NORTEL NETWORKS

BUSINESS WITHOUT BOUNDARIES

Product Brief

Nortel Networks BayStack 470 Switches

- High-density desktop connectivity up to 384 ports
- Cost-effective, plug-and-play with built-in stacking ports
- Two built-in GBIC uplinks for highest uplink capacity and flexibility
- Flexible stacking across different BayStack switches—a stack is managed as a single entity with a single IP address
- Simple software upgrades with single image for different switches
- Resilient connectivity for minimal network downtime
- Fail-safe stacking design assures continuous uptime
- Network availability with QoS features
- Secure access and data traffic protection
- Common look and feel minimizes training and installation costs

Part of the successful Nortel Networks BayStack* family, BayStack 470 Switches are stackable 10/100 Mbps Ethernet Layer 2 switches. BayStack 470 Switches include two built-in GBIC (Gigabit Interface Converter) uplink ports and built-in stacking ports in a compact, one rack-unit high design. They are designed to provide high-density desktop connectivity for mid-size and large enterprise customers' wiring closets.

BoSS (BayStack operating-system Switching Software) allows BayStack 470 Switches to stack with other BayStack switches. BoSS also simplifies software upgrades with a single image for different BayStack switches.

BayStack 470 Switches' comprehensive Quality of Service (QoS) features are designed to ensure connectivity and network availability by managing and prioritizing data traffic for maximum performance. These switches offer a scalable, resilient solution that minimizes capital and operational expenses. Their robust security features offer protection against unauthorized access to data traffic.

The BayStack 470 Switches are available in two models—the BayStack 470-48T Switch and the BayStack 470-24T Switch *(Figure 1)*.

High-density, high-speed desktop switching

The BayStack 470-48T Switch features 48 10/100BASE-TX RJ-45 ports for desktop switching and two built-in GBIC ports for uplink. Port 47 and Port 48 offer configuration flexibility by allowing the network administrator to configure each port as either 10/100BASE-TX or make use of the built-in GBIC. Up to eight BayStack 470-48T Switches can be stacked to achieve up to 384 10/100 ports that can be easily managed as a single unit. The 2.56-Gbps cascading bandwidth offers dedicated bandwidth between switches without sacrificing any uplink ports. The uplink ports can be used for connections to backbone switches such as the Passport* 8600 Switch.

The BayStack 470-24T Switch offers 24 10/100BASE-TX RJ-45 ports for desktop switching and two built-in GBIC ports for uplink. All 26 ports may be used simultaneously. Up to eight BayStack 470-24T and 470-48T switches may be combined in a single stack for maximum flexibility.

The BayStack 470 Switches can also be stacked with BayStack 460-24T-PWR, BayStack 450, and BayStack Business Policy Switch. (BoSS 3.1 is the last revision to support the Business Policy Switch.)

Full autosensing on every port

Every UTP port on the BayStack 470 Switch is equipped with autosensing technology to automatically detect and support the speed and mode of a connected device. The ports determine whether a connected device is operating at 10 Mbps or 100 Mbps, and automatically adjust to the optimal speed. Each of the switched ports also automatically detect and support full-duplex connections to servers, power-user end-stations, or other switches, as well as half-duplex connections to legacy NICs or hubs.

BayStack 470-24T

BayStack 470-48T

Figure 1. The BayStack 470 Switches

Two built-in GBIC ports

BayStack 470 Switches have two built-in GBIC ports for dedicated uplink connectivity to network core switches such as the Passport 8600. This doubles the uplink bandwidth as GBIC ports are not required for stacking purposes. Using the Distributed Multi-Link Trunking, up to 16 GBIC or 10/100BASE-T ports are available for pure uplink connectivity in a full stack—the highest in the market.

Innovative built-in stacking ports

BayStack 470 Switches have built-in stacking ports for simpler, quicker, and more cost-effective stacking, as cascade modules are not required. This unique stacking design frees up both of the uplink ports for dedicated connectivity to the backbone.

BoSS (BayStack operating system Switching Software)

With the release of BoSS, Nortel Network became the first vendor to offer a single software image that can support four different switch types: BayStack 460-24T-PWR, BayStack Business Policy Switch, BayStack 470-48T, and BayStack 470-24T. BoSS simplifies network operations and provides the flexibility of stacking different switches in the same stack.

