that includes Nortel Enterprise Network Management System for discovery, diagnostics and troubleshooting; Nortel Ethernet Switching Element Manager for online configuration of Ethernet switching devices; and Nortel Communication Server Manager for comprehensive enterprise voice management.

2.2.8.2.3 Enterprise Subscriber Manager

Enterprise Subscriber Manager is a powerful PC-based tool that simplifies, streamlines, and automates the management of Nortel PBX systems. With Enterprise Subscriber Manager you can save time and money every day and help maximize uninterrupted, quality phone service. Enterprise Subscriber Manager gives detailed reports on switch data and provides a single, easy-to-use interface to perform moves, adds, and changes (MAC).

2.2.8.3 Network Management

2.2.8.3.1 Nortel Enterprise Network Management System (ENMS)

Nortel Enterprise Network Management System, (formerly known as Optivity NMS) enables network administrators to identify and resolve problems and performance bottlenecks before they impact network services. ENMS is essential for maintaining user quality of experience in multi-cast video, IP Telephony, and other business-critical applications. While competitors require multiple systems to manage the network, Nortel offers one management system for wired and wireless, voice and data, and converged networks, making it more compelling for our customers to standardize on Nortel solutions.

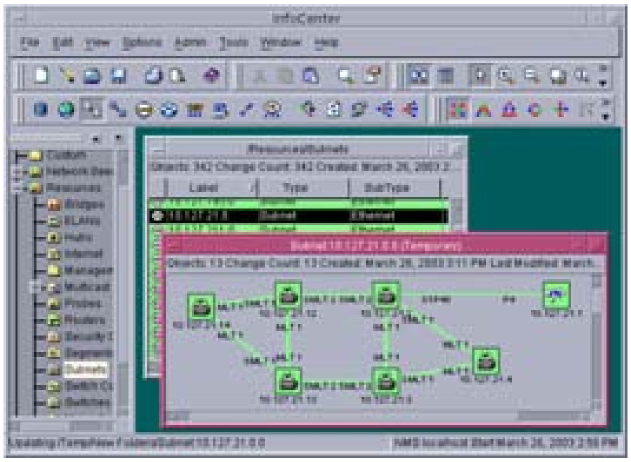


Figure 16: Enterprise Network Management System

Key Features

- Know when new devices are added to the network, through automatic discovery
- View what the network looks like, on a topology map, and where traffic bottlenecks occur
- Group faults together for easier troubleshooting
- Analyze network performance in real time
- Keep track of devices deployed in the network (inventory management)
- Managing Nortel VPN Router Deployments
    - Discover and visualize branch office VPN tunnels
    - IP-VPN view for monitoring and problem resolution
    - Fault propagation to IP-VPN view
- Managing IP Telephony deployments
    - Discover and visualize servers and gateways
    - Integrated fault management for IP Telephony interfaces
    - Performance measurement and reporting
    - PVQM alarm capabilities and integration with NetIQ Vivinet Manager
- Managing Virtual Private LAN Services
    - Discover and visualize VPLS tunnels on Optical Ethernet devices
    - Use VPLS view to track tunnels and VPN endpoints
    - Fault propagation to VPLS view

Key Benefits

- Control network management cost

  With new applications, network convergence, and increased security requirements, networks are more complex than ever. The automated discovery process and visualization capabilities in ENMS 10.2 help to reduce the complexity and control the costs of managing and maintaining a secure, high-performance converged network.

- Improve troubleshooting

  The organization relies on its network. Application or service downtime results in missed commitments and lost opportunities. The fault correlation and visualization capabilities in ENMS 10.2 give network managers the tools they need to quickly resolve and correct network problems. The intelligent fault engine in ENMS links the topology of the network to alarm conditions for consolidation and correlation of network faults – this helps the network manager quickly resolve fault or performance issues.

- Ensure converged network performance

  As companies consolidate servers and optimize their use of new applications and services, there is increased demand placed on the network. ENMS 10.2 has real-time performance analysis and visualization tools that help network managers to gauge and assess the impact of new applications and services on the network – helping to ensure acceptable levels of performance and reliability for all business functions.

  To further convergence deployment, Nortel has codeveloped a Proactive Voice Quality Management (PVQM) solution with NetIQ. This solution is a critical component in converged networks as it gives the network manager the capability to measure the user quality of experience for all IP Telephony communications. It also provides a system health status for IP Telephony server components. In this PVQM solution, Nortel Enterprise Network Management System provides troubleshooting and resolution for any performance degradation or fault conditions forwarded by the NetIQ Vivinet Manager. Now network managers have a methodology for ensuring the total quality of their IP Telephony deployments.

