Cisco Catalyst Blade Switch 3020 for HP

The Cisco® Catalyst® Blade Switch 3020 (Figure 1) for HP is an integrated switch for HP c-Class BladeSystem customers that extends resilient and secure Cisco infrastructure services to the server edge and utilizes existing network investments to help reduce operational expenses.

Figure 1. Cisco Catalyst Blade Switch 3020

The Cisco Catalyst Blade Switch 3020 for HP provides HP c-Class BladeSystem customers with an integrated switching solution that dramatically reduces cable complexity. This solution offers consistent network services such as high availability, quality of service (QoS), and security. It utilizes the comprehensive Cisco management framework to simplify ongoing operations. Cisco advanced network services in combination with simplified management help reduce total cost of ownership.

Configuration

The Cisco Catalyst Blade Switch 3020 for HP provides the following hardware configuration:

- Sixteen internal 1000BASE ports connected to servers through the c-Class BladeSystem backplane
- Up to eight external Gigabit Ethernet uplink ports:
  - Four external dual-media Ethernet interfaces. Interfaces can be either 1000BASE-SX, 1000BASE-LX/LH Small Form-Factor Pluggable (SFP) or 10/100/1000BASE-T ports. The SFP cage supports Gigabit Ethernet Fiber short-wavelength SFP modules from Cisco Systems.
  - Four additional external 10/100/1000BASE-T ports. Two of these ports can be configured to provide an internal crossover connection to an associated additional Cisco Catalyst Blade Switch 3020.
- One Fast Ethernet connection to the HP Enclosure Onboard Administrator
- One external console port

Available with Cisco IOS® Software, LAN Base image, the Cisco Catalyst Blade Switch 3020 offers a complete set of intelligent services to deliver security, QoS, and availability in the server farm access environment.

Intelligence in the Server Access Network

As companies increasingly rely on the network as the strategic business infrastructure, and with servers having Gigabit Ethernet capabilities, it is more important than ever to consistently try to ensure network security, high availability, and QoS-from the server edge out to the clients at the network edge.

Cisco Catalyst switches, including the Cisco Catalyst Blade Switch 3020, enable companies to realize the full benefits of adding intelligent services into their networks. These capabilities make the server network infrastructure:

- Secure, to protect confidential information
- Highly available, to meet on time-critical needs
- Capable of differentiating and controlling traffic flows to handle the increasing number of critical business applications
- Easily manageable, to reduce operational expenses

Enhanced Security

With the wide range of security features that the Cisco Catalyst Blade Switch 3020 offers, businesses can protect important information, keep unauthorized people off the network, guard privacy, and maintain uninterrupted operation.

To guard against denial-of-service and other attacks, access control lists (ACLs) can be used to restrict access to sensitive portions of the network, blocking unauthorized access to servers and applications, by denying packets based on source and destination MAC addresses, IP addresses, or Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. ACL lookups are done in hardware, so forwarding performance is not compromised when ACL-based security is implemented.

Port security can be used to limit access on an Ethernet port based on the MAC address of the device to which it is connected. It can also control the total number of devices plugged into a switch port, reducing the risks of unauthorized servers being plugged into the blade enclosure.

Secure Shell (SSH) Protocol, Kerberos Protocol, and Simple Network Management Protocol Version 3 (SNMPv3) encrypt administrative and network management information, protecting the network from tampering or eavesdropping. TACACS+ and RADIUS authentication enable centralized access control of switches and restrict unauthorized users from altering the configurations. Alternatively, a local username and password database can be configured on the switch itself. Fifteen levels of authorization on the switch console and two levels on the Web-based management interface provide the ability to give different levels of configuration capabilities to different administrators.

The MAC address notification feature can be used to monitor the network and track servers by sending an alert to a management station so that network administrators know when and where servers are plugged into or removed from a blade enclosure. The Dynamic Host Configuration Protocol (DHCP) Interface Tracker (Option 82) feature can provide location-based IP address assignment by providing both the switch and the port ID to a DHCP server. An Option 82-aware DHCP server such as the Cisco Network Registrar can use this information to assign the specific IP address to the requesting server.

The Private VLAN Edge feature isolates ports on a switch, helping to ensure that traffic travels directly from the entry point to the aggregation device through a virtual path and cannot be directed to another port. This can help isolate a server from other servers in the same blade enclosure.

High Availability

The Cisco Catalyst Blade Switch 3020 offers several high-availability features to minimize network downtime, maintain mission-critical servers and applications, and reduce total cost of ownership.