Simplified network operations

BoSS simplifies network operations by reducing the number of steps required for switch software updates. With BoSS, you need to download only a single image from Nortel Networks for four different switch types. Loading the image to different switches is also considerably simplified. The image is loaded only to the base unit of the stack which automatically loads it to other switches in the stack. Finally, keeping track of the version numbers is much easier as only one version number needs to be remembered.

Figure 2. Stacking with existing BayStack 450 or BPS stacks

Flexible stacking with other BayStack Switches

Using BoSS, the BayStack 470 Switches are able to stack with other BayStack switches *(Figure 2)*. Two types of stacks are supported:

- BayStack 470-48T can stack with any combination of BayStack 470-24T, BayStack Business Policy Switch, and BayStack 460-24T-PWR.
- BayStack 470-24T can stack with any combination of BayStack 470-48T, BayStack Business Policy Switch, BayStack 460-24T-PWR, and BayStack 450.

It should be noted that the BayStack 470-48T cannot be stacked with BayStack 450.

BoSS protects customers' existing investment in BayStack 450 and BayStack Business Policy Switch stacks by allowing newer, feature-rich and cost-effective switches—such as the BayStack 470-24T—to stack with the legacy stacks.

Using BoSS, a maximum of eight switches can be stacked together in any valid combination *(Table 1)*.

Table 1. Stacking matrix

	BayStack 460-24T-PWR	BayStack 470-24T	BayStack 470-48T	BayStack Business Policy Switch	BayStack 450
BayStack 460-24T-PWR with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 470-24T with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 470-48T with BoSS v3.1	Yes	Yes	Yes	Yes	No
BayStack Business Policy Switch with BoSS v3.1	Yes	Yes	Yes	Yes	Yes
BayStack 450†	Yes	Yes	No	Yes	Yes

Note: † BayStack 450 must have BayStack 450 software v4.2 or higher. BoSS v3.1 is the last revision that will support BayStack BPS.

BoSS v3.1 features

BoSS version 3.1 is downloadable from the Web for free and includes support for the following new features, in addition to those supported in v3.0:

- 802.3ad link aggregation
- Unit replacement feature
- User-based policies
- Copper GBIC support
- Custom autonegotiation advertisements (CANA)
- ASCII configuration generator
- Simple Network Time Protocol (SNTP)
- Enhanced message logging

802.3ad link aggregation

IEEE 802.3ad provides an industry-standard method for bundling multiple links together to form a single trunk between two networking devices. BoSS 3.1 supports both Dynamic Link Aggregation Group (LAG) trunks and MLT trunks. Once configured, the Link Aggregation Group or trunk group is managed by the Link Aggregation Control Protocol (LACP). BayStack supports both Link Aggregation and MLT groups. Up to six LAG or MLT groups are supported. The maximum number of active links per group is four. The link aggregation allows more than four links to be configured in one LAG. The first four high-priority links will be active links and the lower-priority link will be the standby link. When one of the active links goes down, the standby link will become active. This feature can be implemented by using Command Line Interface (CLI), Device Manager, or SNMP.

Unit replacement feature

In the unlikely event that a switch fails in a stack, the affected switch can easily be replaced without disrupting the stack. This feature provides the capability of upgrading a new unit with the configuration of the affected unit off-line, before adding the new unit to the stack. The configuration of the affected switch may be copied from the Trivial File Transfer Protocol (TFTP) server to the new switch. The new switch can then be inserted into the stack without requiring a reboot of the entire stack. This feature can be implemented by using menu, Web interface, or CLI commands.

User-based policies

This feature enables network services (i.e., QoS) to follow the user regardless of the PC logged into or the port connected to. The switch requires a user to be authenticated using EAP and sends username/password information to the Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS server provides the user's role/group attributes to the switch that allows user access to the port with the default configuration. The switch then passes role/group/port information to the Optivity* Policy Services (OPS) server that configures the user port based on the specific policy information.

Custom Autonegotiation Advertisements (CANA)

This feature enables the network manager to tune the capabilities that a particular Ethernet port can advertise via autonegotiation. The capabilities include half-duplex and full-duplex modes with speeds of 10, 100, and 1000 Mbps. Autonegotiated Ethernet ports establish a connection based upon the highest common capabilities. This feature is implemented by using CLI commands and saves the network manager from having to go to each workstation and switch to configure a “fixed” speed.

ASCII configuration generator

The ASCII configuration generator allows the configuration settings of the switch to be displayed or saved to an external ASCII configuration file made up of a series of CLI commands. This editable ASCII configuration file can then be uploaded to a switch from an external file server.