2.2.8.3.2 IP Address Domain Manager

The Nortel IP Address Domain Manager software solution provides automated IP Address, DHCP and DNS server management to increase IP network performance, availability and reduce costs associated with IP network management. IP Address Domain Manager minimizes downtime by streamlining IP address management. In addition, the software supplies innovative tools to simplify Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) management.

The Nortel IP Address Domain Manager software solution allows network managers to control IP addressing and standards-based DNS and DHCP services from a common interface, increasing the efficiency of management personnel and reducing the possibility of errors. Simplifying IP addressing is at the core of Nortel IP Address Domain Manager’s functionality. By providing a central platform from which an organization’s entire IP address domain can be managed as a whole, the software enables static addresses, dynamic addresses, and IP Address Domain Manager DNS and DHCP Servers to be effectively managed in relation to one another. Nortel IP Address Domain Manager also removes major technical barriers to DHCP implementations by supporting dynamic DNS (DDNS) updates and DHCP redundancy at every level of the product.

2.2.8.4 Element Management

2.2.8.4.1 Enterprise Switch Manager (ESM)

The Nortel Enterprise Switch Manager (ESM) provides a simple solution to the complex problem of configuring and managing Ethernet switches and WLAN configurations. It lowers the total cost of network ownership with reduced network administration costs and deployment time. Configuration time and errors are greatly reduced by configuring and monitoring Ethernet products with a simple point, click, and drag operation. This easy-to-use application expands the pool of administrators capable of performing complex network configurations. Enterprise Switch Manager is a key component for effectively configuring and maintaining the switches in an enterprise data network.

Enterprise Switch Manager (ESM) 4.0 is a Java™-based, real-time configuration management application for Nortel Ethernet products including Ethernet Switches, Ethernet Routing Switches, Application Switch Operating System (21.0 or higher), and WLAN devices. It enables network managers to discover, view, and configure more than 500 network devices and their physical links on a topology map. Network managers can import, export, or modify individual port settings, default gateways, SNMP traps, VLAN configurations, and product or image files.

Key Features

- VLAN Manager

  Configures and manages port, protocol, subnet or MAC-based VLAN configurations across switches in a network.

- MultiLink Trunk Manager

  Allows creation, deletion, and editing of MultiLink Trunking (MLT) and Split MultiLink Trunking (SMLT) membership information.

- Multicast Manager

  Configures multicast parameters and allows viewing paths of multicast streams across the network.

- Log Manager

  Enables network administrators to open, analyze, filter and sort syslog files for troubleshooting.

- Device Manager

  Provides a graphical representation of devices and provides remote configuration capabilities.

- Security Manager

  Manages access rights for Ethernet Routing Switches.

- File and Inventory Manager

  Enables configuration and upgrade/downgrade of devices networks as well as provides a centralized inventory of the same.

Key Benefits

- Operational Simplicity
  - Uses intuitive GUI for simplified device configuration
  - Platform independent (Java-based)
  - Unified management and configuration
  - One tool to configure Nortel LAN Campus devices
- High Availability
  - Presents system level view of network
  - Real-time graphical SNMP view
  - Support for configuring SMLT
- Lower Cost of Ownership
  - Lower network administration costs

    - Reduces time to deployment
    - Eliminates configuration errors
- Secure
    - SNMPv3 support
    - Allows password and community string changes in a bulk fashion using SSH (Secure Shell)

2.2.8.4.2 Optivity Telephony Manager (OTM)

The Nortel Optivity Telephony Manager (OTM) is a sophisticated package of application tools for managing Nortel Communication Server 1000 and Meridian 1 PBX systems. It is an integral part of Nortel strategy to help companies lower their total cost of ownership in operating and managing next-generation telephony networks. Companies can rely on Optivity Telephony Manager's integrated suite of management tools for configuration, control and analysis of their telephony network, either through a Windows graphical user interface (GUI) or web browser interface. In addition, Optivity Telephony Manager can be easily integrated with other Nortel management products to provide a complete management view of an entire converged network infrastructure.