Enhancements to the standard Spanning Tree Protocol, such as Per-VLAN Spanning Tree Plus (PVST+), UplinkFast, and PortFast, maximize network uptime. PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. UplinkFast and PortFast help reduce the standard 30- to 60-second Spanning Tree Protocol convergence time. Loop Guard and Bridge Protocol Data Unit (BPDU) Guard provide Spanning Tree Protocol loop avoidance.

Customers can achieve maximum power and cooling availability for a server farm data network when a Cisco Catalyst Blade Switch 3020 uses the redundant power and cooling capabilities of the blade enclosure.

Advanced QoS

The Cisco Catalyst Blade Switch 3020 offers superior multilayer, granular QoS features to avoid congestion and help ensure that network traffic is properly classified and prioritized. The Cisco Catalyst Blade Switch 3020 can classify, police, mark, queue, and schedule incoming packets and can queue and schedule packets at egress. Packet classification allows the network elements to discriminate between various traffic flows and to enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, the Cisco Catalyst Blade Switch 3020 first identifies traffic flows or packet groups and classifies or reclassifies these groups using the differentiated services code point (DSCP) field or the 802.1p class-of-service (CoS) field. Classification can be based on criteria as specific as the source/destination IP address, source/destination MAC address, or Layer 4 TCP/UDP port. At the ingress, the Cisco Catalyst Blade Switch 3020 will also police to determine whether a packet is in or out of profile; mark to change the classification label, pass through, or drop out of profile packets; queue packets based on classification; and service based on configured weights. Control plane and data plane ACLs are supported on all ports to help ensure proper treatment on a per-packet basis. The Cisco Catalyst Blade Switch 3020 supports four egress queues per port, which allows the network administrator to be discriminating and specific in assigning priorities for the various applications in the server farm. At egress, the switch performs scheduling and congestion control. Scheduling is a process that determines the order in which the queues are processed. The Cisco Catalyst Blade Switch 3020 supports Shaped Round Robin (SRR) and strict priority queuing. The SRR queuing algorithm helps to ensure differential prioritization.

Management

The Catalyst Blade Switch 3020 comes with an embedded GUI device manager that simplifies initial configuration of a switch. Users now have the option to set up the switch through a Web browser. Users familiar with the Cisco command-line interface (CLI) can also use the CLI to do initial configuration and setup. Hence, users do not need any retraining.

The Cisco Catalyst Blade Switch 3020 provides for extensive management using SNMP network management platforms such as CiscoWorks for switched internetworks. Managed with CiscoWorks, Cisco Catalyst switches can be configured and managed to deliver end-to-end device, virtual LAN (VLAN), traffic, and policy management. As part of CiscoWorks, the Web-based Cisco Resource Manager Essentials (RME) offer automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Product Specifications

Table 1 shows product features and benefits.

Table 1. Product Features and Benefits

Category	Features and Benefits
Ease of use and ease of deployment	• Device Manager simplifies initial configuration using a Web browser • DHCP autoconfiguration of multiple switches through a boot server eases switch deployment. • Autosensing detects the speed of the upstream switch and automatically configures each 10/100/1000 uplink port for 10-, 100-, or 1000-Mbps operation, easing switch deployment in mixed 10, 100, and 1000BASE-T environments. • Autonegotiating on 10/100/1000 ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all switch ports. • Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel® groups or Gigabit EtherChannel groups to link to the upstream switch/router or server blades. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with upstream switches that conform to IEEE 802.3ad. This feature is similar to Cisco EtherChannel technology and PAgP. • Auto-media-dependent interface crossover (MDIX) automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed on a copper 10/100/1000 Base-T port. • Combo ports support an auto-media detect feature. No special configuration is required if a copper interface is used instead of the SFP. • DHCP Relay allows a DHCP relay agent to broadcast DHCP requests to the network DHCP server. • The default configuration stored in Flash memory helps ensure that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.
Availability and Scalability	

