Third party information brought to you courtesy of Dell

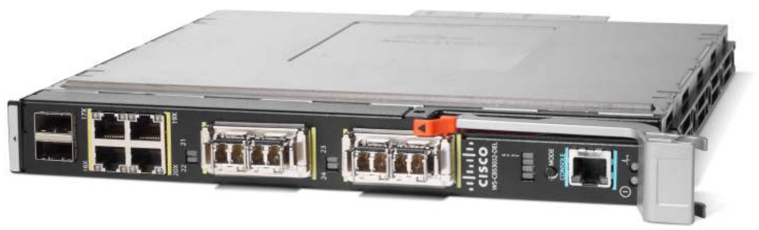
Data Sheet

Cisco Catalyst Blade Switch 3032 for Dell M1000e

Product Overview

The Cisco Catalyst® Blade Switch 3032 for Dell M1000e (Figure 1) is an integrated switch for Dell M1000e customers that extends resilient and secure Cisco® infrastructure services to the server edge and uses existing network investment to help reduce operating expenses.

Figure 1. Cisco Catalyst Blade Switch 3032 for Dell M1000e



The Cisco Catalyst Blade Switch 3032 for Dell M1000e provides Dell M1000e 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 uses the comprehensive Cisco management framework to simplify ongoing operations. Cisco advanced network services in combination with simplified management help reduce total cost of ownership (TCO).

Configuration

The Cisco Catalyst Blade Switch 3032 for Dell M1000e provides the following hardware configuration:

- 16 internal 1000BASE ports connected to servers through the Dell M1000e backplane
- Up to 8 Gigabit Ethernet uplink ports: 4 10/100/1000BASE-T ports and 4 Small Form-Factor Pluggable (SFP) Gigabit Ethernet ports (using Cisco TwinGig Converter Modules in the X2 slots)
- One external console port

Available with Cisco IOS® Software, with the IP Base image, the Cisco Catalyst Blade Switch 3032 offers a complete set of intelligent services to deliver security, QoS, basic IP routing, and high availability in the server farm access environment.

Features and Benefits

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 to the clients at the network edge.

Cisco Catalyst switches, including the Cisco Catalyst Blade Switch 3032, enable companies to realize the full benefits of adding intelligent services to 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 3032 offers, businesses can protect important information, keep unauthorized people off the network, guard privacy, and maintain uninterrupted operation.

To guard against denial-of-service (DoS) 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, and TCP and User Datagram Protocol (UDP) ports. ACL lookups are performed 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 the port is connected. Port security can also control the total number of devices plugged into a switch port, reducing the risk from unauthorized servers 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 and eavesdropping. TACACS+ and RADIUS authentication enable centralized access control of switches and restrict unauthorized users from altering the configurations. Alternatively, a local user name 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 capability 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 and Private VLAN Edge features isolate ports on a switch, helping ensure that traffic travels directly from the entry point to the aggregation device through a virtual path and cannot be directed to another port and thus helping isolate a server from other servers in the same blade enclosure.

High Availability

The Cisco Catalyst Blade Switch 3032 offers several high-availability features to minimize network downtime, maintain mission-critical servers and applications, and reduce TCO.

Enhancements to the standard Spanning Tree Protocol, such as Per-VLAN Spanning Tree Plus (PVST+), UplinkFast, and PortFast, maximize network uptime. PVST+ allows 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.

The Cisco Catalyst Blade Switch 3032 uses redundant power and cooling capabilities of the Dell PowerEdge M1000e infrastructure to provide maximum availability to customers.

Advanced QoS

The Cisco Catalyst Blade Switch 3032 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 3032 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 traffic flows and enforce policies based on Layer 2 and 3 QoS fields.

To implement QoS, the Cisco Catalyst Blade Switch 3032 first identifies traffic flows or packet groups and classifies or reclassifies these groups using the differentiated services code point (DSCP) field or the IEEE 802.1p class-of-service (CoS) field. Classification can be based on criteria as specific as the source or destination IP address, source or destination MAC address, or Layer 4 TCP or UDP port. At ingress, the Cisco Catalyst Blade Switch 3032 will also police to determine whether a packet is in or out of profile; mark to change the classification label, pass-through, or dropout of profile packets; queue packets based on classification; and queue services 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 3032 supports four egress queues per port, which allows the network administrator to be discriminating and specific in assigning priorities for the 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 3032 supports Shaped Round Robin (SRR) and strict priority queuing. The SRR queuing algorithm helps ensure differential prioritization.

Management

The Catalyst Blade Switch 3032 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 perform initial configuration and setup. Hence, users do not need any retraining.

The Cisco Catalyst Blade Switch 3032 provides extensive management capabilities 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, VLAN, traffic, and policy management. As part of CiscoWorks, the Web-based

CiscoWorks Resource Manager Essentials (RME) offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Basic IP Routing

The Catalyst Blade Switch 3032 offers customers high-performance basic IP routing. It uses Cisco Express Forwarding (CEF/dCEF) hardware routing architecture to deliver basic IP unicast routing protocols that include static routing, Routing Information Protocol, and Cisco Enhanced Integrated Gateway Routing Protocol (EIGRP) Stub. The switch does not support Open Shortest Path First (OSPF) Protocol and Border Gateway Protocol (BGP).