Key Benefits

- User-friendly interface provides speed through everyday management tasks and shortens the learning curve.
- End-user self-management frees up skilled resources.
- Single point of data entry allows administrators to spend less time, eliminates duplication of effort, and provides increased accuracy.
- Provides a consolidated collection point for alarms and events for multiple devices so that administrators can monitor the health of their network from a single view.
- Extends the administration reach by providing access to documentation, phone configuration, maintenance tasks and alarm information from anywhere through the web browser.
- Allows customers to ensure that network investments are effectively utilized.
- Call monitoring and billing applications provide a mechanism for monitoring usage and detecting unauthorized system access.
- Reduced costs

2.2.9 Converged Applications and Clients

The Converged Campus solution described and detailed in the above sections provides the infrastructure for the media-rich clients. The infrastructure is a means and the applications and clients are the end. The ability to provide a secure, resilient, and high-performing infrastructure is key to enhancing productivity and the end-user experience. As applications and services converge onto a single infrastructure, it is critical to ensure resiliency and quality of service from end to end – the network is now mission critical to the Enterprise.

Many clients and applications can now take advantage of the Converged Campus. These include:

- IP Telephony
- IP Phones/IP Softphone 2050/Mobile Voice Client 2050
- Multimedia Communication Server (MCS)

- Unified Messaging
- Wireless VoIP

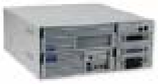
The following sections provide a brief overview of the solutions available for the Converged Campus.

2.2.9.1 Small IP Telephony Platforms – Business Communications Manager

The Nortel Business Communications Manager (BCM) 50/200/400 is an integrated communications platform for both multi-site enterprises and single-site small to medium-size businesses. Each delivers a highly reliable, innovative, converged voice/data solution that enables a business to save money by streamlining costs and to make money by increasing revenues, expanding market reach and improving customer service. The BCM delivers PBX functionality along with no-compromise voicemail and auto attendant features. Combined with its robust quality of service (QoS) routing capability, it provides a single cost-effective solution for both data and voice needs. As businesses grow, the BCM functionality can be extended with a simple key code to deliver business-critical applications that positively impact the bottom line. The BCM provides enterprise-level telephony and data services, all in an easily managed platform. From one platform, a business can cost-effectively extend its communication capabilities. The Nortel Business Communications Manager system's built-in routing capabilities and data services, such as firewall, web caching and network address translation (NAT), enable a business to connect its LAN to the Internet quickly, reliably and securely. The Nortel Business Communications Manager also offers an extensive range of communications applications – call center, unified messaging, VPN, auto attendant, wireless telephony – all accessed by simply entering a key code.

Nortel BCM 50

Nortel BCM 200


Nortel BCM 400

The top differentiators of the BCM 50/200/400 include:

- Comprehensive solutions that are easily implemented
- Choice of either IP-enabled or pure IP solutions
- Investment protection, because businesses may migrate without investing in completely new infrastructures
- The delivery of value-added applications, such as multimedia call center, IP Telephony, voice and data networking, virtual private networks (VPN), unified messaging and mobility
- Redundancy options, including power, fans and hard drive, which automatically detect failures and switch over seamlessly without any loss of service

2.2.9.2 Enterprise IP Telephony Platforms

The Nortel Enterprise IP Telephony offering is comprised of the Nortel Communication Server (CS) 1000 portfolio of fully featured IP-distributed communications systems that deliver the benefits of network convergence along with collaborative communications for today's increasingly "virtual" enterprise environment. The Communication Server 1000 portfolio includes the CS 1000S, 1000M, and 1000E platforms along with a variety of IP Communications Gateways and IP Remote Gateways. Nortel's innovative Remote Gateway Portfolio allows the enterprise to extend communications services to teleworkers and branch offices. With the wide variety of solutions, customers can choose the solution that best fits their needs based on branch office size, feature requirements, environment and budget.

The Communication Server 1000 platform operates on Nortel CS 1000 Software. It offers a robust set of telephony features coupled with new SIP-based functionality that provides a fully integrated multimedia solution. System administration is performed using Optivity Telephony Manager along with Element Managers.