Category	Features and Benefits
Superior redundancy for fault backup	• IEEE 802.1D Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • Cisco UplinkFast and BackboneFast technologies help to ensure quick failover recovery, enhancing overall network stability and reliability. • Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree convergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) allows a spanning-tree instance per VLAN and enables each VLAN to use a different uplink, allowing better utilization of uplinks. • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) provides rapid spanning-tree convergence independent of spanning-tree timers. • Unidirectional Link Detection (UDLD) and Aggressive UDLD allow unidirectional links to be detected and disabled to avoid problems such as spanning-tree loops. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. • The Trunk Failover feature allows rapid failover to the redundant switch in the blade enclosure if all uplinks from the primary switch fail. When the uplinks fail, the switch shuts down the ports connected to the blade servers and lets network interface card (NIC) teaming software direct traffic to the redundant switch. This feature is also known as Link State Tracking. • Switch port autorecovery (errdisable) automatically attempts to reenable a link that is disabled because of a network error. • Power and cooling resiliency are provided through redundant power and cooling capabilities from the blade enclosure. • Bandwidth aggregation of up to 6 Gbps through Gigabit EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between this integrated switch and upstream switches/routers. • Per-port broadcast, multicast, and unicast storm control prevents faulty servers from degrading overall systems performance. • Internet Group Management Protocol (IGMP) snooping provides fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. • Multicast VLAN Registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.
QoS	
Advanced QoS	• Wire-rate performance for highly granular QoS functions (for example, granular rate limiting). • Asynchronous data flows upstream and downstream from the end station or on an uplink are easily managed using ingress policing and egress shaping. • 802.1p CoS and DSCP field classification are provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP/UDP port number. • Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps. • Up to 64 aggregate or individual policers per port are allowed. • Cisco control-plane and data-plane QoS ACLs on all ports help to ensure proper marking on a per-packet basis. • 4 egress queues per port enable differentiated management of up to 4 traffic flows • SRR scheduling helps to ensure differential prioritization of packet flows by intelligently servicing the egress queues. • Weighted Tail Drop (WTD) provides congestion avoidance at the ingress and egress queues before a disruption occurs. • Strict priority queuing guarantees that the highest-priority packets are serviced ahead of all other traffic. • The Cisco Committed Information Rate (CIR) function guarantees bandwidth in increments as low as 8 Kbps.
Security	

Category	Features and Benefits
Networkwide security features	• IEEE 802.1x allows dynamic, port-based security, providing server authentication. • IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific server, regardless of where the server is connected. • IEEE 802.1x and port security are provided to authenticate the port and manage network access for all MAC addresses, including those of the server. • IEEE 802.1x with an ACL assignment allows for specific identity-based security policies, regardless of where the server is connected. • IEEE 802.1x with Guest VLAN allows servers without 802.1x clients to have limited network access on the Guest VLAN. • Cisco security VLAN ACLs (VACLs) on all VLANs prevent unauthorized data flows from being bridged within VLANs. • Port-based ACLs (PACLs) allow security policies to be applied on individual switch ports. • SSH Protocol (v2), Kerberos, and SNMPv3 provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions. • Secure Sockets Layer (SSL) provides a secure means to use Web-based tools such as HTML-based device managers. • Private VLAN Edge provides security and isolation between switch ports, helping to ensure that users cannot snoop on other users' traffic. • Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Secure Intrusion Detection System (IDS) to take action when an intruder is detected. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • MAC address notification allows administrators to be notified of servers added to or removed from the network. • Port security secures the access to an access or trunk port based on the MAC address. • After a specific timeframe, the aging feature removes the MAC address from the switch to allow another server to connect to the same port. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • The user-selectable address-learning mode simplifies configuration and enhances security. • BPDU Guard shuts down Spanning Tree Protocol PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops. • Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes. • IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port. • Dynamic VLAN assignment is supported through implementation of the VLAN Membership Policy Server (VMPS) client function to provide flexibility in assigning ports to VLANs. Dynamic VLAN enables the fast assignment of IP addresses. • 1000 security access control entries are supported.

Category	Features and Benefits
Manageability	
	• Cisco IOS Software CLI support provides a common user interface and command set with all Cisco routers and Cisco Catalyst desktop switches. • Cisco Service Assurance Agent (SAA) support facilitates service-level management throughout the LAN. • VLAN trunks can be created from any port, using either standards-based 802.1Q tagging or the Cisco Inter-Switch Link (ISL) VLAN architecture. • Up to 1005 VLANs per switch and up to 128 spanning-tree instances per switch are supported. • 4096 VLAN IDs are supported. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • IGMP snooping provides fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. • Remote Switch Port Analyzer (RSPAN) allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network. • For enhanced traffic management, monitoring, and analysis, the Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events). • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination. • All four RMON groups are supported through a SPAN port, which permits traffic monitoring of a single port, a group of ports from a single network analyzer, or an RMON probe. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Time Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches. • Multifunction LEDs per port for port status, and switch-level status LEDs for system.
Device Manager	• Device Manager simplifies initial configuration of a switch through a Web browser. • The Web interface enables less-skilled personnel to quickly and simply set up switches, thereby reducing the cost of deployment.
CiscoWorks support	• CiscoWorks network-management software provides management capabilities on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. • SNMP v1, v2c, and v3 and Telnet interface support deliver comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Cisco Discovery Protocol versions 1 and 2 enable a CiscoWorks network-management station for automatic switch discovery.

Table 2 describes hardware.