The ASCII configuration file contains configuration settings for the following network management applications:

- Core applications (system information, topology, etc.)
- Internet Protocol
- Multi-Link Trunking (MLT)
- Port configuration

- Partial Spanning Tree configuration, including configuration of port priority and path cost
- VLAN configuration
- Quality of Service (QoS)
- RMON

Simple Network Time Protocol (SNTP)

Simple Network Time Protocol allows the synchronization of the switch or stack's clock to the real-time clock on the SNTP server. If the system (switch or stack) uses SNTP, then SNTP time is used to time-stamp system log (Syslog) messages. If SNTP is not in use, then the system uses a time-stamp relative to boot time.

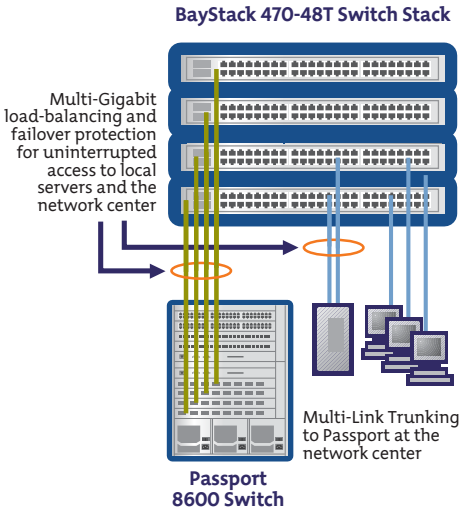
Enhanced message logging

Several new features have been added for enhanced message logging. Log entries can now be time-stamped in real time when the SNTP is in use. With the remote logging feature, the system has the ability to copy internal system log messages onto a remote Syslog server. Lastly, the *Show Logging* feature gives the administrator flexibility to view and sort the login entries in forward or reverse manner.

Multi-Link Trunking

Multi-Link Trunking (MLT) enables grouping of links between the BayStack 470 and another switch or server to provide greater bandwidth with active redundant links. With Nortel Networks unique Distributed Multi-Link Trunking (DMLT) feature, trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center. This can provide greater bandwidth of up to 800 Mbps (when used with 10/100 ports) or up to 8 Gbps (when used with Gigabit uplink ports) with active redundant links in one trunk. Up to six trunks are supported per switch or stack *(Figure 3)*.

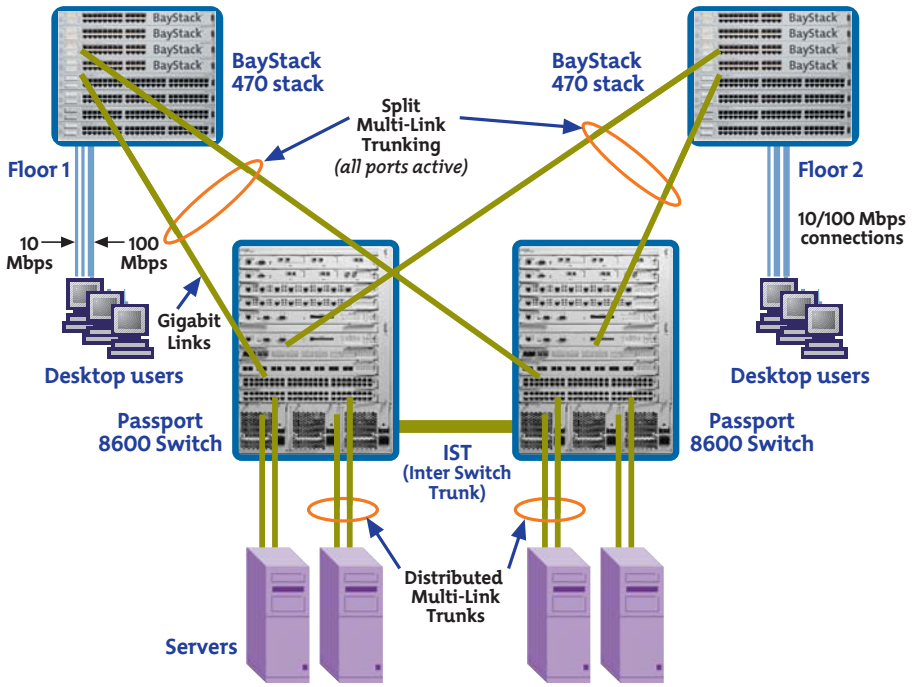
Figure 3. Distributed Multi-Link Trunking across stack for higher bandwidth and fault tolerance



The BayStack 470's ability to have multiple connections to a Passport 8600 network core using the Split Multi-Link Trunking (SMLT) feature of the Passport 8600 allows customers to double their network bandwidth with no extra investment. The Passport 8600 provides a self-healing network which delivers the reliability and availability required by today's mission-critical applications. By combining the reliability of the Passport 8600 with the resilient trunking features of the BayStack 470, such as DMLT and MLT, Nortel Networks has created the next generation of flexible networking solutions.