- Nortel Communication Server 1000 portfolio
  - Communication Server 1000 Software
  - Communication Server 1000S
  - Communication Server 1000E
  - Communication Server 1000M Chassis/1000M Cabinet/1000M Single-Group (SG)/1000M Multi-Group (MG)
- CS 1000 Element Manager
- Nortel Media Gateway 1000 portfolio
  - Media Gateway 1000S
  - Media Gateway 1000E
  - Media Gateway 1000T
- Nortel Remote Media Gateway portfolio
  - Media Gateway 1000B
  - Survivable Remote Gateway portfolio
  - Survivable Remote Gateway 50 (built on BCM 50 platform)
  - Survivable Remote Gateway 1.0 (built on BCM 200 and BCM 400 platforms)
  - Remote Gateway 9100 Series
  - Remote Gateway 9115
  - Remote Gateway 9150
- Nortel Optivity Telephony Manager (OTM)

2.2.9.2.1 Nortel Communication Server 1000

The Nortel Communication Server 1000 portfolio is an enterprise IP Telephony solution supporting a flexible mix of phones, applications and PSTN gateways connected over a converged network. Telephones supported include IP phones, digital Time Division Multiplexing (TDM) phones, analog TDM phones, DECT cordless and 802.11 wireless LAN phones as well as software phones on PCs and PDAs. The Communication Server 1000 contains all the business telephony features and services developed for the market-leading Nortel Meridian 1 PBX, plus new innovative features for IP convergence. It supports business applications for personal productivity, team productivity, mobility, customer service and management control. The Communication Server 1000 also provides advanced networking services to other Nortel and non-Nortel equipment using industry standards to protect customer investments and to keep total cost of ownership among the lowest in the industry.

Key areas of the Communication 1000 portfolio include:

- Distributed architecture over converged network
- Software built upon the highly reliable, feature-rich Meridian PBX feature set

- Full application portfolio support – Nortel and Developer Partner Program compatible applications
- Multiple built-in reliability mechanisms – no single point of failure, robust operating systems per call server (100 000 in a centrally managed network)
- Highly scalable – from 1000 to 15 000 IP clients per call server (100 000 in a centrally managed network)
- Centralized management control and dialing plan for 100 000 IP clients
- Centralized and networked business communication services
- IP Telephony service overlay that works on any open standards-based data network
- Optional support for campus and geographic redundancy with CS 1000E

2.2.9.2.1.1 Nortel Communication Server 1000S

The Communication Server 1000S is a fully distributed IP Telephony solution with all of the features and capabilities of a PBX, designed primarily to support Nortel IP Phones, but with support for analog and digital phones as well.

- Scalable – supporting up to 1000 IP clients per call server
- Distributed Call Server and Gateways
- Redundant Gatekeepers, Gateways and Client Proxies
- WAN Gateway survivability
- Uses Media Gateway 1000S (up to four per system) to provide local access to TDM devices such as RAN/Music, Conference/Tones, Analog/Digital lines and Analog/Digital
- Seamless network integration, simplified management, greater flexibility in deployment and reduced support costs

2.2.9.2.1.2 Nortel Communication Server 1000E

For enterprises that want to deploy a full IP PBX architecture supporting a large number of users, the Communication Server 1000E can be deployed either at a single location or distributed throughout a QoS managed IP network. The Communication Server 1000E introduces a redundant call processor configuration.

- Scalable – supporting up to 15 000 IP clients per call server
- Redundant Call Servers, Gatekeepers, Gateways and Client Proxies
- Campus Mirroring – known as “split core,” allows active and inactive call servers of the system to be physically separated up to 25 miles (40 km) across a campus using a high-speed link
- Geographic Redundancy – allows for a redundant CS 1000 system to be deployed at a remote location over any distance through the WAN to take over call processing if the primary system fails or is the subject of a major disaster
- Uses Media Gateway 1000E (up to 30 per system) to provide local access to TDM devices, to support Analog/Digital lines and to support Analog Trunks
- Uses Media Gateway 1000T to provide Digital Trunk PSTN access

2.2.9.2.1.3 Nortel Communication Server 1000M

The Communication Server 1000M transforms a Nortel Meridian 1 PBX into an IP PBX. Equipped with signaling servers and running on Communication Server 1000 software, the Communication Server 1000M functionally is no different than that of a CS 1000S/E. It is available in the following configurations:

- Communication Server 1000M – Cabinet/Chassis (11C Cabinet/Chassis)
- Communication Server 1000M – Half-Group (51C)
- Communication Server 1000M – Single Group (61C)
- Communication Server 1000M – Multi-Group (81C)

The Communication Server 1000M supports:

- Scalable up to 15 000 IP clients per call server and 16 000 digital or analog clients
- Redundant Centralized Call Processor and Gateways
- Distributed Remote Gateways • Integrated Media Gateways for trunk and line application interfaces
- Provides investment protection and allows for migration to IP Telephony