Table 2. Hardware

Description	Specification
Performance	• 48-Gbps switching fabric • Forwarding rate based on 64-byte packets; up to 36 Mpps • 128 MB DDR SDRAM and 32 MB Flash memory • Configurable up to 8192 MAC addresses • Configurable up to 1000 IGMP groups and bridging entries • Configurable maximum transmission units (MTUs) of up to 9018 bytes (jumbo frames)
Connectors and Cabling	• Up to 8 external Gigabit Ethernet uplink ports: • 4 external 10/100/1000 SFP or 10/100/1000BASE-T combo ports. The SFP cage supports Gigabit Ethernet fiber short-wavelength SFP modules from Cisco Systems. • 4 additional external 10/100/1000BASE-T ports. Two of these ports can be configured to provide an internal crossover connection to an associated additional Cisco Catalyst Blade Switch 3020. • Management console port: RJ-45-to-DB9 cable for PC connections
Power Consumption	• 12V @ 5A (60 W)
Indicators	• Total of 18 LEDs on the faceplate: • 12 LEDs for uplink port status • 4 switch status LEDs • Two HP-specific LEDs to indicate health and UID status
Dimensions (L x W x H)	• 10.5 in. x 7.6 in. x 1.1 in.
Weight	• 2.8 lb
Environmental Ranges	• Operating temperature: 0°to 40℃ • Storage temperature: -25°to 70℃ • Operating relative humidity: 10 to 85% noncondensing • Storage relative humidity: 5 to 95% noncondensing
Predicted Mean Time Between Failure (MTBF)	• 334,000 hr

Table 3 shows management and standards support.

Table 3. Management and Standards Support

Description	Specification
MIB Support	• BRIDGE-MIB (RFC1493) • CISCO-CDP-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IGMP-FILTER-MIB • CISCO-IMAGE-MIB • CISCO IP-STAT-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-RTTMON-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TCP-MIB • CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • ETHERLIKE-MIB • IF-MIB (in and out counters for VLANs are not supported) • IGMP-MIB • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-FLASH-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-SYS-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (per the agent, capabilities specified in the CISCO-RFC1213-CAPABILITY.my) • RFC1253-MIB • RMON-MIB • RMON2-MIB • SNMP-FRAMEWORK-MIB • SNMP-MPD-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB • TCP-MIB • UDP-MIB

Description	Specification
Standards	• IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.3ad • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • 1000BASE-SX • 1000BASE-LX/LH • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3

Table 4 shows safety and compliance information.

Table 4. Safety and Compliance

Description	Specification
Safety Certifications	• UL/CUL recognition to UL/CSA 60950-1 • TUV to EN 60950-1 • CB report and certificate to IEC 60950-1 with all country deviations • CE Marking
Electromagnetic Compatibility Certifications	• FCC Part 15 Class A • EN 55022 Class A (CISPR22 Class A) • VCCI Class A • AS/NZS 3548 Class A or AS/NZS CISPR22 Class A • MIC Class A • CE Marking
Telecommunications	• CLEI code
Warranty	• 90 days

Service and Support

Cisco is committed to minimizing total cost of ownership and offers technical support services to help ensure that Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software. Table 5 describes service and support that is available directly from Cisco and through resellers.

Table 5. Service and Support

Technical Support Service	Features	Benefits
Cisco SMARTnet®	• Access to Cisco IOS Software updates • Web access to technical support tools and repositories • 24-hour telephone support through the Cisco Technical Assistance Center (TAC) • Advance replacement of hardware	• Minimizes network downtime through reliable day-to-day support and prompt resolution of critical network issues • Lowers total cost of ownership by using Cisco networking expertise and knowledge • Protects your network investment through Cisco IOS Software updates that provide patches and new function

Table 6 shows ordering information.

Table 6. Ordering Information

Part Number	Description
WS-CBS3020-HPQ	Cisco Catalyst Blade Switch 3020 for HP
GLC-LH-SM=	Gigabit Ethernet SFP, LC connector, long-wavelength / long-haul transceiver (single mode)
GLC-SX-MM=	Gigabit Ethernet SFP, LC connector, short-wavelength transceiver (multimode)
CON-SNT-CBS3020	Cisco SMARTnet with 8x5 next business day (NBD) hardware advance replacement
CON-SNTE-CBS3020	Cisco SMARTnet with 8x5 4-hour hardware advance replacement
CON-SNTP-CBS3020	Cisco SMARTnet with 24x7 4-hour hardware advance replacement
CON-S2P-CBS3020	Cisco SMARTnet with 24x7 2-hour hardware advance replacement

For more information about Cisco products, contact:

- United States and Canada: (toll free) 800 553-6387
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- http://www.cisco.com

For more information about HP's c-Class BladeSystem, contact http://www.HP.com

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-351226-01 4/07