For example, an enterprise solution consisting of BayStack 470 Switch stacks in the wiring closets, collapsing in to the network core switch (Passport 8600), provides high-density desktop connectivity as well as fault-tolerant connections to core switch and mission-critical servers *(Figure 4)*.

Figure 4. Split Multi-Link Trunking (SMLT)



Redundancy

With connectivity to the BayStack 10 Power Supply Unit (PSU), paired with a –48V DC-to-DC converter module, BayStack 470 Switches deliver redundant power supply (RPS) support crucial in mission-critical environments. The Uninterruptible Power Supply (UPS) capability is supported on the switch with BayStack 10 PSU.

Enhanced security

BayStack 470 Switches offer the highest level of security with features including Secure Shell (SSH), IEEE 802.1x based security (also known as Extensible Authentication Protocol - EAP), Simple Network Management Protocol (SNMPv3), IP Manager's list, MAC address-based security, and RADIUS authentication.

SSHv2 supports strong authentication and encrypted communications. It allows a user to log into the switch from an SSH client and perform a secure Telnet session using CLI commands. This feature is ideal for security conscious customers such as federal governments.

For added security, BayStack 470 Switches support the 802.1x-based security feature—EAP. Based on the IEEE 802.1x standard, EAP limits access to the network based on user credentials. A user is required to "login" to the network using a username/password; the user database is maintained on the authentication server (not the switch). EAP prevents network connectivity without password authorization for added security and control in physically non-secure areas. It is used where the network is not 100 percent physically secure or where physical security needs enhancement—for example, banks, trading rooms, or classroom training facilities. EAP supports client access to the network and interoperates with Microsoft Windows XP and other standards-based clients.

SNMPv3 provides user authentication and data encryption for higher security. It also offers secure configuration and monitoring.

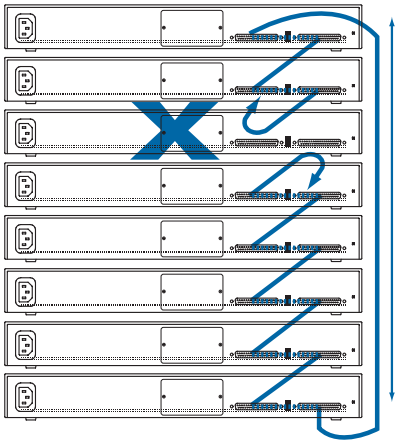
IP Manager List limits access to the management features of BayStack 470 Switches by a defined list of IP addresses, providing greater network security and manageability.

The BayStack 470 Switches feature BaySecure* MAC address-based security, which allows authentication of all access, not only to the switches for management and configurations but also access to the infrastructure through these switches. This software feature limits access to only network authorized and trusted personnel, including full tracking of network connections. With BaySecure, network access is granted or denied via proper MAC address (up to a maximum of 448) identification. In addition, with the Distributed Access List Security feature, network access is granted or denied on a per-port basis. BayStack 470 Switches also provide RADIUS authentication for switch security management.

Fail-safe stacking and resiliency

A key differentiator for BayStack 470 Switches is their resilient stacking feature. BayStack 470 Switches can stack up to eight units with a cascade stacking design, assuring continuous uptime even if a single switch in the stack should fail. A loop-back or cascade cable is used to seamlessly connect the entire stack to provide no single point of failure *(Figure 5)*.

Figure 5. In the unlikely event of a switch failure, the stack integrity is maintained: cascade signals loop back at point of failure.



Common look and feel

All BayStack switches, including the BayStack 470, have a common "look and feel" which minimizes training costs. This allows the switches to be managed in a similar fashion via a broad set of management tools. These tools include Web, Java™-based Device Manager (JDM), Command Line Interface (CLI), menus, Optivity Network Management System (ONMS), Optivity Switch Manager (OSM), and Optivity Policy Services (OPS).