2.2.9.2.2 Nortel Communication Server 1000 Element Management

CS 1000 Series System Management Systems Management is performed using the Nortel Optivity Telephony Manager along with Element Manager. Element Manager is a simple, user-friendly web-based interface that supports a broad range of system management tasks, including:

- Configuration and maintenance of IP Peer and IP Telephony features
- Configuration and maintenance of traditional routes and trunks
- Configuration and maintenance of numbering plans
- Configuration of Call Server data blocks
- Maintenance commands, system status inquiries, backup and restore functions
- Software download, patch download and activation

Element Manager resides on the Signaling Server and can be accessed directly through a web browser or through Optivity Telephony Manager. The Optivity Telephony Manager System Navigator includes integrated links to each network system and its respective instances of Element Manager.

2.2.9.2.3 Nortel Media Gateway 1000

Distributed throughout the IP network, Nortel Media Gateway 1000 acts as a bridge between IP and traditional telephony networks (such as the PSTN) by housing various cards that perform line, trunk and translation functions. The hardware for the entire Media Gateway 1000 portfolio has the same characteristics: four slots that can be used for media cards, analog and digital line cards, analog and digital trunk cards as well as various applications.

2.2.9.2.3.1 Nortel Media Gateway 1000S

The Media Gateway 1000S is used with the Communication Server 1000S to support PSTN trunks, analog/digital telephone resources, TDM application cards and Voice Gateway Media Cards. Each Media Gateway can support one Media Gateway Expander. The Media Gateway 1000S contains a gateway controller card (called SSC card) and four slots for flexible configurations of line, trunk and application cards. The SSC card controls the interface and application cards and acts as a call processor in the survivable mode. The Call Server database is automatically synchronized onto this controller. Application cards provide interfaces to applications such as CallPilot and Nortel Integrated Applications portfolio.

2.2.9.2.3.2 Nortel Media Gateway 1000E

The Media Gateway 1000E is used with the Communication Server 1000E to provide basic telephony media services – including tone detection and generation and conference – to phones. It operates under direct control of the call server and can support an optional Media Gateway 1000E Expander. The Media Gateway 1000E contains a gateway controller card (called SSC card) and four slots for IPE cards and Voice Gateway Media Cards. The Media Gateway 1000E supports CallPilot and Nortel Integrated applications. It also provides direct physical connections for digital and analog (500/2500-type) telephones as well as analog trunks for telephone and fax.

2.2.9.2.3.3 Nortel Media Gateway 1000T

The Media Gateway 1000T provides the Communication Servers 1000E/S with digital trunk and Primary Rate Interface (PRI) access to the PSTN and to other PBX systems. The Media Gateway 1000T contains a gateway controller card (called SSC card) and four slots for IPE cards. It also supports an optional MG 1000T Expander. Unlike the MG 1000Es, the MG 1000T platform does not operate under the direct control of the CS 1000E Core Call Servers. Instead, the MG 1000T provides the primary processing for the MG 1000T platform. The MG 1000T Core SSC card controls the circuit cards in the MG 1000T Core and all cards in up to four MG 1000T Expansions. The MG 1000T supports Media Cards, Digital PSTN Interface Cards (E1, T1, ISDN), Analog Trunk Cards, Service Cards and DECT Mobility Cards.

2.2.9.2.4 Nortel Remote Gateway

Nortel offers a wide variety of remote gateway solutions that extend enterprise communications to teleworkers and remote offices. With Nortel Remote Gateway 9100 Series, the enterprise can extend more than 450 features and system resources to those working away from the main office, while leveraging the investment of a central corporate PBX. Using the Nortel Survivable Remote Gateway (Release 1.0) and Survivable Remote Gateway 50, an enterprise under network failure conditions can continue telephone services in a cost-effective manner for IP clients at even the smallest remote sites. Using Nortel Media Gateway 1000B, up to 400 users can be distributed across an IP WAN in a survivable environment that supports the same analog and digital line and trunk cards and phones as that of the main site.

2.2.9.2.4.1 Nortel Media Gateway 1000B

The Media Gateway 1000B allows larger groups of users to be distributed across an IP WAN to branch office sites with seamless feature and application transparency with a Communication Server 1000 at the main site. It supports up to 400 IP users and provides access to an array of PSTN trunk types as well as line interfaces located at the branch office. IP Phones at the branch office are managed from the main site. The survivability feature allows IP Phones that are centrally managed from the main site to fail over to survival mode, retaining all available features. Survival mode engages automatically if the IP WAN fails and reverts back when the IP WAN is back to normal operation.