Table 1 summarizes product features and benefits.

Table 1. Features and Benefits

Category	Features and Benefits
Ease of use and ease of deployment	• Integration with the chassis management controller (CMC) in the Dell PowerEdge M1000e enclosure enables customers to configure IP address and access the console. • Cisco 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. • Autonegotiation 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 or 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 10/100/1000BASE-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	

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 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 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 and routers. • Per-port broadcast, multicast, and unicast storm control prevents faulty servers from degrading overall system 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 enables 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. • IEE 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 or UDP port number. • Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP or 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 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 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	

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 specific identity-based security policies, regardless of where the server is connected. • IEEE 802.1x with guest VLAN allows servers without IEEE 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. • SSHv2, 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 ensure that users cannot snoop on other users' traffic. • Bidirectional data support on the Switched Port Analyzer (SPAN) port allows the Cisco Secure Intrusion Detection System (IDS) [[PLS PROVIDE FULL PRODUCT NAME; NOT ON MDS]] 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 access to an access or trunk port based on the MAC address. • After a specific time period, 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. • Dynamic Address Resolution Protocol (ARP) Inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP. • DHCP Snooping prevents malicious users from spoofing a DHCP server and sending out bogus addresses. This feature is used by other primary security features to prevent a number of other attacks such as ARP poisoning. • IP Source Guard prevents a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. • Private VLANs restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multi-access-like segment.
High-Performance Basic IP Routing	
	Cisco Express Forwarding hardware routing architecture delivers basic high-performance IP unicast routing. Protocols supported include: • Static Routes • Routing Information Protocol Version 1 (RIPv1) and RIPv2 • EIGRP Stub
Manageability	

	• Cisco IOS Software CLI support provides a user interface and command set in common 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 IEEE 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 SPAN (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 enabling downloading from a centralized location. • Network Time Protocol (NTP) provides an accurate and consistent timestamp for all intranet switches. • Multifunction LEDs are provided per port to show port status, and switch-level status LEDs are provided for the system.
Cisco Device Manager	Cisco 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.
Cisco Network Assistant	A PC-based network management application designed for server administrators in small to medium-sized data centers, Cisco Network Assistant offers centralized network management and configuration capabilities. This application also features an intuitive GUI where users can easily apply common services across Cisco switches and routers, such as the following: • Configuration management • Troubleshooting advice • Inventory reports • Event notification • Network security settings • Password synchronization • Drag-and-drop Cisco IOS Software upgrades • Secure wireless For detailed information about Cisco Network Assistant, visit http://www.cisco.com/go/cna.
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. • SNMPv1, v2c, and v3 and Telnet interface support delivers 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.

Product Specifications

Table 2 summarizes hardware specifications.

Table 2. Hardware Specifications

Description	Specification
Performance	• 48-Gbps switching fabric • Forwarding rate based on 64-byte packets; up to 36 million packets per second (mpps) • 256 MB DDR SDRAM and 64 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 10/100/1000BASE-T ports and 4 SFP Gigabit ports (using Cisco TwinGig Converter Modules in the X2 slots) • Management console port: RJ-45-to-DB9 cable for PC connections
Power consumption	12 volts (V) at 6.25 amperes (A)
Indicators	Total of 19 LEDs on the faceplate: • 12 LEDs for uplink port status • 5 switch-status LEDs • 2 Dell-specific LEDs
Dimensions (L x W x H)	9.8 x 9.1 x 1.1 inches (24.8 x 23.1 x 2.9 cm)
Weight	Approximately 4.0 lb (1.8 kg)
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)	Approximately 390,000 hours

Table 3 summarizes 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 (by agent; capabilities specified in 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

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 summarizes safety and compliance information.

Table 4. Safety and Compliance

Description	Specification
Safety certifications	• UL/CUL Recognition to UL/CSA 60950-1 • TUV Bauart 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) • EN55024 (CISPR24) • VCCI Class A • AS/NZS CISPR22 Class A • MIC • China EMC requirements • GOST
Telecommunications	CLEI code
Warranty	90 days

Service and Support

Cisco is committed to minimizing TCO 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 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 concerns • Lowers TCO by using Cisco networking expertise and knowledge • Protects your network investment through Cisco IOS Software updates that provide patches and new functions

Ordering Information

Table 6 provides ordering information.

Table 6. Ordering Information

Part Number	Description
WS-CBS3032-DEL	Cisco Catalyst Blade Switch 3032 for Dell M1000e
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-CBS3032	Cisco SMARTnet with 8x5 next business day (NBD) hardware advance replacement
CON-SNTE-CBS3032	Cisco SMARTnet with 8x5 4-hour hardware advance replacement
CON-SNTP-CBS3032	Cisco SMARTnet with 24x7 4-hour hardware advance replacement
CON-S2P-CBS3032	Cisco SMARTnet with 24x7 2-hour hardware advance replacement

For More Information

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 Dell M1000e, contact: http://www.dell.com.

Dell has tested and certified the Cisco 3032, 3130G, and 3130X switches for use in the Dell PowerEdge M1000e.

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 (USA) Pte. Ltd.
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

C78-442943-00 01/08