MAC addresses

BayStack 470 Switches support up to 16,000 MAC addresses per switch or stack, for deployment of large-scale, enterprise networks with many attached devices and work-groups, allowing for scalability and cost-effectiveness.

VLAN support

Up to 256 port-based VLANs can be configured per individual switch or per stack to extend the broadcast domain and segment network traffic. The 256 VLANs can be spread among port-based and MAC source address-based VLANs (up to a maximum of 48 MAC source address-based VLANs). The 256 VLANs can be on a standalone switch or across a stack. Protocol-based VLANs allow switch ports to be assigned to a broadcast domain based on the protocol information within the packet. These VLANs localize broadcast traffic and assure that the specified protocol type packets are sent only to the protocol-based VLAN ports.

Shared VLAN (SVL) and Independent VLAN Learning (IVL) are supported. With SVL support, all VLANs in the switch share the same forwarding database. IVL allows individual VLANs to have separate forwarding databases within the switch, and it allows the switch to handle duplicate MAC addresses if the addresses are in different VLANs.

IGMP snooping

BayStack 470 Switches feature IP Multicast support by examining ('snooping') all Internet Group Multicast Protocol (IGMP) traffic in hardware at line rate, and pruning unwanted data streams from affecting network or end-station performance.

Multiple spanning tree protocol groups

BayStack 470 Switches support multiple spanning tree groups (STGs). They support a maximum of eight STGs, either all in one standalone switch or across a stack consisting solely of BayStack 470 Switches. Multiple STGs provide multiple data paths, which can be used for load balancing and redundancy.

Command Line Interface (CLI)

The CLI is used to automate general management and configuration of BayStack 470 Switches. The CLI may be used through a Telnet/Secure Shell session or through the serial port on the console.

ASCII configuration file

BayStack 470 Switches can download a user-editable ASCII configuration file from a Trivial File Transfer Protocol (TFTP) server. The ASCII configuration file can be loaded automatically at boot time or on-demand using the management systems (console menus or CLI). Once downloaded, the configuration file automatically configures the switch or stack according to the CLI commands in the file. This feature allows the flexibility of creating command configuration files that can be used on several switches or stacks with minor modifications.

Support for Spanning Tree Protocol

Built-in support for Spanning Tree Protocol (IEEE 802.1D) detects and eliminates logical loops in the network. When multiple paths exist, the switch will automatically place some ports on standby to form a network with the most efficient traffic pathways, avoiding the continual looping of frames.

Port mirroring

The port mirroring feature (sometimes referred to as 'conversation steering') allows the network administrator to designate a single switch port as a traffic monitor for a specified port. Port mirroring copies packets flowing into a specified port and sends the replicated data to the mirrored port for in-depth analysis of switched traffic patterns to troubleshoot problems and optimize network configurations. Additionally, an external probe device can be attached to the designated monitor port.

Advanced management features

BootP and TFTP support allows centralized switch IP address assignment, software upgrades, and SNMP agent updates over the network. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console and TELNET logins.

LED indicators

The LED indicators on the front panel make it easy to monitor the switch and port status and help in isolating and diagnosing switch problems.

Auto MDI/MDIX

BayStack 470 Switches can be connected to a hub or another switch quickly and cost-effectively. Normally, a crossover cable is needed for this purpose, but with the BayStack 470 Switch, an inexpensive straight-through cable or a crossover cable can be used.

When a cable is connected to one of the 10/100 ports on the switch, the switch port automatically can detect the energy on the cable and configures itself. This feature makes configuration easier, as it eliminates the need for an MDI/MDIX port; any port may be used for connection to a hub or switch.

Network management

Web-based management

Web-based network management makes managing the BayStack 470 Switch stack easy with a Web browser. Summary, configuration, fault, statistics, application, administration, and support pages can be provided for the entire stack. Traffic classification and prioritization can be set via the Web-based QoS Wizard and advanced configuration tool. Real-time sampling provides up-to-date LED statistical information for stacked units. The Web interface also allows for static configuration of numerous parameters of the device.

On-box management

Network management begins with the device. BayStack 470 Switches support four groups of Remote Monitoring (RMON) on all ports and are SNMPv3 (Simple Network Management Protocol) compliant. RMON2 is supported via the port mirroring function using an external RMON2 probe. The SNMP agent software resides in the switch and uses the information it collects to provide management for all ports in the stack, providing comprehensive network monitoring capabilities. In addition, the agent also provides the ability to set up policy-based networks by supporting the Common Open Policy Support (COPS) protocol.