2.2.9.2.4.2 Nortel Survivable Remote Gateway

The Nortel Survivable Remote Gateway (SRG) 1.0 (BCM 200) and SRG 1.0 (BCM 400) seamlessly extend the services and applications of a Nortel Communication Server 1000 Series system at a headquarters site to the smallest remote sites. In addition to the SRG 1.0 (BCM 200) and the SRG 1.0 (BCM 400), there is a new “mini” model for the smaller branch office, known as the Nortel Survivable Remote Gateway (SRG) 50 (available Q3 2005). Introduced with

Communication Server 1000 Software Release 4.5, it is cost optimized for sites ranging from 5 to 32 users.

While the Nortel SRG 1.0 platform is based on the market-leading small site IP telephony solution and Nortel Business Communications Manager 200 and 400, the Nortel Survivable Remote Gateway 50 is based on the BCM 50. The SRG series has been designed to provide continued telephony services for IP clients under network failure conditions – and to do so in a very cost-effective manner at smaller locations.

The SRG portfolio is not only cost effective at smaller sites, but also provides highly reliable solutions that include the intelligence to drive Nortel IP terminals while providing IP routing capabilities and a suite of PSTN interfaces to enable local PSTN access. SRGs are capable of addressing the needs of smaller branch offices ranging in size from 5 to 80 users.

2.2.9.2.4.3 Nortel Remote Gateway 9100 series

The award-winning Nortel Remote Gateway 9100 Series provides an ideal solution for extending cost-effective, high-quality communications to remote teleworkers and remote offices. The Nortel Remote Gateway 9115 extends the features and functions of a Nortel Meridian 1 PBX, Meridian SL-100, or Communication Server 1000 (CS 1000) system out to a single telephone at a small remote office or telecommuter home office, utilizing a standard IP-based network connection and/or an analog PSTN telephone line and a Nortel Meridian digital telephone. The Nortel Remote Gateway 9150 is a powerful option for extending these features and functions to remote branch offices using up to 32 Nortel Meridian digital telephones and a standard IP-based connection and/or PSTN circuit-switched telephone lines. With each Nortel Remote Gateway solution, the remote workers have full access to the corporate telephone network, just as if they were working at the main corporate site. All of the more than 450 features and system resources enjoyed in the main office are available remotely, such as unified messaging, the corporate directory, and corporate dialing plans, as well as features such as boss-secretary filtering, audio conferencing, and automatic call distribution.

The Remote Gateway Series 9100 products are configured and maintained using the Remote Gateway 9100 Series Configuration Manager software, a Windows™-based application that is installed on a PC. It provides a simple Configuration Wizard for initial installation that prompts the user, obtaining the minimum information needed to get the remote site communicating with the main site.

2.2.9.3 IP Phones/IP Softphone 2050/Mobile Voice Client 2050

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/or 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.

2.2.9.3.1 Nortel IP Phone 2001

- Multi-line 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 in-line 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

2.2.9.3.2 Nortel IP Phone 2002

- Multi-line 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 in-line power from 802.3af-compliant switches
- Desk or wall mounting
- ADA-compliant dialpad

2.2.9.3.3 Nortel IP Phone 2004

- Multi-line 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 in-line power from 802.3af-compliant switches
- Desk or wall mounting
- AD-compliant dialpad

2.2.9.3.4 Nortel IP Phone 2007

- Multi-line 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 in-line 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 (set has built-in amplifier)
- User-selectable ringtones
- Adjustable LCD brightness and contrast
- Personalized soft keys
- Desk or wall mounting
- ADA-compliant dialpad
- Integrated three-port switch

2.2.9.3.5 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
- 10 fixed keys (Line, Release, Hold, Mute, Volume Up Down, Messages, Services and Scroll Up/Down)
- Intelligent and Synchronized status indicaton 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 or direct in-line power from 802.3af-compliant switches
- Automatic IP address assignment with DHCP

2.2.9.3.6 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 Communication 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
- Message waiting indicator alerts users to new voice messages and incoming calls
- Supports direct headset connection through PC USB port
- 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
- TAPI compliance for operation with other telephony applications

