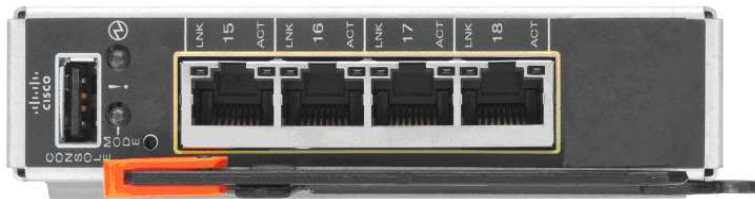# Cisco Catalyst Switch Module 3012 for IBM BladeCenter

Product Overview

The Cisco Catalyst® Switch Module 3012 (Figure 1) for IBM BladeCenter is an integrated switch for IBM BladeCenter customers that extends resilient and secure Cisco® infrastructure services to the server edge and uses existing network investments to help reduce operating expenses.

Figure 1. Cisco Catalyst Switch Module 3012

The Cisco Catalyst Switch Module 3012 provides IBM BladeCenter 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 Switch Module 3012 for IBM provides the following hardware configuration:

- Fourteen internal 1000BASE-T ports connected to servers through the BladeCenter backplane
- Four external 10/100/1000BASE-T uplink ports
- One external console port

Available with Cisco IOS® Software, with the IP Base image, the Cisco Catalyst Switch Module 3012 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, consistently providing network security, high availability, and QoS, from the server edge to the clients at the network edge, is more important than ever.

Cisco Catalyst switches, including the Cisco Catalyst Switch Module 3012, enable companies to achieve the full benefits of intelligent services they add to their networks. These capabilities make the server network infrastructure:

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

Enhanced Security

With the wide range of security features that the Cisco Catalyst Switch Module 3012 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, or 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 be used to control the total number of devices plugged into a switch port, reducing the risk that unauthorized servers may plug 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 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 allow different levels of configuration capabilities to be given 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 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 feature can help isolate a server from other servers in the same blade enclosure.

High Availability

The Cisco Catalyst Switch Module 3012 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.

Customers can achieve maximum power and cooling availability for a server farm data network when a Cisco Catalyst Switch Module 3012 uses the redundant power and cooling capabilities of the blade enclosure.

Advanced QoS

The Cisco Catalyst Switch Module 3012 offers superior multilayer, granular QoS features to avoid congestion and help ensure that network traffic is properly classified and prioritized. The Cisco Catalyst Switch Module 3012 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 Layer 3 QoS fields.

To implement QoS, the Cisco Catalyst Switch Module 3012 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/UDP port. At ingress, the Cisco Catalyst Switch Module 3012 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 queue 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 Switch Module 3012 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 Switch Module 3012 supports Shaped Round Robin (SRR) and strict priority queuing. The SRR queuing algorithm helps ensure differential prioritization.

Management

The Catalyst Switch Module 3012 comes with an embedded GUI device manager that simplifies initial configuration of a switch. Users now have the option of setting 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 Switch Module 3012 enables extensive management using SNMP network management platforms such as CiscoWorks solutions for switched internetworks. Using with the CiscoWorks platform, Cisco Catalyst switches can be configured and managed to deliver end-to-end device, virtual LAN (VLAN), traffic, and policy management. 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 Switch Module 3012 offers customers high-sperformance 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 (RIP), 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 the features and benefits of the Cisco Catalyst Switch Module 3012.

Table 1.   Features and Benefits

Feature	Benefits
Ease of use and ease of deployment	• 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. • 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 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. • 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.

Feature	Benefits
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+ enables 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 Gigabit EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth of up to 4 Gbps with upstream switches and routers and up to 8 Gbps with downstream servers.
	• 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.
	• IEEE 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 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 helps ensure 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.

Feature	Benefits
Security	
Networkwide security features	• IEEE 802.1x allows dynamic, port-based security, providing server authentication.
	• IEEE 802.1x with VLAN assignment allows 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 the use of 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 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.
	• Dynamic ARP Inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.
	• 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.
	• 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 Cisco Secure Intrusion Prevention System (IPS 4200 Series Sensors) 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 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.
High-Performance Basic IP Routing	

Cisco Express Forwarding hardware routing architecture delivers basic high-performance IP unicast routing. Protocols supported include:
- Static routes
- RIPv1 and v2
- EIGRP Stub

Feature	Benefits
Manageability	
	• The Cisco IOS Software CLI support provides a common user interface and command set for 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.
	• 4k 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 downloading from a centralized location.
	• Network Time Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.
	• Multifunction LEDs per port show port status, and switch-level LEDs show the status 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.
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 enables 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 lists hardware specifications for the Cisco Catalyst Switch Module 3012.

Table 2.   Hardware Specifications

Description	Specification
Performance	• 36-Gbps switching fabric • Forwarding rate based on 64-byte packets; up to 36 million packets per second (mpps) • 256 MB SDRAM and 64 MB flash memory • Up to 8192 MAC addresses configurable • Up to 1000 IGMP groups and bridging entries configurable • Maximum transmission units (MTUs) up to 9018 bytes (jumbo frames) configurable
Connectors and cabling	• 4 external 10/100/1000BASE-T ports. • Management console port: RJ-45-to-DB9 cable for PC connections
Power consumption	12V at 3.75A (45W) (maximum)
Indicators	Total of 10 LEDs on the faceplate: • 8 LEDs for uplink port status • 2 switch-status LEDs
Dimensions (L x W x H)	4.4 X 1.2 X 10.2 in (112 X 30 X 260 mm)
Weight	2.3 lb (1.1 kg)

Description	Specification
Environmental ranges	• Operating temperature: 32°to 104°F (0 to 40℃) • Storage temperature: -13°to 158℉ (–25 to 70℃) • Operating relative humidity: 10 to 85% noncondensing • Storage relative humidity: 5 to 95% noncondensing
Predicted mean time between failure (MTBF)	Approximately 436,000 hours

Table 3 summarizes Cisco Catalyst Switch Module 3012 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 • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3

Table 4 summarizes safety and compliance information for the Cisco Catalyst Switch Module 3012.

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

Ordering Information

Table 5 provides ordering information for the Cisco Catalyst Switch Module 3012.

Table 5.   Ordering Information

Part Number	Description
WS-CBS3012-IBM-I	Cisco Catalyst Switch Module 3012 for IBM
CON-SNT-CBS3012	Cisco SMARTnet with 8x5 next business day (NBD) hardware advance replacement
CON-SNTE-CBS3012	Cisco SMARTnet with 8x5 4-hour hardware advance replacement
CON-SNTP-CBS3012	Cisco SMARTnet with 24x7 4-hour hardware advance replacement
CON-S2P-CBS3012	Cisco SMARTnet with 24x7 2-hour hardware advance replacement

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 6 describes service and support that is available directly from Cisco and through resellers.

Table 6.   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 TCO by using Cisco networking expertise and knowledge • Protects network investments through Cisco IOS Software updates that provide patches and new functions

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 IBM BladeCenter, contact http://www.ibm.com.

ıllıılı.
CISCO™

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.