Configuration management

The process of configuration begins with a single device but finishes across multiple devices. Java Device Manager (JDM) is the GUI device configuration tool for configuring a single device. It uses a common user interface and workflow that supports many Nortel Networks Ethernet switches. This commonality allows the network manager to become familiar with one tool instead of multiple tools. Furthermore, JDM also supports SNMPv3, allowing network managers to securely manage their network. Optivity Switch Manager (OSM) 4.0 is a Java™-based, real-time, configuration management application for Nortel Networks Ethernet products including BayStack 470 Switches. It enables network managers to discover, view, and configure more than 500 network devices and their physical links on a topology map. Configuration is stored in Non-Volatile Random Access Memory (NVRAM).

Fault management and resolution

With Optivity Network Management System (ONMS), the network manager has quick access to the information required to manage and isolate all network events on BayStack 470 switches. Tools such as Physical Topology View inform the network manager of how a particular event is affecting the physical connectivity within the network. End Node Locate tool provides the ability to locate a failing end node and, with one mouse click, provides access to the RMON statistics for the failing Ethernet port supporting that end node. These solutions provide visual and statistical tools necessary to quickly resolve any network event or to manage performance in real-time. The BayStack 470 Switches support "syslog" capability that helps in troubleshooting network issues.

Quality of Service

The BayStack 470 Switch's QoS features allow you to not just utilize bandwidth more efficiently, optimizing existing network resources and capabilities, but also provide packet classification and marking at the edge of the network—simplifying the QoS deployment at the aggregation and core of the network. By classifying, prioritizing, policing, and marking LAN traffic, networks can offer reliable connectivity and required bandwidth for mission-critical applications like IP Telephony and mission-critical data applications to specific groups and users, and to individual devices.

For each of these applications, advanced QoS features support Internet Engineering Task Force (IETF) standard DiffServ QoS architecture—a packet classification based on the content of packet header fields (voice, video, data), traffic policing, and remote sniffing.

Queuing function

BayStack 470 Switches provide network availability for mission-critical applications, devices, and users. This is done by classifying, prioritizing, and marking LAN IP traffic using up to eight hardware-based IP service class queues (on the Gigabit uplink ports) based on the following parameters:

- ToS/DSCP marking
- IP source address/destination address or subnets
- TCP/UDP source/destination port/port range
- 802.1p priority bits
- Ingress physical source port
- IP protocol ID (e.g., TCP, UDP, IGMP, ICMP, RSVP)
- EtherType (e.g., IP, IPX)
- VLAN ID

The switches have the ability to read packets that have been marked from other devices such as the Passport 8600 Switch. The switches support Strict Priority Queuing as well as the Weighted Round Robin method. The Weighted Round Robin prevents normal priority traffic from being starved by expedited traffic (on a per packet basis).

QoS and policy management

QoS provides the ability to read, alter, prioritize, tag, or mark IP traffic based upon information imbedded in the Type of Service (ToS) field. Based on the IETF Committee's industry standards, BayStack 470 Switches provide the ability to prioritize traffic based upon the required level of service for a given transaction. This level of service can be marked in the embedded information inside each IP packet's ToS field. DiffServ is based upon the ToS field. BayStack 470 Switches have Application Specific Integrated Circuits (ASICs) to enable DiffServ Code points to be mapped to 802.1p. The QoS policies can be configured via the BayStack 470 Switch's built-in Web-based management tools to facilitate QoS or alternatively, Optivity Policy Services can be utilized for dynamic end-to-end enterprise-wide policy and QoS management—facilitated through the Common Open Policy Service (COPS) protocol.

Quality of Service provisioning

With Optivity Policy Services, policies can be created through a simple and intuitive drag-and-drop workflow. Optivity Policy Services is the Policy Decision Point in a DiffServ QoS implementation.

Further benefits include:

- Simple intuitive policy creation
- Ability to re-use common filter sets
- Provision of a network-wide view of policies currently being enforced
- Ability to avoid QoS provisioning errors
- Centrally managed DSCP and 802.1p queue mapping tables
- Saved time in provisioning the network—as thousands of CLI or Web transactions are reduced to a few simple actions

Simplified QoS

The BayStack 470 Switch supports Nortel Networks Service Classes (NNSC), which provide simplified QoS provisioning. NNSCs provide factory-default QoS configurations, eliminating the complexities often associated with QoS-enabled network deployments.