2.2.9.3.7 Nortel Mobile Voice Client 2050

The Nortel Mobile Voice Client 2050 (MVC 2050) also extends access to the same services and capabilities as the Nortel IP Phones 2002 and 2004, but it uses a pocket-PC PDA. The Nortel MVC 2050 delivers the convenience of a single, extremely portable device that allows mobile workers to take advantage of the easy-to-use, rich, reliable, and secure business telephony features from Nortel Communication Servers. The Nortel Mobile Voice Client 2050 supports the following features:

- Centralizes business applications access over an 802.11b WiFi connection, eliminating the need for stand-alone voice and data devices
- Thirteen fixed keys, which include hold, answer/originate, goodbye, mute, volume up, volume down, directory, services, messages, shift, expand, copy and quit
- Four programmable interactive soft label keys
- Ability to synchronize Microsoft Outlook contact lists with the PC using ActiveSync or beam to another PDA
- Customized online Help with full index search capabilities
- Customer choice in headset and headphone options (use of headset or headphone varies by type of PDA)
- Global IP sounds (GIPS) software from NetEQ as standard, supporting packet loss concealment up to 30 percent in high packet loss environments

2.2.9.4 Multimedia Communication Server 5100

The Nortel Multimedia Communication Server (MCS) 5100 is the Nortel enterprise multimedia applications solution, providing innovative communications, real-time collaboration and productivity services for enterprise users. Nortel MCS 5100 uses open, industry-standard hardware to evolve TDM as well as IP networks to highly collaborative multimedia networks. Nortel MCS 5100 is seamlessly deployed alongside an enterprise's current network infrastructure, enriching the enterprise user's communications experience and providing new SIP multimedia applications.

The Nortel MCS 5100 supports an impressive suite of integrated multimedia capabilities that allow users to enjoy a feature-rich multimedia experience. The following summarizes the key capabilities:

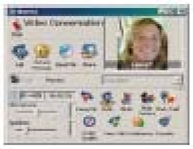
- Desktop video calling is delivered through coordinated video display on the PC screen and audio conversation through the hard or soft client. Low-cost desktop multi-point video conferencing extends video to all users.
- Presence – Notification is provided on the status of a "watched" user. When a user is on the phone, dynamic presence shows the person as on the phone, and when a user is away from their desk, the presence changes to inactive.
- Picture calling line ID – Incoming and outgoing communications present a picture of the originating caller on the PC screen along with CLID.
- Personal agent – Call screening – This user-friendly html (web) interface provides a Find me/Follow me service, with call screening provisioning for communication personalization. Users define who, where, when, and how callers can reach them. Calls

can be screened and routed based on the individual caller (or group), or on when calls are received (time of day, day of week). Calls can be directed to try multiple locations at once (office, cell phone and house), or to ring sequentially one after the other, or a combination. This solution set provides tremendous flexibility and control of the communication experience.

- Network-based incoming and outgoing call logs are kept for easy access and retrieval.
- Directory – Personal and global directories allow users to store information and utilize these directories for click-to-call capability.
- Click to Call – This feature can be used from the directory on the multimedia PC client, from the incoming/outgoing call logs, or from the Outlook contact or inbox.
- Mobility solution – The multimedia PC client can provide the primary voice service for users who are not in their office, or those who do not leverage their existing voice infrastructures.
- Conferencing – “Meet-Me” media conferencing delivers multimedia services, such as visual notification to the conference chair of all participants entering or leaving the conference. Conferencing also supports file exchange, web push and cobrowse, and allows Instant Message Chat for side-bar real-time communications. This solution set delivers a very impressive return on investment (ROI) over outsourced conference solutions, as well as improved functionality.
- Collaborative applications – The Nortel MCS 5100 provides a suite of applications such as Instant Messaging, web collaboration, IM Chat, file sharing, white boarding and web pushing. Video conferencing is another key application in today’s collaborative environments, improving the effectiveness of distance conferencing.
- PDA support – Many MCS 5100 applications are supported on PDA devices such as the RIM Blackberry, giving users extended use of presence, secure Instant Messaging, Click to Call and Route Management.

2.2.9.4.1 Nortel Multimedia Clients

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 Clients. 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.

2.2.9.5 Unified Messaging

Nortel Messaging solutions incorporate the latest technology and add web-based graphical user interfaces to bring feature-rich communications to the desktop or mobile device while making message management easy and effective. For any size enterprise, the Nortel Messaging portfolio of products provides unified, personalized messaging to both office and mobile or remote workers.