NNSCs provide default settings such as:

- DSCP marking per class
- DiffServ forwarding behavior (PHB) per class
- DSCP to queue mapping
- DSCP to 802.1p mapping
- Default scheduler per class

By classifying the traffic and placing it into an NNSC, complex QoS configurations are eliminated. NNSCs simplify the deployment of a QoS-enabled network with Nortel Networks switching solutions. Using the Web-based interface, select the NNSC that best suits the type of traffic or application being classified on each Nortel Networks switching product and take advantage of the default QoS settings. This saves on provisioning time but most importantly, ensures that the QoS functions are provisioned consistently across the network.

NNSCs are also supported on the Passport 8600 Routing Switch, BayStack 470 Switches, and the BayStack Business Policy Switch.

Traffic policing

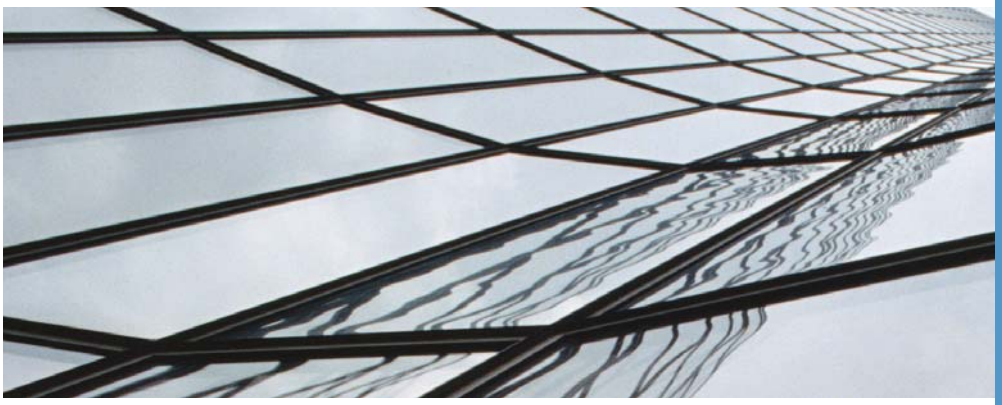
Traffic policing enables provisioning of different levels of service by limiting traffic throughput at the ingress (incoming) port of the BayStack 470 Switch. For example, if a port is set to a certain speed, such as 10 Mbps, all traffic above 10 Mbps will be dropped or re-marked with lower priority in the event of congestion. The bandwidth guarantee can be specified in increments as small as 1 kbps. Service providers will find this especially useful to control bandwidth to their customers.

IP traffic shaping

IP traffic shaping offers the ability to smooth IP classified traffic from the Gigabit uplink ports of a single BayStack 470 Switch. While traffic policing is needed to provide different levels of service to data streams on the ingress ports, traffic shaping is needed to smooth the traffic on the uplink connection from the BayStack 470 Switch to the network core, yielding the most efficient bandwidth utilization. Service providers or carriers utilize this feature when they are selling Ethernet in place of the traditional Frame Relay, ISDN, or ATM WAN access solutions. Some enterprise customers use traffic shaping as a mechanism to limit bandwidth without having to swap out physical interfaces, leaving them room to grow.

Summary

With more than 100 years in telecommunications, Nortel Networks is uniquely positioned to help your business reduce cost by combining voice and data into an integrated system. Why take a chance on a vendor that only understands part of the equation? Let us show you how the BayStack 470 Switches, along with other Nortel Networks products, can increase your profitability, streamline your business operations, increase productivity, and help you gain the competitive edge.