2.2.9.5.1 Nortel CallPilot

CallPilot is a unified messaging tool that brings together voicemail, e-mail and fax to create a personalized, feature-rich communications and message management system. CallPilot incorporates the latest technology, including advanced speech activated messaging and e-mail-by-phone, which enables access to messages using telephone user interface (TUI) through either voice commands or dual tone multi frequency (DTMF) tones from virtually anywhere. CallPilot builds on the customer-driven functionality of proven Nortel messaging products, and adds web-based graphical user interfaces (GUI) to make system management easy and effective.

The CallPilot portfolio includes CallPilot 100/150 (Current Software Release 3.5) for the Nortel Norstar Integrated Communications System, CallPilot Unified Messaging (Current Software Release 3.0) for the Nortel Communication Server 1000 Series, and CallPilot as an integrated version for Business Communications Manager 50/200/400.

2.2.9.5.2 Nortel Hospitality Messaging Server 400

The Hospitality Messaging Server 400 (HMS 400) replaces the Meridian Mail HVS as the messaging solution for the hospitality industry. It is a global product with multi-language support. The HMS 400 platform provides ample resources to add additional features and capabilities in the future. It is scalable up to 7000 users with the choice of single server or multi-server configurations.

2.2.9.6 Wireless VoIP

Nortel WLAN Handsets 2210, 2211 and 2212 are mobile phones for workplaces with Nortel communication servers. Nortel WLAN Handsets reside on the wireless LAN with other wireless devices using direct sequence spread spectrum (DSSS) radio technology. They operate over an 802.11b wireless Ethernet LAN, providing users a wireless voice over IP (VoIP) telephony extension, sending and receiving packets at up to 11 Mbps. Quality of service on the wireless LAN for IP Telephony is provided through the WLAN Telephony Manager 2245. The WLAN Application Gateway 2246 is an open application interface (OAI), which enables third-party software applications to communicate with the Nortel WLAN Handsets. By seamlessly integrating with the infrastructure IP telephony system, wireless telephone users are provided with high-quality mobile voice communications throughout the workplace. The wireless telephone gives users the freedom to roam throughout the workplace while providing all the features and functionality of an IP desk phone. The Nortel WLAN IP Telephony Handset is one of the components of the Nortel WLAN IP Telephony solution.

Please refer to the *Wireless VoIP Solution Guide* for a detailed overview of the entire Wireless LAN solution.

3. Converged Campus Summary

The Converged Campus solutions presented in this guide show the components, features, and functionality available when implementing a Nortel solution. Nortel is uniquely positioned to provide a secure, resilient infrastructure capable of supporting a wide range of converged applications, including data, multimedia, and voice applications. By taking a solutions approach to the Converged Campus, this guide highlights the areas of concern during design and provides recommendations and best practices when implementing an end-to-end solution.

3.1 Performance Scalability and Interoperability

The performance, scalability, and interoperability of the Converged Campus solution is a major competitive differentiator for Nortel. Several third-party test results have been published, along with internal testing on the various components within the solution.

The following Tolly Group reports highlight the performance, scalability, interoperability, and resiliency of the Nortel Ethernet switching products.

- Nortel Networks
  Passport 8600
  High Availability and Reliability Evaluation
  (No. 202123)

- Nortel Networks
  Passport 8600 and BayStack 470-48T
  Layer 2 & Layer 3 Interoperability Evaluation
  (No. 202142)

- Nortel Networks Ltd.
  Passport 8600 Routing Switch
  Layer 2/3 Performance
  (No. 203106)

- Nortel Networks
  BayStack 425, 470, 460 and 5510 Switches
  Layer 2 Interoperability Evaluation – Convergence Focus
  (No. 204112)

- Nortel
  Ethernet Routing Switch 8600 and Ethernet Routing Switch 5520/5530
  Performance Evaluation of Nortel Resilient Terabit Cluster Solution
  (No. 205116)

3.2 Deployment Scenarios

The Convergence Lab within Nortel has implemented the Converged Campus solution described in this guide along with the WLAN 2300 solution. The Convergence Configuration Guide documents all the various configurations necessary to demonstrate interoperability and performance of the converged solution components. This document details the exact configurations of all the equipment to ensure full mobility of Voice over IP, whether wired or wireless, using the designs and best practices described in this guide.

- *Convergence Configuration Guide with WLAN 2300*

Contact us:

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

http://www.nortel.com

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