Technical specifications

Table 2. BayStack 470 Switches technical specifications

Performance specifications	
Switch fabric	2.56 Gbps
Frame forward rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic
Memory	16 MB SDRAM
Port forwarding/filtering performance (64-byte packets)	For 10 Mbps 14,880 pps maximum For 100 Mbps 148,810 pps maximum
For 1000 Mbps	1,488,100 pps maximum
Address database size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Frame length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)
Data rate 10 Mbps Manchester encoded or 100 Mbps 4MB - 5MB encoded	
Interface options	
10BASE-T/100BASE-TX	RJ-45 (8-pin modular) with Auto MDI/MDIX
The BayStack 470 Switches support the following GBICs:	
1000BASE-SX	Uses shortwave length 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable
1000BASE-LX	Uses longwave length 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable
1000BASE-XD	Uses single mode fiber to connect devices over distances up to 40 km (31 mi), depending on the quality of the cable
1000BASE-ZX	Uses single mode fiber to connect devices over distances up to 70 km (43 mi), depending on the quality of the cable. The ports on this GBIC operate only in full-duplex mode.
1000Base-CWDM	Eight GBIC types with 1470-1610nm (in 20nm intervals) with LC connector to connect devices over distances up to 70km
LED indicators	
Per-port status LEDs	10 or 100 Mbps port speed, Power over Ethernet detection, link status
System status LEDs	Power, system, RPSU, stack mode, base mode
Network protocol and standards compatibility	
IEEE 802.3 10BASE-T (ISO/IEC 8802 3, Clause 14)	
IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)	
IEEE 802.3u Autosensing (ISO/IEC 8802-3, Clause 28)	
IEEE 802.3x (Flow control on the Gigabit uplink port)	
IEEE 802.1p (Prioritizing)	
IEEE 802.1Q (VLAN tagging)	
IEEE 802.3z (Gigabit)	
IEEE 802.1D (Spanning Tree Protocol)	
IEEE 802.3ad (Static/dynamic- LACP)	
IEEE 802.1s†	
IEEE 802.1w†	
IETF DiffServ	

† Future software release

Technical specifications

Table 2. BayStack 470 Switches technical specifications (continued)

RFC support

RFC 791 (IP); RFC 792 (ICMP); RFC 793 (TCP); RFC 783 (TFTP); RFC 826 (ARP); RFC 768 (UDP); RFC 854 (TELNET); RFC 951 (Bootp); RFC 2236 (IGMPv2); RFC 1112 (IGMPv1); RFC 1945 (HTTP v1.0); RFC 2138 (RADIUS); RFC 1573 (IF-MIB); RFC 894 (IP over Ethernet); RFC 2674 (Q MIB); RFC 2030 (Simple NTP); RFC 1213 (MIB-II); RFC 1493 (Bridge MIB); RFC 2863 (Interfaces Group MIB); RFC 2665 (Ethernet MIB); RFC 2737 (Entity MIBv2); RFC 2819 (RMON MIB); RFC 1757 (RMON); RFC 1271 (RMON); RFC 1157 (SNMP); RFC 2748 (COPS); RFC 2940 (COPS Clients); RFC 3084 (COPS Provisioning); RFC 2570 (SNMPv3); RFC 2571 (SNMP Frameworks); RFC 2572 (SNMP Message Processing) RFC 2573 (SNMPv3 Applications); RFC 2574 (SNMPv3 USM); RFC 2575 (SNMPv3 VACM); RFC 2576 (SNMPv3);

Electrical specifications

Input voltage (AC version) 100-240 VAC @ 47 to 63 Hz
Input power consumption (AC version) 90 W max
Input current (AC version) 1.0 A @ 100 VAC, 0.5 A @ 240VAC

Physical specifications

Weight: 4.8 kg (10.56 lb) for -24T, 5.0 kg (11.0 lb) for -48T
Height: 4.37 cm (1.72 inches)
Width: 43.82 cm (17.25 inches)
Depth: 35.29 cm (13.89 inches)

Environmental specifications

Operating temperature: 0° to 40°C (32° to 104°F)
Storage temperature: –25° to +70°C (-13° to 158°F)
Operating humidity: 85% maximum relative humidity, non-condensing
Storage humidity: 95% maximum relative humidity, non-condensing
Operating altitude: Up to 3,024 m (10,000 ft) above sea level
Storage altitude Up to 12,096 m (40,000 ft) above sea level

Safety agency approvals

USA, UL60950
Canada, CAN/CSA-22.2 No.60950
Europe, EN60950/IEC 60950, CB report with all national deviation
Australia/New Zealand, AS/NZS 60950
Mexico NOM-019

Electromagnetic emissions summary

Meets the following standards USA, FCC CFR47 Part 15, subpart B, Class A
Canada, ICES-003, Class A
Europe, EN55022, CISPR 22, Class A
Australia/New Zealand, AS/NZS 3548, Class A
Japan, VCCI-V-3/02.04, Class A
Taiwan, CNS 13438, Class A
CE

Electromagnetic immunity

Europe, EN55024, CISPR 24